İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
HUKUK YÜKSEK LİSANS PROGRAMI

ÇOK ULUSLU GRUP ŞİRKETLERDE KİŞİSEL VERİ AKTARIMLARI

Baybora GÖKBORA
118613017

Dr. Öğr. Üyesi Candan YASAN TEPETAŞ

İSTANBUL
2022

Çok Uluslu Grup Şirketlerde Kişisel Veri Aktarımları

Personal Data Transfers in Multinational Group Companies

Baybora GÖKBORA

118613017

Tez Danışmanı : **Dr. Öğr. Üyesi Candan YASAN TEPETAŞ**
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Doç. Dr. Mesut Serdar ÇEKİN**
Türk-Alman Üniversitesi

Dr. Öğr. Üyesi Mehmet Bedii KAYA
İstanbul Bilgi Üniversitesi

Tezin Onaylandığı Tarih : 26 Temmuz 2022
Toplam Sayfa Sayısı : 213

Anahtar Kelimeler (Türkçe)
1) Çok Uluslu Grup Şirketler
2) Bağlayıcı Şirket Kuralları
3) Yurt Dışına Veri Aktarımı
4) Kişisel Verilerin Korunması
5) Gizlilik

Anahtar Kelimeler (İngilizce)
1) Multinational Group Companies
2) Binding Corporate Rules
3) Data Transfer to Abroad
4) Personal Data Protection
5) Privacy

İÇİNDEKİLER

KISALTMALAR

AAD : Avrupa Adalet Divanı

ABA : Avrupa Birliği Antlaşması

ABTHB : Avrupa Birliği Temel Haklar Bildirgesi

AB : Avrupa Birliği

AEA : Avrupa Ekonomik Alanı

APEC : Asya-Pasifik Ekonomik İş Birliği

AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi

BDDK : Bankacılık Denetleme ve Düzenleme Kurumu

BŞK : Bağlayıcı Şirket Kuralları

Direktif : 95/46/EC sayılı Avrupa Parlamentosu Direktifi

İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

Komisyon : Avrupa Komisyonu

Kurul : Kişisel Verileri Koruma Kurulu

Kurum : Kişisel Verileri Koruma Kurumu

KVKK : 6698 sayılı Kişisel Verilerin Korunması Kanunu

OECD : Ekonomik Kalkınma ve İş Birliği Örgütü

RKHK : 4054 sayılı Rekabetin Korunması Hakkında Kanun

TBK : 6098 sayılı Türk Borçlar Kanunu

TMK : 4721 sayılı Türk Medeni Kanunu

TTK : 6102 sayılı Türk Ticaret Kanunu

Tüzük : 2016/679 sayılı Avrupa Parlamentosu Genel Veri Koruma Tüzüğü

VERBİS : Veri Sorumluları Sicili için Geliştirilen Veri Sorumluları Sicil Bilgi Sistemi

WP : Avrupa Komisyonu Çalışma Grubu (Working Party)

ÖZET

Kişisel veriler, kimliği belirli ya da belirlenebilir bir kişiyi tanımlamaya yarayan her türlü bilgiyi ifade eder ve ait oldukları ilgili kişiyi tanımlamak adına farklı amaçlarla veri sorumluları ve veri işleyenlerce işlenir ve/veya aktarılır. Kişisel verilerin iş dünyasında işlenmesi ve aktarılması ise daha çok ticaret şirketleri ve bilhassa çok uluslu grup şirketler tarafından gerçekleştirilmektedir. Şirketlerin yürüttükleri ticari faaliyetleri ve yatırım hareketleri ile farklı ülkelerde ortaklıklar, bağlı şirketler, şubeler ve temsilcilikler kurması ile ülkeler arası veri aktarımları daha da ivme kazanmaktadır. Aynı topluluğun farklı grup üyeleri tarafından yürütülen üretim, satış, pazarlama, insan kaynakları vb. gibi faaliyetler ile eş zamanlı olarak grup üyesi şirketler arasında da kişisel verileri içeren bilgi ve belgeler aktarıma tabi tutulmakta ve bu aktarımların yoğunluğu şirketlerin söz konusu ticari faaliyetleri devam ettikçe her geçen gün daha da artış göstermektedir. Uluslararası ticaretin sürdürülmesine ve gelişimine engel yaratmamakla birlikte bir yandan da topluluk şirketleri arasında gerçekleşen söz konusu kişisel veri aktarımlarının hukuki bir zemine oturtulması gerek aktarıma tabi tutulan kişisel verilerin sahibi ilgili kişilerin kişisel verilerinin korunması hakkından doğan temel hak ve özgürlüklerinin gözetilmesi gerekse mevzuata uyum açısından büyük önem arz etmektedir. Bu kapsamda çok uluslu grup şirketlerin birer veri sorumlusu ve/veya veri işleyen olarak kabul edilmesi ve belirli veri koruma yükümlülükleri ile donatılmaları, grup üyesi şirketler arasındaki kişisel verilerin aktarım amaçlarının ve bunların veri işleme şartları ile uyumlu olup olmadıklarının incelenmesi ve bu aktarımların hukuka uygun bir şekilde gerçekleşmesi için gerekli güvenlik tedbirlerinin tespit edilerek aktarımın tarafı olan her bir grup üyesi şirket tarafından uygun bir şekilde alındığının kontrolü ve bu tedbirlerin devamlılığının sağlanması, aktarıma tabi tutulan kişisel verilerin korunması ve gizliliklerinin temin edilmesi noktasında önemli bir rol oynaktadır.

ABSTRACT

Personal data refers to any information that helps to identify an identified or identifiable person and is processed and/or transferred by data controllers and data processors for different purposes in order to identify the relevant person to whom they belong. The processing and transfer of personal data in the business world is mostly carried out by trading companies and especially multinational group companies. With the commercial activities and investment movements of said companies and the establishment of partnerships, subsidiaries, branches and representative offices in different countries, data transfers between countries are gaining acceleration. Activities like production, sales, marketing, human resources, etc., carried out by each group members cause that information and documents containing personal data are transferred between group member companies simultaneously, and the intensity of these transfers increases day by day as the said commercial activities of the companies continue. While it does not create an obstacle to the continuation and development of international trade, it is of great importance to establish a legal basis for personal data transfers between group companies, to observe the fundamental rights and freedoms arising from the protection of personal data of the data subject to the transfer, and to comply with the legislation. In this context, accepting multinational group companies as data controllers and/or data processors, charging them with certain data protection obligations, examining the purposes of transferring personal data between these group member companies and whether they are compatible with data processing conditions, ensuring that these transfers are legally enforced, determining the necessary security measures for the realization of the transfer, controlling that it is taken appropriately by each group member company that is a party to the transfer and ensuring the continuity of these measures play an important role for protection of the personal data that is transferred and ensuring their confidentiality.

GİRİŞ

Küreselleşen dünyada baş döndürücü bilimsel ve teknolojik gelişmeler sonucu kişisel verilerin üçüncü kişilere aktarımı çok hızlı ve oldukça kolay bir hale gelmiştir. Kişisel verilerin bu şekilde hızlı ve gelişigüzel aktarımı, bu verilerin aktarımından kaynaklı bir ekonomiyi de beraberinde getirmektedir. Günümüz dünyasında kişisel veriler de ekonomik bir değer olarak görülmekte ve büyük ölçekli global şirketler ve özellikle çok uluslu grup şirketler bu aktarımlardan çeşitli menfaatler sağlamayı amaçlamaktadır. Özellikle ticaret ağlarını ve yatırımlarını farklı ülkelerde kurdukları ve işlettikleri temsilcilikler, şubeler ve bağlı şirketler gibi yapılarla yürüten çok uluslu grup şirketler de kişisel verilerin yurt dışına aktarımında büyük rol oynamaktadır. Bu kapsamda gerek topluluk hukukundan gerekse grup üyesi şirketlerin sözleşmesel borçlarından doğan yükümlülüklerin yerine getirilmesi gerekse topluluk amaçları ve kurumsal politikalar uyarınca üye şirketlerce ve aralarında yürütülen çalışmalar ile kişisel verilerin bir ülkedeki grup üyesi şirketten diğer ülkedeki grup üyesi şirkete aktarılması gündeme gelebilmektedir. Ancak sınır ötesi veri alışverişinin işlerliği sağlanırken, kişisel verilere ilişkin temel hak ve özgürlüklerin de ulusal ve uluslararası düzeyde korunması ihtiyacı doğmuştur. Bu sebeple kişisel verileri koruma hukukunun ulusal niteliği dışında uluslararası niteliği de gelişim göstermekte ve bu aktarımları da düzenleme altına alacak şekilde kişisel verileri koruma hukuku başlı başına bir hukuk alanı olarak ortaya çıkmaktadır.

Şirketler ve hatta ülkeler ve ülke toplulukları arasında gerçekleşen büyük ve hızlı veri aktarımları, ekonomik ilerleme ve toplumların kültürel ve medeniyet gelişimi açısından belirli faydaları beraberinde getirse de veri aktarımı alanındaki bu büyüme ve hız, kişisel verilerin korunması ve kişisel verilerinin de bir parçası olduğu özel hayatların gizliliğine ilişkin önemli sorunlara ve endişelere yol açmaktadır. Bu kapsamda kişisel verilerin korunması için gerek ulusal gerekse uluslararası düzenlemeler ile bu duruma çözüm aranmaya çalışılmış ve aktarımların hukuki bir zemine oturtulması için çaba harcanmıştır. Öyle ki 1981 yılında çıkarılan

108 sayılı Kişilerin Otomatik Yollarla Verilerin İşlenmesine Karşın Korunmasına Dair Avrupa Konseyi Sözleşmesi ("108 Sayılı Sözleşme[1]") bu alanda yapılan ilk çalışmalardan biri olmuştur. Kişisel veri alanındaki öncü hukuklardan biri olan Avrupa Birliği ("AB") hukukunda ise 7 Aralık 2000 tarihinde imzaya açılan Avrupa Birliği Temel Haklar Bildirgesi[2] ("ABTHB") ile kişisel verilerin korunmasını talep hakkı, AB düzeyinde temel bir hak olarak benimsenmiştir. Bundan sonra kişisel veriler ve kişisel verilerinin oluşturduğu özel hayatın gizliliği, bu konuda yapı taşı bir düzenleme olan (mülga) 95/46 sayılı Avrupa Parlamentosu Direktifi[3] ("Direktif") ve sonrasında yürürlüğe giren 2016/679 sayılı Genel Veri Koruma Tüzüğü[4] ("Tüzük" veya "GDPR") ile korunmaya çalışılmıştır. Direktif ve Tüzük ile yurt dışına kişisel veri aktarımı konusunda ve özellikle çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına ilişkin ayrıntılı düzenlemelere ve aktarımın tarafı olan grup üyesi şirketlerce alınabilecek veri güvenliği tedbirleri mekanizmalarına yer verildiği görülmektedir. Diğer taraftan Avrupa Parlamentosu ve Konseyi'nin fikri mülkiyet haklarına ilişkin düzenlediği ve 2004/48/EC sayılı Direktif de kişilerin fikri mülkiyet haklarının yanı sıra bunlara bağlı kişisel veri haklarının korunmasına dair birtakım önemli hükümler içermektedir[5].

Türk hukukunda ise kişisel verilerin işlenmesi, kullanılması, kaydedilmesi ve aktarımı kuralları 6698 sayılı Kişisel Verilerin Korunması Kanunu[6] ("KVKK")'nda düzenleme altına alınmıştır. KVKK 7 Nisan 2016 tarihinde Resmî Gazete'de yayımlanmış ve hazırlanması esnasında AB hukukuna ait Direktif hükümleri esas

[1] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), https://www.coe.int/en/web/data-protection/convention108-and-protocol

[2] Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[4] The General Data Protection Regulation No. 2016/679 (EU) (GDPR) https://eur-lex.europa.eu/eli/reg/2016/679/oj

[5] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0048R%2801%29

[6] 6698 sayılı Kişisel Verileri Koruma Kanunu, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf

alınmıştır. KVKK uyarınca kişisel verilerin aktarımı bir kişisel veri işleme faaliyeti olarak sayılmış ve aktarımın hukuka uygunluğu için aktarıma tabi tutulacak kişisel verilerin sahibi ilgili kişinin açık rızasının bulunması temel şart olarak kabul edilmiştir. Kişisel verilerin işlenmesinin özel bir türü olan kişisel verilerin aktarımı yurt içine aktarım ve yurt dışına aktarım olarak iki bölümde ele alınmıştır. Kanun koyucu tarafından kişisel verilerin aktarıldığı ülkede de Türkiye'deki ile mevcut şartlara ve koruma düzeyine eşit bir korumadan faydalanabilmesi için kişisel verilerin yurt dışına aktarımı halinde yurt içine aktarımdan farklı olarak daha sıkı şartlar öngörülmüştür. Her ne kadar KVKK ve alt mevzuat hükümlerinde çok uluslu grup şirketler arasındaki kişisel veri aktarımına ilişkin açık düzenlemelere yer verilmemiş olsa da yurt dışına aktarıma ilişkin mevcut düzenlemeler çok uluslu grup şirketler arasındaki kişisel verilerin aktarımı için de uygun olduğu ölçüde uygulama alanı bulmaktadır.

KVKK kapsamında aktarımın yapılacağı ülke ilgili ülkede yeterli korumanın bulunup bulunmadığına göre bir ayrıma tabi tutmakta ve yeterli korumanın olduğu ülkelere veri aktarımında yurt içine aktarıma dair şartlardan en az birinin varlığı aranmaktadır. Diğer taraftan, yeterli korumanın olmadığı ülkelere aktarım yapılması durumunda ise KVKK kendi özgü yurt dışı tedbirlerinin alınması gerektiğini düzenlemekte ve Kişisel Verileri Koruma Kurulu ("Kurul")'nun bu aktarıma dair onay vermesini aramaktadır. Kurul tarafından halihazırda yeterli korumanın bulunduğu ülkeler listesi açıklanmış olmadığından ve bu sebeple Türkiye dışındaki tüm ülkelerin yeterli korumayı bulundurmayan ülke olduğu kabul edildiğinden yurt dışına kişisel veri aktarımına dair alınacak tedbirler ve Kurul onayı büyük bir önem taşımaktadır. Bu noktada Kurul, Türkiye'de kurulu grup üyesi şirketler tarafından veri sorumlu sıfatıyla yeterli korumanın bulunmadığı ülkelere kişisel veri aktarımı için belirli taahhütleri içeren özel sözleşmeler hazırlama yükümlülüğü getirmektedir. Bu taahhütnamelerde kişisel veri aktaran Türkiye'de kurulu veri sorumlusunun ve alıcı taraftaki grup üyesi şirketin yükümlülükleri, aktarıma tabi kişisel verilerin güvenliğini için alınması gereken teknik ve idari tedbirler, herhangi bir veri ihlalinde izlenmesi gereken yollar, ilgili kişilerin haklarını kullanabilmesi için topluluk

dahilinde kurulan şikâyet ve başvuru mekanizmalarına yer verilerek aktarımın hukuka uygun bir şekilde gerçekleşmesi amaçlanmaktadır.

Veri aktarım taahhütnamelerinin özel bir görünümü olan bağlayıcı şirket kuralları da yurt dışına veri aktarımında alınabilecek tedbirler arasında özellikle çok uluslu grup şirketler için büyük bir önem arz etmektedir. Bağlayıcı şirket kurallarının düzenlenme amacı, bu kuralları hazırlayıp taahhüt eden çok uluslu grup şirketler arasında sınırları hukuk kuralları ile belirlenmiş bir şekilde serbest veri aktarımlarının yapılabilmesidir. Bağlayıcı şirket kuralları, Tüzük kapsamında AB dışında bulunan ülkelere kişisel veri aktarımı yapılması halinde alınması gereken uygun güvenlik tedbirleri arasında yer almakta ve kişisel verileri koruma hukuku mevzuatına uyum sağlanması açısından temel yükümlülüklerin aktarıma taraf şirketlerce anlaşılması ve icra edilmesi noktasında yol gösterici niteliktedir.

Bağlayıcı şirket kurallarının hazırlanması ve Kurul'a sunulması ile birlikte çok uluslu bir grup şirketin vereceği kişisel verilerin işlenmesi ve aktarımına dair taahhüdünün, kişisel verileri koruma hukukuna temin edebileceği faydalar göz önünde bulundurulduğunda Kişisel Verileri Koruma Kurumu ("Kurum") da 10.04.2020 tarihli duyurusuyla Türkiye'de yerleşik veri sorumluları tarafından bağlayıcı şirket kurallarının hazırlanabileceği belirtmiştir. Kurum, duyurusunda çok uluslu şirketlerin kendi aralarında gerçekleştirecekleri kişisel veri aktarımları bakımından yurt dışına veri aktarım yollarının uygulamada yetersiz kalabildiğini kabul ederek, aslında bu kuralları bir aktarım seçeneği olarak sunmuştur. İlk olarak Tüzük'te düzenlenmiş olan bağlayıcı şirket kuralları, bu sayede KVKK uyarınca da Kurum'ca uygun görülen ve yurt dışına veri aktarımlarında kullanılabilecek alternatif uygun bir güvenlik tedbiri ve yolu haline gelmiştir. Bağlayıcı şirket kuralları ile veri güvenliğinin sağlanması adına ilgili kişiye tanınan yasal haklar, başvuru ve şikayet mekanizmaları, tazminat olanağı, topluluğun kişisel verilerin korunmasına ilişkin yasal düzenlemelere ve temel veri koruma ilkelerine uyum konusunda hesap verilebilirliğinin sağlanmasına dair taahhütler, aktarıma tabi verilerin korunması ve gizliliklerin sağlanması için alınması gereken idari ve teknik

tedbirler, topluluk dahilinde yapılacak risk analizleri ve yürütülecek denetimler ve aktarımın tarafı olan grup üyesi şirketler arasındaki sorumluluk mekanizması gibi konularda grup üyesi şirketleri bağlayıcı hukuki düzenlemelere yer verilmektedir.
Çalışmamızın ilk bölümünde kişisel veri ve aktarımı, aktarımın çeşitleri olarak yurt içine ve dışına aktarım kavramlarına genel bir bakış, AB hukuku, Türk hukuku ve ABD hukuku uyarınca kişisel verilerin yurt dışına aktarım kuralları ile çok uluslu grup şirketler arasındaki aktarımları ele alan hukuki düzenlemeler incelenmiştir. Çalışmamızın ikinci bölümünde ise, grup şirket ve çok uluslu şirket tanımları incelenmiş ve çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına ayrıntılı bir şekilde değinilerek bu aktarımların altında yatan ekonomik, ticari, hukuki, vergisel ve diğer sebepler irdelenmeye çalışılmıştır ve bu amaçlar ile ilgili olarak KVKK uyarınca kişisel veri aktarımı için öngörülen veri işleme şartları ışığında değerlendirmelere yer verilmiştir. Bununla birlikte çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının hukuka uygunluklarının temin edilmesi ve sürdürülebilir kılınması için uyulması gereken temel veri işleme ilkelerinden ve alınabilecek idari ve teknik tedbirlerden bahsedilmiştir. Çalışmamızın üçüncü ve son bölümünde ise çok uluslu grup şirketlerin kendi aralarındaki kişisel veri aktarımlarının hukuka uygun olarak yürütülmesi için alınabilecek tedbirler arasında önemli bir yere sahip olan bağlayıcı şirket kurallarına yer verilerek bağlayıcı şirket kurallarının hukuki niteliğine, tarihsel gelişimine, düzenlenme amaçlarına, faydalarına, mehaz düzenleme olan Tüzük kapsamında yer alan bağlayıcı şirket kuralları hükümlerine, bu kurallar ile grup üyesi şirketlerce verilen taahhütlere ve oluşturulan mekanizmalara değinilmiştir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİ AKTARIMI

1.1. Kişisel Veri Kavramı

1.1.1. Genel Olarak

Kişisel veri, KVKK m.3/1(d)'de "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, (...) ifade eder*." şeklinde tanımlanmıştır. Bir başka ifadeyle, kişisel veri; bir kişinin bireysel, ailevi, mesleki bilgilerine ilişkin olan, bu kişiyi diğer kişilerden ayırmaya yarayacak özellikleri sunan bütün verilerdir[7]. Bu kapsamda kişinin kimliğini ortaya çıkaran bilgiler, sağlık ve öğrenim bilgileri, ırk ve fiziksel özellikleri, tanıdıkları ile yaptığı haberleşmeleri, ikamet adresi, banka ve kart bilgileri, özel hayatına ilişkin bilgiler, sosyal medya hesapları, arkadaşları, dini inancı, siyasi fikirleri, çevrimiçi alışveriş hareketleri gibi bilgileri kişisel veri olarak tanımlanır[8]. Kısaca bir kişinin kişisel verileri o kişinin fiziki, tıbbi, fikri, ekonomik, kültürel veya sosyal kimliğine ilişkin tüm bilgilerdir. KVKK'nın kişisel verilere ilişkin getirdiği düzenlemelerine bakıldığında KVKK'nın sağladığı korumadan ancak gerçek kişilerin yararlanabildiği görülmektedir.

1.1.2. Özel Nitelikli Kişisel Veriler

"Özel nitelikli kişisel veriler", 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ("108 sayılı Sözleşme")'de "hassas veri" şeklinde tanımlanan ve özellikleri gereği kişilerin hak ve özgürlüklerini doğrudan ihlal edebilecek nitelikte ve bu nedenle özel ve ayrıcalıklı

[7] Çiğdem Ayözger Öngün, Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, İstanbul, Beta Yayınları, Genişletilmiş 2. Baskı, İstanbul, 2019, s.6.

[8] Hüseyin Can Aksoy, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 1. Baskı, Ankara, Çakmak Yayınevi, 2010, s.1.

olarak korunmaları zaruri görülen veri türleridir. Bununla birlikte Türk hukuku da dahil olmak üzere kişisel verilerin korunmasına ilişkin uluslararası hukuk düzenlemelerinin pek çoğunda özel nitelikli kişisel verilerin doğrudan bir tanımı yapılmamış ve yalnızca hangi verilerin bu kapsama gireceği sayma yöntemiyle tespit edilmiştir[9].

Özel nitelikli kişisel veriler KVKK m.6'da *"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"* şeklinde tanımlanmıştır[10]. KVKK m. 6'da yer almayan bir kişisel veri kategorisi, özel nitelikli kişisel veri olarak kabul edilmez. Çeşitli bilgilerin ancak belirli şartlar altında özel nitelikli kişisel veri olabildiği görülmektedir. Örneğin kişinin deniz aşırı bir seyahatte ya da uçakta seçtiği yemek, bu kişinin dini inancı hakkında da fikir veriyorsa, bu bilginin de özel nitelikli veri olduğunun kabulü gerekmektedir[11]. KVKK uyarınca özel nitelikli kişisel veriler işlenirken kural olarak ilgili kişinin açık rızasının alınması gerekmektedir. Fakat özel nitelikli kişisel verilerin işlenmesi için alınacak açık rıza konusunda KVKK'da özel nitelikli kişisel verinin türüne göre bir ayrıma gidilmiştir. Bu ayrıma göre sağlık ve cinsel hayata dair veriler haricindeki özel nitelikli kişisel veriler, kanunlarda açıkça gerekli görülen hallerde de ilgili kişinin açık rızası olmaksızın işlenebilecektir[12]. Aynı şekilde Direktif'in 8. maddesi ve Tüzük'ün 9. maddesindeki düzenlemeler de hassas verilerin işlenme şartlarını benzer bir ayrım gözeterek düzenlemektedir.

[9] Aksoy, s.30.
[10]Erbil Beytar, İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2018, s.54; Hale Akdağ, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, 1. Baskı, 2013, s.33-34.
[11]Cemil Kaya, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İÜHFM, 2011, C. 69, S. 1-2, s. 322.
[12] Özkan, s.23.

1.2. Kişisel Veri Aktarımı ve Türleri

Kişisel verilerin aktarımından önce kişisel verilerin işlenmesi kavramını anlatmak faydalı olacaktır. Kişisel verilerin işlenmesi kavramı[13], kişisel verilere dair aktarım faaliyetleri de dahil olmak üzere kişisel veriler üzerinde gerçekleştirilen bütün işlemleri kapsamaktadır[14]. KVKK m. 3/1 (e) uyarınca kişisel verilerin aktarılması da, kişisel veri işleme faaliyetleri arasında sayılmıştır. Kişisel verilerin aktarımı belirli durumlarda kişisel veri sahibinin kendi kişisel verisini üçüncü bir kişiye aktarımı ile gündeme gelebileceği gibi belirli durumlarda da veri sahibine ilişkin kişisel verilerin veri sahibi dışında başka bir kişi tarafından üçüncü kişilere aktarımı söz konusu olabilecektir. Bununla birlikte alıcı olan kişinin yurt içinde ya da yurt dışında olması da mümkündür. Buna göre aktarımın alıcısının Türkiye dışında olması halinde kişisel veri aktarımın yurt dışına yönelik gerçekleştiği kabul edecektir. Bu noktada kişisel verilerin gerek yurt içinde gerekse yurt dışında gelişi güzel aktarımının önüne geçilmesi ve aktarım faaliyetleri ile birlikte veri sahibinin kişisel verilerinin korunması gerekliliğinden doğan haklarını gözetebilmek adına kişisel veri aktarımlarının hukuka uygun bir çerçevede yürütülmesi önem taşımaktadır. KVKK m. 8/1 uyarınca kural olarak veri sahibi olan ilgili kişinin açık rızası bulunmaksızın kişisel verilerinin yurt içinde üçüncü bir kişiye aktarılamayacağı düzenlenmiştir. Bununla birlikte KVKK m. 8/1'de yer alan bu düzenlemenin istisnalarına ise aynı maddenin bir sonraki hükümleri olan 2. ve 3. fıkralarında yer verilmiştir. Bu hükümlerde düzenlenen istisnalar esasında kişisel verilerin KVKK m. 8/1'de yer alan açık rıza şartının sağlanması gerekmeksizin hukuka uygun bir veri aktarımı gerçekleştirilebilmesi için gerekli olan diğer şartları başka bir deyişle veri işleme şartları veya veri işlemenin hukuka uygunluk sebepleri hüküm altına almaktadır. Unutmadan belirtmek gerekir ki kişisel verilerin yurt içine

[13]İbrahim Korkmaz, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Seçkin Yayıncılık, Ankara, 1. Baskı, 2017, s.95.

[14] KVKK m.3/1-e: "Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (…) ifade eder".

ya da yurt dışına olduğuna bakılmaksızın aktarımı faaliyeti de bir veri işleme faaliyeti olduğundan veri aktarım faaliyetleri de ancak veri işleme şartlarından en az birini taşıdığında hukuka uygunluk kazanmaktadır.

Kişisel verilerin yurt içine aktarımının yanı sıra yurt dışına aktarılması ise KVKK m.9'da ele alınmıştır. Bu maddeye bakıldığında esasında kişisel verilerin yurt içinde aktarımının düzenlediği KVKK m.8'de belirtilen veri işleme şartlarının ötesinde daha farklı ve nitelikli düzenlemelere yer verildiği görülmektedir. Öyle ki KVKK kişisel verilerin yurt dışına aktarımını ilgili kişinin kişisel verilerinin Türkiye dışında bir alanda işlenecek olmasından hareketle ilgili kişinin haklarının bu ülkede koruma altına alınıp alınmayacağı kaygısıyla daha ciddi bir faaliyet olarak görmekte ve kişisel verilerin yurt içine ve yurt dışına aktarımının şartlarının ve yöntemlerini birbirinden farklı şekilde düzenlemektedir. Bu sebeple söz konusu aktarımların hukuka uygunluklarının incelenirken de kişisel verilerin aktarımının kişisel verilerin yurt içine ve yurt dışına aktarılması şeklinde ikili ayrıma tabi tutulması ve her bir şartın ayrı ayrı yerine getirilip getirilmediğinin irdelenmesi faydalı olacaktır[15].

Benzer bir durum AB mevzuatında da görülmekte AB kendi içinde bir ekonomik topluluk olarak üye ülkelerin kabul ettiği ve taraf oldukları Tüzük hükümleri ışığında kişisel verilerin AB üyesi ülkeler dışında üçüncü bir ülkeye aktarımını AB üyesi ülkeler arasındaki kişisel veri aktarımından farklı bir şekilde düzenlemektedir. Tüzük ile kabul edilen prensip AB üyesi ülkeler arasında serbest veri dolaşımı iken bu durum kişisel verilerin aktarıldığı AB üyesi olmayan üçüncü ülkeler için geçerli değildir ve AB üyesi olmayan ülkelere yapılacak aktarımlar sınırlandırılmış aktarım olarak tanımlanmaktadır. Kişisel verilerin AB üyesi olmayan üçüncü bir ülkeye aktarımı halinde kişisel verilerin AB tarafından kabul edilen ve Tüzük'te yer alan koruma standartlarının dışında bir alana aktarılacağı düşüncesiyle bunu sıkı şartlara bağlanmıştır. AB dışında üçüncü ülkelere ve

[15] Özkan, s.158.

uluslararası örgütlere yapılacak kişisel veri aktarımları, Tüzük'ün 40 ila 50. maddeleri arasında düzenlenmiştir. Tüzük m.45 uyarınca ancak Komisyon'un, sağlanan koruma düzeyini yeterli gördüğü ve yeterlilik kararı verdiği AB üyesi olmayan üçüncü ülkelere kişisel veri aktarımına izin verilmektedir[16]. Bu kararın varlığı AB üyesi olmayan bir üçüncü ülkeye yapılacak kişisel veri aktarımlarının temel yöntemi olarak görülmektedir ve böyle bir kararın varlığı halinde Komisyon'un bu aktarım için ayrıca bir onay vermesi aranmaz. Komisyon tarafından verilecek yeterlilik kararları daha çok aktarımın yapılacağı üçüncü ülkenin de Tüzük'ye yer alan temel veri işleme ilkelerini ve şartlarını ya da bunlara yakın standartları kabul etmiş ve uyguluyor halde olmasına bağlıdır. Bu kapsamda AB ile ABD arasında 12 Temmuz 2016'da imzalanan Gizlilik Kalkanı Anlaşması uyarınca Komisyon, ABD'nin kişisel veri aktarımı için yeterli korumayı taşıdığına karar vermiştir[17].

Bunun yanında, Tüzük m. 46 uyarınca Komisyon'un yeterlilik kararının olmadığı hallerde bile, veri kontrolörünün ya da veri işleyenin yeterli ve uygun güvenlik önlemlerini alması ve kişisel veri aktarımının yapılacağı ülkede ilgili kişilerin hakların etkili hukuki çözüm ve mekanizmalar ile korumasının sağlanacak olması şartıyla, söz konusu üçüncü ülkeye AB'den kişisel veri aktarımı yapılmasına imkân tanınmıştır. Bu kapsamda Komisyon için yeterli güvenlik tedbirlerinin alınması söz konusu kişisel aktarımı için taraflar arasında veri güvenliğinin sağlanması adına gerekli idari ve teknik tedbirlerinin alındığının bir bağlayıcı şirket kuralları hazırlaması ya da Komisyon tarafından kabul edilmiş standart veri koruma maddelerinin (SCC ya da standart sözleşme hükümleri) kabul edilmesi gibi şartlara bağlanmıştır. Bu düzenlemelerin yanı sıra Tüzük m.47'de ise çok uluslu grup şirketler arasındaki kişisel veri aktarımının hukuka uygunluğunun sağlanmasında büyük bir rol oynayan ve bu aktarımlara tabi tutulan kişisel verilerin korunması için uygun güvenlik tedbirlerinden biri olarak kabul edilen bağlayıcı şirket kurallarına

[16]Küzeci, s.180.
[17] Welcome to the Privacy Shield," The International Trade Administration (ITA)- U.S. Department of Commerce, erişim 18 Şubat, 2020, https://www.privacyshield.gov/welcome.

ilişkin ilke ve kurallar üzerinde durularak kişisel veri aktarımına ilişkin özellikli durumlara yer verilmiştir. Son olarak Tüzük kapsamında m.49 uyarınca Komisyon'un yeterlilik kararı bulunmasa ya da yeterli güvenlik tedbirleri alınmamış olsa da AB üyesi dışındaki üçüncü bir ülkeye istisnai şartların varlığı halinde de kişisel veri aktarımı yapılabileceği düzenlenmiştir. Tüzük m.49'da düzenlenen bu istisnai haller arasında açık rıza, sözleşmenin ifası, kamu yararı ve yasal talepler gibi sebepler yer almaktadır.

1.2.1. Yurt İçinde Kişisel Veri Aktarımı

Kişisel veriler, KVKK m.8/1 uyarınca yukarıda da belirttiğimiz gibi kural olarak ancak ilgili kişinin açık rızası ile yurt içinde aktarıma tabi tutulabilmektedir. Buna karşılık açık rızanın bulunmadığı hallerde ise kişisel verilerin yurt içinde aktarımı ancak KVKK m.8/2'de yer alan şartların sağlanması ile mümkündür. KVKK m. 8/2 kapsamında aktarımın hukuka uygunluğu kişisel verinin niteliğine göre iki halde düzenlenmiştir. Bunlardan ilki KVKK m.8/2 (a) uyarınca, KVKK m. 5/2'de[18] yer alan veri işleme şartlarından en birinin bulunmasıdır; bu durumda açık rıza aranmaksızın kişisel veriler yurt içinde aktarılabilecektir. Bununla birlikte özel nitelikli bir kişisel verinin yurt içinde aktarımı ise ancak yeterli güvenlik tedbirlerinin alınması kaydıyla KVKK m.6/3'de[19] yer alan şartlardan en az birinin sağlanması ile hukuka uygun kabul edilecektir. Bu noktada veri işlemenin hukuka

[18] KVKK m.5/2: "Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması".

[19] KVKK m.6/3: "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir".

uygun şartları olarak da bilinen ve KVKK m.5'te düzenlenen açık rıza dışındaki diğer veri işleme şartlarından da bahsetmek faydalı olacaktır. KVKK m.5/2 uyarınca (a) kanunlarda açıkça öngörülmesi, (b) fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, (c) bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, (ç) veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, (d) ilgili kişinin kendisi tarafından alenileştirilmiş olması, (e) bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ya da (f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde kişisel verilerin işlenmesi için aranan hukuka uygunluk şartı yerine getirilmiş olur. Genel nitelikli kişisel verilerin işlenmesinin yanı sıra KVKK m.6/3 uyarınca sağlık ve cinsel hayat verileri dışındaki özel nitelikli verilerin Kurul'un öngördüğü idari ve teknik tedbirlerin alınması şartıyla kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği ve sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği kabul edilmiştir. Bu şartlar kişisel veri işlemenin özel bir görünümü olan kişisel veri aktarımı halinde de uygulama alanı bulmaktadır. Sonuç olarak belirtmek gerekir ki kişisel verilerin KVKK m.5 ve m.6'da düzenlenen işlenme şartları ile KVKK m.8'de yer alan yurt içinde aktarımı şartları birbiriyle paralellik göstermektedir[20].

Uygulamada KVKK m.8 kapsamında hangi hallerin kişisel veri aktarımı sayılacağı hususunda çeşitli sorunlar yaşandığı görülmektedir. Öyle ki veri sorumlusu tüzel

[20] Özkan, s.158.

kişinin kendi organları arasında yaptığı kişisel veri aktarımları, KVKK kapsamında herhangi bir kişisel veri aktarımı faaliyeti olarak kabul edilmemektedir. Ancak kişisel veri aktarımı bir üçüncü kişiye, başka bir ifadeyle, aktarımda bulunacak farklı bir gerçek ya da tüzel kişiye yönelik gerçekleştirilirse, ancak bu durumda KVKK kapsamında bir kişisel veri aktarımından bahsedilebilecektir. Bu noktada örneğin şirketin yönetim kurulunun genel kurulu toplantıya çağırması ya da şirket esas sözleşmesinin tadili için öneride bulunması veya süresi dolan yönetim kurulu üyelerinin yeni dönem için tekrar seçimi için bilgi aktarımında bulunulması gibi iki organ arasında gerçekleşebilecek kişisel veri aktarımları KVKK kapsamındaki kişisel veri aktarımı olarak değerlendirilemeyecektir. Buna karşılık uygulamada kişisel veri aktarımına ilişkin belirtilebilecek özellikli durumlardan biri de TTK m. 195 ve devamı maddelerinde düzenlenen "şirketler topluluğu" bünyesindeki birden çok şirket arasında gerçekleşen kişisel veri aktarımlarıdır. Şirketler topluluğu içerisinde birden çok şirket, diğer bir deyişle birden fazla tüzel kişiliğe sahip veri sorumlusu ve veri işleyen bulunmaktadır. Bu şirketler tek bir şirketler topluluğuna bağlı olsalar ve aralarında TTK kapsamında kabul edilen bir kontrol ve bağlılık ilişkisi bulunsa da TMK kapsamında her bir grup üyesi tek başına ayrı bir tüzel kişilik teşkil ettiğinden grup şirketler arasında yapılan kişisel veri aktarımları KVKK m. 8 kapsamında kişisel veri aktarımı olarak değerlendirilebilecektir[21]. Bu nedenle Türkiye'de bulunan grup şirketler arasındaki kişisel veri aktarımlarında KVKK m. 8'deki yer alan şartlara uygun hareket edilmesi önem arz etmektedir.

Grup şirketler arasındaki kişisel veri aktarımı da kural olarak ancak aktarılan kişisel verinin ilgilisine ait açık rızanın bulunması durumunda hukuka uygun kabul edilir. Fakat bu durumda dahi Türkiye'de yer alan grup şirketler arasında gerçekleşecek kişisel aktarımları, yukarıda belirttiğimiz üzere ilgili kişinin açık rızası bulunmasa bile KVKK m. 5/2 veya 6/3'te yer alan açık rıza dışındaki veri işleme şartlarından en az birinin sağlanması ile hukuka uygun olarak gerçekleşebilecektir[22]. Öyle ki

[21]KVKK, Uygulama Rehberi, s. 89-90.
[22]Mesut Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3.Baskı, İstanbul 2020, s.121-122.

Kurul tarafından "İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması" başlıklı ilke kararında da bir şirketler topluluğu bünyesinde faaliyet gösteren birden fazla veri sorumlusu/veri işleyen şirketler arasında gerçekleştirilen kişisel veri aktarımlarının üçüncü bir kişiye yönelik yapılan kişisel veri aktarımı olarak değerlendirilmesi ve bu kapsamda aynı şirketler topluluğu içerisinde bulunan veri sorumlusu/veri işleyen şirketler arasında yapılacak kişisel veri aktarımında da KVKK m.8'de yer alan hükümlerinin esas alınması gerektiği belirtilmiş ve bu şartları temin etmeksizin aktarım gerçekleştiren şirket idari para cezasına tabi tutulmuştur[23].

Kişisel veri aktarımının özellik arz ettiği bir farklı uygulama da kişisel verilerin veri sorumlusu şirketler arasında gerçekleştirilmesinin ötesinde bir veri sorumlusu ve bir veri işleyen arasında gerçekleşmesidir[24]. Böyle bir durumda aktarımın alıcı tarafı olarak veri işleyen bir gerçek kişi ya da şirket, kendisine aktarımda bulunan veri sorumlusu bir gerçek kişi veyahut şirketin talimatları uyarınca ve onun verdiği yetkiye dayanarak kişisel veri işleme faaliyetleri gerçekleştirir. Türkiye'de bulunan bir veri sorumlusu şirketin aralarındaki hizmet sözleşmesi uyarınca onun gibi Türkiye'de bulunan başka bir şirkete veri işleyeni olarak kişisel veri aktarımında bulunması halinde yine KVKK m. 8 uyarınca yurt içine yönelik bir kişisel veri aktarımı gündeme geleceğinden KVKK m. 8'de düzenlenen şartların dikkate alınması gerekmektedir. Türkiye'de kurulu bir şirketin yine Türkiye'de sunucularını tutan bir yazılım şirketinden yıllık olarak muhasebe yazılımı hizmetleri alması halinde veri sorumlusu olarak hizmet alan şirketin ilgili yazılıma yaptığı kişisel veri girişleri ile bu yazılımın sunucularını barındıran yazılım şirketine kişisel veri aktarması veri sorumlusu ile veri işleyen arasında yapılan yurt içi kişisel veri aktarımlarına örnek gösterilebilecektir.

[23]Kurum, https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi
[24]Ayözger Öngün, s.199.

1.2.2. Yurt Dışına Kişisel Veri Aktarımı

Global düzende teknoloji ve ticaretin gelişimiyle büyük boyutlarda gerçekleşen kişisel veri aktarımları, özellikle sınır ötesi biçiminde her geçen gün daha da artmaktadır. Kişisel verilerin korunmasının bir amacı da yukarıda belirttiğimiz üzere büyük miktarlara ulaşan kişisel veri aktarımlarının kişilerin hak ve özgürlüklerine zarar vermeyecek şekilde yapılmasının sağlanmasıdır. Bu noktada bilhassa gelişen uluslararası ticarette pazarlama ve profilleme gibi amaçlarla bir araç olarak hatta belirli durumlarda doğrudan bir amaç kullanılan kişisel verilerin korunması oldukça zorlaşmaktadır. Uluslararası ticaretin gelişmesiyle birlikte şirketlerin yeni pazarlara girme, bu pazarlardaki tüketici alışkanlıklarını en iyi şekilde anlayarak yüksek oranda karlılık gütme çabası gündeme gelmekte ve bu faaliyetlerin kişisel verilerin korunmasının adeta bir hak olduğunun göz ardı edilmesi ve gelişi güzel kişisel veri aktarımı faaliyetlerinin artması şeklinde farklı birçok kişisel veri sorunlarına yol açtığı görülmektedir. Bir temel hak problematiği olarak da ele alınabilecek bu sorunların çözüme kavuşturulması için ise sınır ötesi kişisel veri aktarımlarının belirli yasal düzenlemeler içerisinde gerçekleştirilmesinin sağlanması büyük önem arz ülkeler için bir pozitif yükümlülük teşkil etmektedir. Öyle ki AB'nin kuruluş amacının temel yapı taşını teşkil eden 7 Şubat 1992'de imzalanan Maastricht Anlaşması ile AB üyesi ülkeler arasında kişi, mal, hizmet ve sermayenin serbest şekilde dolaşımı fikri kabul edilmiş, bu dört amacın yerine getirilmesinde, kişisel verilerin üye ülkeler arasında aktarımının ve işlenmesinin de bir zorunluluk olduğu ifade edilmiştir[25].

Diğer taraftan kişisel verilerin aktarılacağı ülkelerin aktarımın kurallarını belirleyen yeterli mevzuat hükümlerine sahip olmaması kadar birbirleriyle uyumlu olmayan ve uygulaması oldukça sıkı şartlar içeren düzenlemeler kabul etmesi de bu aktarımların hukuka uygunluklarının sağlanmasında büyük bir engel teşkil etmektedir. Öyle ki AB üyesi ülkelerin kişisel verilerin korunmasına dair hukuki

[25]Nilgün Başalp, Kişisel Verilerin Korunması Ve Saklanması, Ankara, Yetkin Yayınları, 2004, s.25.

düzenlemelerinin birbirinden farklılık arz etmesi Direktif ve Tüzük öncesi dönemlerde kişisel veri aktarımlarında belirli sıkıntıları beraberinde getirmekteydi. Bunun yanında AB üyesi olmayan üçüncü ülkelere yapılacak aktarımlar da kişisel verilerin sahibi ilgili kişilerin haklarının korunması açısından büyük bir sorun oluşturmaktadır. Örneğin merkezi AB'de bulunan ancak AB üyesi olmayan üçüncü ülkelerde de kurduğu bağlı şirketler ile ticari faaliyetlerini yürüten çok uluslu grup şirketlerin bu ülkelere AB'den kişisel veri aktarımı halinde grup üyesi şirketler bakımından kişisel verilerin AB dışına aktarılması ve bu aktarımın tabi olacağı kurallar hususunda belirsizlikler bulunuyordu. Yurt dışına aktarıma bağlı bu tür sorunların her biri karşısında hem kişisel veri sahibi olan ilgili kişilerin haklarını korurken hem de aynı zamanda uluslararası ticarete engel teşkil etmeyecek şekilde söz konusu kişisel verilerin serbest ya da sınırlandırılmış dahi olsa belirli şartlar altında aktarımımın mümkün olduğu şekilde dolaşımını sağlayan bir mevzuat düzenlemesine ihtiyaç duyulmuştur. Bunun üzerine AB'nin kişisel verilere ilişkin ilk hukuki düzenlemesi olan 25 Ekim 1998 tarihli Direktif yürürlüğe girmiş ve Direktif m.1 uyarınca kişisel verilerin işlenmesinde mahremiyetin sağlanması ve gerçek kişilerin hak ve hürriyetlerin korunmasının amaçlandığı, ancak aynı zamanda kişisel verilerin AB içinde serbestçe dolaşımının amaçladığı da açıkça ifade edilmiştir. Öyle ki Avrupa Parlamentosu ve Avrupa Konseyi tarafından kabul edilen bu Direktif'te görüldüğü üzere hem kişisel verilerin hukuka aykırı işlenmesi engellemeye çalışılırken hem de serbest şekilde veri dolaşımı temin edilerek gerçek kişilerin menfaatleri ile veri işleme faaliyeti gerçekleştiren gerçek kişi ve şirketlerin ticari faaliyetleri ile güttükleri menfaatleri arasında makul bir denge oluşturulmaya çalışılmıştır[26]. Şirketler arasındaki uluslararası ticaret faaliyetleri ile ülkeler arasındaki ekonomik ilişkiler nedeniyle, kişisel verilerin yurt dışına aktarımının tamamıyla yasaklanması olanaklı değildir[27].

[26]Turan, s.41; TBMM 117 sayılı Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, bkz., https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, (TBMM Komisyon Raporu), s.6, Erişim Tarihi:28.11.2021.
[27]Küzeci, s.357.

AB büyük ve önemli bir ekonomik pazar olduğundan, kişisel verilerin korunması hukuku mevzuatı hem AB içinde yerleşik gerçek kişi vatandaşlar ile AB'de kurulu şirketler hem de AB sınırları dışında kurulu olsa da AB'de faaliyet gösteren gerçek kişi ve şirketler açısından önemli bir düzenleme niteliğindedir[28]. Diğer taraftan AB'deki kişisel verilerin aktarımına ilişkin bu düzenlemeler AB üyesi olmayan pek çok üçüncü ülke için de AB ile yürüttüğü ticari, ekonomik ve siyasi ilişkilerinin hukuka uygun bir şekilde sürekliliğinin sağlanması sebebiyle AB mevzuatına uyum sağlamak suretiyle kendi ülkelerindeki hukuki düzenlemelerin kabul edilmesinde de büyük etkisi olmuştur ve öncü rolünü oynamıştır[29]. Bu kapsamda Türkiye de dahil olmak üzere AB'nin kişisel verileri koruma hukukuna dair mevzuatını dikkate alma yoluna gitmiştir.

Kişisel verilerin aktarıldığı bir ülkede kişisel verilerin korunması, işlenmesi ve aktarılmasına dair belirli şartların düzenlenmiş olduğu yasal mevzuat hükümlerinin bulunsa bile kişisel verilerin alıcı olan kişinin bulunduğu ülkede kişisel verilere sağlanacak fiili koruma ve uygulama yeterli olmayabilir ve bu yetersizlik, kişilerin kişisel verilerinin korunmasına ve gizliliğinin sağlanmasına dair temel hak ve özgürlüklerinin ağır ihlallerine yol açabilir. Bu sebeple, yurt dışına kişisel verilerin aktarımında gerek uluslararası gerekse ulusal mevzuatlarda aktarıma tabi tutulacak kişisel verinin niteliğinin ve aktarımın amacının yanı sıra aktarımın yapılacağı ülkenin kişisel veri mevzuatına ve bu mevzuatın etkinliğine ilişkin belirli özel şartlara ve hükümlere yer verildiği görülmektedir. Türk kanun koyucu da bu kapsamda KVKK'da kişisel verilerin yurt dışına aktarılmasını yurt içine aktarımdan ayrı tutarak yurt dışına aktarıma ilişkin özellikli düzenlemeler getirmiştir. Yukarıda da belirttiğimiz gibi tıpkı yurt içine aktarımlarda olduğu gibi ilgili kişinin açık rızası, kural olarak yurt dışına kişisel veri aktarımlarında bir hukuka uygunluk sebebi olarak kabul edilmektedir[30]. Öyle ki KVKK m.9/1'de ilgili kişinin açık rızası olmaksızın kişisel verilerin yurt dışına aktarılamayacağı düzenlenmiştir. Bunun

[28]Akgül, s.198.
[29]Turan, s.39
[30]Sinem Göçmen Uyarer, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Seçkin Yayıncılık, Ankara, 2019, s.137.

yanı sıra, yurt dışına kişisel veri aktarımında ilgili kişinin açık rızasının aranmadığı haller de bulunmaktadır; bu istisnai haller KVKK m.9/2'de düzenlenmiştir[31]. Kişisel verilerin yurt içi aktarımında ilgili kişinin açık rızasının aranmadığı durumlarda olduğu gibi yurt dışı aktarımının söz konusu olduğu durumlarda da KVKK m.5/2 ve 6/3 maddelerine atıf yapılsa da bu şartlardan birinin tek başına bulunması yeterli görülmemiştir. Bu maddelerde yer alan şartlara ek olarak ilgili kişinin açık rızasının aranmadığı hallerde kişisel verilerin hukuka uygun bir şekilde yurt dışına aktarılabilmesi için KVKK m.9/2'de ikili bir ayrıma gidilerek KVKK m.5/2 ve 6/3'deki veri işleme şartlarından en az biri bulunsa da kişisel verinin aktarılacağı ülkede *"yeterli koruma"*nın olup olmadığına bakılması gerektiği hüküm altına alınmıştır[32].

Öte yandan yurt dışına kişisel veri aktarılmasına ilişkin olarak ulusal mevzuat hükümlerinin yanı sıra ülkeler arasında akdedilen uluslararası anlaşmaların da göz önünde bulundurulması gerektiği unutulmamalıdır. Anayasa'nın 90. maddesi uyarınca uluslararası anlaşmaların kabul edilmesi ile birlikte bu anlaşma hükümleri de ilgili ülke hukukunun mevzuatına dahil olduğundan tıpkı KVKK uyarınca hükümleri uyarınca bu anlaşma hükümlerine de itibar edilmesi gerekmektedir. Kurum tarafından yurt dışına kişisel veri aktarımına ilişkin yayımlanan rehberde de Kurul'un yurt dışına kişisel veri aktarımının hukuka uygunluğunu değerlendirirken öncelikle Türkiye'nin aktarımın gerçekleşeceği ülke ile taraf olduğu herhangi bir uluslararası anlaşmanın olup olmadığına baktığı anlaşılmaktadır[33]. Özellikle söz konusu uluslararası anlaşma hükümlerinin KVKK gibi iç hukuk düzenlemeleri ile çeliştiğinin tespit edilmesi halinde uluslararası anlaşmanın ayrık düzenlemeleri uygulama alanı bulacağından Türkiye'nin taraf olduğu ve iç hukukuna kabul ettiğim uluslararası anlaşmalar da kişisel veri aktarımlarında büyük bir öneme sahip olduğu görülmektedir.

---

[31]Nafiye Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İÜHFM, 2017, C. 75, S. 2, s. 774.

[32] Özkan, s.161.

[33] "Kişisel Verilerin Yurtdışına Aktarılması," Kişisel Verileri Koruma Kurumu, erişim 12 Ocak 2020,https://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20YURTDIŞINA%20AKTARILMASI.pdf.

1.2.2.1. Yeterli Korumanın Bulunduğu Ülkelere Aktarım

Yeterli korumanın bulunduğu ülkeler, kişisel verilerin korunması mevzuatına ve bu mevzuatın etkili bir uygulamasına sahip olan ve genel kabul olarak kişisel verilerin korunması hakkına saygı duyan ülkelerdir. Bu nedenle bu ülkelere kişisel veri aktarımında aktarımda bulunan ve/veya aktarımın alıcı olan taraftan ek şartlar ve/veya taahhütler talep edilmesine gerek duyulmamaktadır. KVKK m. 9/2 uyarınca, KVKK 5/2 ve 6/3'de yer alan veri işleme şartlarından en az birinin ve kişisel veri aktarımının yapılacağı yabancı ülkede yeterli korumanın bulunması halinde kişisel veriler, ilgili kişinin açık rızası aranmaksızın yurt dışına hukuka uygun bir şekilde aktarılabilmektedir. KVKK m. 9/3 uyarınca Kurul'un yeterli korumanın bulunduğu ülkeleri belirleyeceği ve ilan edeceği düzenlenmekte ve bu hüküm yeterli korumanın bulunduğu ülkelerin tespiti yetkisini Kurul'a vermiştir. Ancak şu ana kadar Kurul'un bu yönde bir ilanı yapmadığı görülmektedir. Doktrinde Kurul'ca güvenli ülkeler listesi ilan edilinceye kadar bütün ülkelerin güvenli olmayan ülke şeklinde kabul edilmesi ve yeterli korumanın bulunduğu değerlendirmesi ile bu şarta dayanılarak yapılacak kişisel veri aktarımlarının hukuka aykırı veri aktarımı teşkil edeceği ifade edilmektedir[34]. Fakat bilhassa AB üye ülkelerinin uymak zorunda olduğu Tüzük ve kişisel verilerin korunmasına dair bu ülkelerin taraf olduğu uluslararası anlaşmalar ve standartlar ile ABAD tarafından kişisel verilerin korunması alanında verilen kararların mahiyeti ile Türkiye'nin de Tüzük'ün yürürlüğünden önce AB'de uygulanan Direktif hükümleri ışığında KVKK'yı kabul etmiş olduğu göz önünde bulundurulduğunda AB üye ülkelerinin kişisel veri aktarımı düzenlemeleri ile uygulamalarının kişisel verilerin korunması anlamında yeterli güvenlikte görülebileceği ve bu ülkelerin aktarılan kişisel veriler için yeterli korumayı sağlayabileceği kanısındayız.

Öte yandan Kurul, KVKK m. 9/4 uyarınca yabancı bir ülkede yeterli koruma olup olmadığının belirlenmesinde; Türkiye'nin taraf olduğu uluslararası sözleşmeleri,

[34] Özkan, s.162.

karşılıklılık ilkesini, kişisel verinin özelliği ile kişisel verinin işlenme amaç ve süresini, aktarımın yapılacağı ülkenin mevzuatı ve uygulamalarını, aktarılacak ülkedeki veri sorumlusunca taahhüt edilen önlemleri göz önüne almaktadır. Kurul, anılan bu hükümde gösterilen kriterleri daha da genişleten bir form ilan etmiş ve bu hükme ilaveten bazı ek kriterler de getirmiştir[35]. Kurul'un 02/05/2019 tarihli ve 2019/125 sayılı kararında belirttiği bu kriterlerden başlıcaları kişisel verinin aktarımının yapılacağı ülkede bağımsız bir veri koruma otoritesinin bulunması, ilgili ülkenin Türkiye ile yürüttüğü ticari faaliyetlerin hacmi ve bu ülkenin veri koruma aktarım konusunda üye olduğu kuruluşlardır.

1.2.2.2. Yeterli Korumanın Bulunmadığı Ülkelere Aktarım

Yeterli korumanın bulunmadığı ülkeler, kişisel verilerin korunması açısından yeterli hukuki düzenlemelerin ve/veya uygulamanın ve/veya bağımsız bir denetim makamının ya da bu elementlerden en az birinin bulunmadığı ülkelerdir. Öyle ki yeterli korumanın bulunduğu ülkeler için yapılacak yeterlilik değerlendirmesinin yalnızca kişisel verilerin korunması ve buna bağlı hususlar için yapıldığını unutmamak gerekir. Yeterli korumanın bulunmadığı ülkelere kural olarak kişisel veri aktarımı yapılması yasak değildir, ancak bu ülkelere yönelik yapılacak kişisel veri aktarımlarında yukarıda belirttiğimiz veri aktarım şartlarına ek koruma önlemlerinin alınması gerekmektedir. Kurul tarafından şimdiye kadar yeterli korumanın bulunduğu ülkeler ilan edilmediği için kişisel veri aktarımının yapılacağı yabancı ülkelerin tamamı yeterli korumayı sağlamayan ve güvenli olmayan ülkeler olarak kabul edilmektedir. Kişisel verilerin yurt dışına aktarımı için ilgili kişinin KVKK'ya uygun olarak alınmış açık rızasının bulunması halinde, ilgili ülkenin yeterli korumaya sahip olup olmadığına bakılmaksızın kişisel veri aktarımında bulunulabileceğini belirtmiştik. Ancak doktrinde, ilgili kişinin açık rızasının bulunması halinde kişisel veri aktarımı yapılacak ülkenin, yeterli koruma

[35]Kurul Kararı, 02.05.2019 T., 2019/125 K. https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-formhakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari, Erişim Tarihi: 30.11.2021.

sağlamayan bir ülke olsa dahi, kişisel verinin yurt dışına hukuka uygun bir şekilde aktarılabileceği belirtilmesine rağmen[36] kanaatimizce aktarılacak ülkenin yeterli bir korumaya sahip olmadığı ve açık rıza alınırken ilgili kişiye bu hususun bildirilmediği durumlarda yurt dışına yönelik yapılacak kişisel veri aktarımının hukuka uygun olduğunu belirtmek zor olacaktır.

Öte yandan ilgili kişinin açık rızasının bulunmadığı durumlarda da yeterli korumanın bulunmadığı ülkelere kişisel veri aktarımları yapılması mümkündür. Bunun için KVKK m.9/2 (b) uyarınca öngörülen taahhüt ve Kurul izni şartının yerine getirilmesi gerekmektedir. Ancak bu durumda dahi aktarımın yapılacağı ülke yeterli korumanın bulunmadığı bir ülke ise m.5/2 ve 6/3'teki veri işleme şartlarından en az birinin bulunması gerekmektedir. KVKK m.9/2 (b) gereğince yeterli korumanın bulunmaması durumunda Türkiye'deki ve atarımın yapılacağı yabancı ülkedeki veri sorumluları tarafından aktarıma tabi tutulacak kişisel verilerin aktarım esnasında ve aktarım sonrasında yeterli korumayı taşıyacak olduklarının yazılı biçimde taahhüt edilmesi ve bu kapsamda hazırlanan taahhütnamenin Kurul'un onayına sunulması gerekmektedir[37]. Kurul, yeterli korumanın bulunmadığı ülkelere yönelik yapılacak kişisel veri aktarımında Türkiye'deki veri sorumlularınca hazırlanacak taahhütnamede yer alması gerekli olan asgari unsurları tespit ederek kendi internet sitesinde yayımlamıştır[38]. Bu taahhütname düzenlenirken Kurul'un belirttiği hususlara riayet edilmesi Kurul'un yurt dışına aktarım için izni vermesi açısından büyük önem taşımaktadır. Bununla birlikte Kurul, internet sitesinde yayımladığı başka bir duyurusunda ise bu taahhütnamelerin *"çok uluslu şirket toplulukları"* bakımından yetersiz olabileceğini ifade ederek Türkiye dışındaki yabancı bir ülkede grup şirketi bulunan şirket topluluklarının kendi aralarında yapacakları kişisel veri aktarımları ile yurt

[36] Özkan, s.164; Muhammet Aydın, Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu ve Yargısal Denetimi, Yayımlanmamış Yüksek Lisans Tezi, Ufuk Üniversitesi, Ankara, 2020, s.17.
[37] Kişisel Verileri Koruma Kurulu, 6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, Yayın No: 31, Ankara 2020, s.34 (Doğru Bilinen Yanlışlar).
[38] Kurul, 16.05.2018 T., https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar, Erişim Tarihi.: 01.12.2021.

dışına aktaracakları kişisel verilerin korunmasına ilişkin bu şirketler tarafından hazırlanarak taraf olunacak *"Bağlayıcı Şirket Kuralları"*nı yayımlamıştır[39]. Bağlayıcı şirket kuralları da söz konusu yurt dışına kişisel veri aktarımı için hazırlanacak taahhütnamelerden biri olup yine hazırlanması sonrasında kişisel veri aktarımına taraf olacak grup üyesi şirketler tarafından imzalanmalı ve Kurul'un onayına sunulmalıdır. Taahhütnamelerin ve bağlayıcı şirket kurallarının içeriklerine ve bu metinlere ilişkin ulusal ve uluslararası mevzuat hükümlerinde yer verilen düzenlemelere çalışmamızın ilerleyen bölümlerinde ayrıntılı olarak yer vereceğiz.

Bununla birlikte KVKK m. 9/2 (b) uyarınca yeterli korumanın bulunmadığı bir ülkeye yapılacak kişisel veri aktarımlarında Kurul'un iznine sunulacak taahhütnamelerin Türkiye'de kurulu veri sorumlusu tarafından hazırlanması gerektiğini belirtmektedir, ancak Türkiye'de bulunan bir veri işleyen tarafından da yurt dışına kişisel veri aktarımında bulunulması gündeme gelebileceğinden bu noktada bir eksikliğin bulunduğunu söylemek yanlış olmayacaktır. Keza Kurum tarafından yayımlanan belgelerde ve yurt dışına veri aktarımına ilişkin doktrinde yer alan görüşlerde de bu konuya dair açıklık getirilmediği görülmektedir[40]. Kurum'un bu yönde bir düzenlemeye gitmemesi ve yurt dışına veri işleyen tarafından yapılacak aktarımlarda veri sorumlusu üzerinden taahhüt almayı tercih etmesinin aktarıma tabi tutulacak kişisel verilerin güvenliğinin sağlanmasından esasında KVKK ve alt mevzuat hükümleri uyarınca veri sorumlusunu sorumlu tutmak olabileceği kanısındayız. Ancak çok uluslu grup şirketler arasında yapılacak kişisel veri aktarımlarının da Türkiye'de kurulu ve veri işleyen sıfatıyla hareket eden bir grup üyesi şirketin veri sorumlusu sıfatını haiz yurt dışındaki grup üyesi şirketine kişisel veri aktarımı şeklinde gündeme gelebileceği göz önünde bulundurulduğunda Kurum tarafından KVKK m.22 uyarınca kendisine tanınan

[39] Kurul, 10.04.2020 T. https://www.kvkk.gov.tr/Icerik/6728/yurt-dısına-kısısel-verıaktarımında-baglayıcı-sırket-kuralları-hakkında-duyuru,Erişim Tarihi: 01.12.2021.
[40] İstanbul Bilgi Üniversitesi Bilgi Teknolojileri Hukuku Enstitüsü Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler Raporu, s. 12.

yetkiler ile bu alanda da ayrıntılı düzenlemelere yer vermesi ve/veya uygulamada görülen bu açıklığı gidermesi faydalı olacaktır.

Kişisel verilerin yurt dışına aktarımına ilişkin düzenlemeler arasında belirtilmesi gereken diğer bir hüküm ise KVKK m.9/5'te düzenlenen ve uluslararası sözleşme hükümlerinin saklı kalması koşuluyla, ülkemizin ya da ilgili kişinin çıkarlarının önemli ölçüde zarar göreceği durumlarda, Kurul'un izniyle kişisel verinin aktarıldığı yabancı ülkede yeterli korumanın olup olmadığına bakılmaksızın, bu verilerin yurtdışına aktarımının yapılabileceği yönündeki istisna hükmüdür[41]. Kanun koyucu tarafından yeterli ülke değerlendirmesinin yapılmasının gerekli görülmediği bu istisna hükmünün geçerli bir şekilde uygulamaya konulabilmesi için aktarımın konusuna ilişkin olarak somut olayda değişiklik gösterebilecek ilgili kamu kurumu veya kuruluşunun uygunluk görüşünün alınması ve nihai olarak da aktarım faaliyetinin Kurul'un iznine sunularak Kurul'ca onaylanmasıdır. Bu hüküm uyarınca kişisel veri aktarımının yapılacağı ülkede yeterli koruma olsa ve KVKK m.5/2 ve m.6/3'deki veri işleme şartları meydana gelse dahi Kurul'un *"ciddi anlamda menfaat ihlali"* gerçekleşebilecek olması gerekçesiyle söz konusu hüküm uyarınca kişisel verilerin yurt dışına aktarımını yasaklama ya da aktarımın yapılacağı ülkenin yeterli korumaya sahip olmamasına rağmen gerekli diğer ek şartlar sağlanmamış olsa dahi bu aktarıma onay verme yetkisi bulunmaktadır. Doktrinde, bu maddede yer alan *Türkiye'nin ya da ilgili kişinin çıkarının ciddi bir şekilde zarar göreceği* ifadesi, belirsiz bir ifade olduğu belirtilerek kanımızca haklı olarak eleştirilmektedir[42]. Öyle ki böyle bir durumda, ilgili kişinin menfaatlerinin ciddi bir biçimde zarar göreceği veri aktarım faaliyetlerine Kurul tarafından izin verilmemesi ve gereğine uygun bir şekilde aydınlatılan ilgili kişiden açık rıza alınması yoluna gidilmesi hukuki açıdan daha isabetli görünmektedir. Çünkü menfaati önemli ölçüde zarar görecek ilgili kişinin, bu konuda tek karar mekanizması olarak belirlenmesi kanımızca KVKK'nın gerekçesi ve amacı ile daha uyumlu olacaktır. Diğer taraftan bu hükmün uygulama alanının Türkiye'nin taraf

[41] Özkan, s.166.
[42]Küzeci, s. 356-357.

olduğu uluslararası sözleşmeler ile sınırlanması kişisel veri aktarımlarının bu hususların düzenlendiği uluslararası düzenlemeler ile standartlara aykırılık teşkil etmemesi açısından isabetli görünmektedir. Aynı maddenin bir sonraki fıkrası KVKK m. 9/6 uyarınca kişisel verilerin yurt dışına aktarımına ilişkin uluslararası sözleşmeler ve KVKK hükümleri dışında diğer kanun hükümlerinin de saklı olduğu belirtilmiştir. Ancak bu hüküm ile diğer kanunlar ile KVKK arasında bir genel kanun-özel kanun ilişkisi ile mi aktarımın değerlendirileceği konusu pek açık olmamakla birlikte doktrindeki ağırlıklı görüş bu hususta tıpkı uluslararası anlaşma hükümleri olduğu gibi KVKK'nın kişisel verilerin yurt dışına aktarımına ilişkin hükümlerinin diğer kanunlar ile çatışması halinde diğer kanun hükümlerinin uygulama bulacağını belirtmektedir[43].

1.3. Kişisel Veri Aktarımına Dair Pozitif Hukuk Düzenlemeleri

Çok uluslu grup şirketler arasındaki kişisel veri aktarımları AB, Türkiye ve ABD mevzuatları kapsamında çeşitli düzenlemeler altında hukuki bir zemine oturtulmaya çalışılmıştır. Bu mevzuat hükümleri çoğu zaman aktarımların birbirleriyle bağlantılı olarak söz konusu ülkeler arasında gerçekleşmesinden hareketle karşılıklı bir mutabakat ve uyum içerisinde hazırlanmıştır. Özellikle Türk Hukuku'nda kişisel verilerin korunması mevzuatı hazırlanırken büyük oranda Tüzük öncesi dönemde AB hukukunda yürürlükte olan Direktif hükümlerinden faydalanılmıştır[44]. Her ne kadar 28 Mayıs 2018 tarihinden itibaren AB'de aynı konuda Tüzük hükümleri yürürlüğe girmiş olsa da KVKK ve alt mevzuat hükümlerinin temelinde yine AB mevzuatındaki mekanizmaların yattığını söylemek yanlış olmayacaktır. Bununla birlikte global şirketlerin merkezlerinin pek çoğunun AB veya ABD'de bulunmasından kaynaklı olarak AB ve ABD arasındaki kişisel veri aktarımlarının kolaylaştırılması adına her iki ülke mevzuatının da

[43]İstanbul Bilgi Üniversitesi Bilgi Teknolojileri Hukuku Enstitüsü Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler Raporu, s. 8

[44] Kişisel Verileri Koruma Korumu (KVKK), ''Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler'', https:/ / www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası -ve-Ulusal-Duzenlemeler, 10.01.2022, s.6.

birbiriyle uyumlu bir şekilde düzenlenmesine gayret edilmiştir. Bu kapsamda kişisel veri aktarımlarına ilişkin hükümlerin AB ve ABD'nin taraf olacağı uluslararası anlaşmalarla yürütüleceği kararlaştırılmıştır. Bu durum AB'nin ABD'ye yönelik gerçekleşecek kişisel veri aktarımlarında Tüzük'te yer alan sıkı şartların uygulanması zorunluluğunu bir nebze olsun azaltmayı başarmıştır. Diğer taraftan her iki ülke arasındaki temel mevzuat farklılıklarının temel hak ve özgürlükler üzerinde doğurduğu etkiler üzere akdedilen uluslararası anlaşmaların ABD tarafından tam olarak yerine getirilmediği fikri sürekli bir tartışma halinde olmuş, hatta bu durum çeşitli veri ihlal kararıyla birlikte uluslararası yargı makamlarının incelemelerine konu olmuştur.

Çalışmamızın bu bölümünde bu ülkelerin mevzuatlarında yer verilen ve çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına ilişkin kabul edilen yasal düzenlemeler genel hatlarıyla ele alınacak ve sırasıyla AB, Türkiye ve ABD mevzuatlarında konunun ne şekilde ele alındığı karşılaştırmalı olarak anlatılmaya çalışılacaktır. Bununla birlikte Çalışmamızın ana konusunu oluşturan ve çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının hedef alınarak bu alanda detaylı hükümlerin düzenlendiği bağlayıcı şirket kuralları ve bu kurallara ilişkin ayrıntılı açıklamalara asıl olarak Çalışmamızın üçüncü bölümünde yer verilecektir.

1.3.1. AB'de Kişisel Veri Aktarımları

AB tarafından kabul edilen 2016/679 sayılı Tüzük ile birlikte 108 sayılı Sözleşme AB içerisinde yer alan kişilerin temel hak ve özgürlüklerini düzenleyen ve kişisel verilerin işlenmesine, aktarımına ve korunmasına dair ayrıntılı hükümler içeren başlıca yasal düzenlemeler arasındadır[45]. Bu düzenlemeler dışında AB'nin üçüncü ülkeler ile taraf olduğu uluslararası anlaşmalar ve her bir AB üye ülkesi tarafından kendi ülkeleri dahilinde yürürlüğe konulan iç hukuk kuralları da kişisel verilerin korunması alanında AB'de ve ilgili AB üyesi ülkede yer alan kişilerin kişisel

[45] Küzeci, Kişisel Veriler, s.24 vd.

verilerinin işlenme ve aktarım faaliyetlerinde uygulama alanı bulmaktadır. 108 sayılı Sözleşme'nin kişisel verilerin korunmasına dair uluslararası seviyede bağlayıcılık gösteren tek anlaşma olma özelliği bulunmaktadır. Bu sebeple 108 sayılı Sözleşme'de doğrudan çok uluslu grup şirketlerin kişisel veri aktarımlarına ilişkin ayrıntılı düzenlemelere yer verilmese de Tüzük ile amaçlanan veri koruma düzeyini tesis etmek adına 108 sayılı Sözleşme'nin önemli düzenlemeler içerdiğini göz önünde bulundurduğumuzda 108 sayılı Sözleşme'den de kısaca bahsedilmesi faydalı olacaktır.

Türkiye'nin ve tüm AB üyelerinin taraf olduğu 108 sayılı Sözleşme, Avrupa Konseyi tarafından 1970'li yılların başından itibaren yürütülen çalışmaların bir sonucu olarak 28 Ocak 1981 tarihinde imzaya açılmış ve 1 Ekim 1985'te kabul edilerek yürürlüğe konulmuştur[46]. Gelişen teknolojik imkanlar uyarınca veri işleme ve aktarım faaliyetlerinin daha da karmaşıklaşması karşısında ülkelerin kendi iç hukuklarında yer alan düzenlemeler uyarınca yurt dışına kişisel veri aktarımında bulunmaları, aktarıma tabi tutulan kişisel verilerin korunması hususunda yeterli koruma tedbirlerinin alınıp alınmadığı riskini de beraberinde getirdiğinden yurt dışına aktarımın uluslararası bir sözleşme ile düzenlenmesi faydalı bulunmuştur. 108 sayılı Sözleşme'nin veri aktarımlarını düzenleyen m. 12 uyarınca taraf ülkeler arasında yapılacak kişisel veri aktarımlarının yalnızca kişisel verilerin aktarıldığı ülkede yeterli korumayı bulamayacağı gerekçesiyle herhangi bir engele veya özel bir izne belirtilmektedir. Buna karşılık aktarımın gerçekleşeceği taraf ülkede aktarıma tabi tutulan kişisel veriler için iç hukuk kuralları bakımından eş değer bir veri koruma düzeninin bulunmadığı hallerde ya da taraf devletler arasından yapılacak aktarımın esasında 108 sayılı Sözleşme'ye taraf olmayan bir ülkeye yönelik gerçekleşme niyetinin bulunduğu hallerde kişisel veri aktarımına sınırlama getirilebileceği düzenlenmektedir[47]. Öyle ki 108 sayılı Sözleşme uyarınca da Tüzük

[46] Kişisel Verileri Koruma Korumu (KVKK), ''Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler'', https:/ / www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası -ve-Ulusal-Duzenlemeler, 10.01.2022, s.7.
[47] Nilgün Başalp, Kişisel Verilerin Korunması Ve Saklanması, Ankara, Yetkin Yayınları, 2004, s.34.

düzenlemeleriyle paralel olarak taraf olmayan bir ülkeye yapılacak aktarımların ancak alıcı ülkenin yeterli korumayı sağlaması halinde mümkün olduğu belirtilmiştir.

Bununla birlikte 108 sayılı Sözleşme'nin bir eki olarak kabul edilen ve Türkiye'nin de 11 Temmuz 2016 yılında onaylayarak iç hukukunda dahil ettiği 181 sayılı Ek Protokol ("Ek Protokol") ile de taraf olmayan ülkelere yapılacak aktarımlara ilişkin belirli düzenlemeler getirilmiştir. Ek Protokol uyarınca 108 sayılı Sözleşme'ye taraf olmayan ve yeterli korumayı sağlayamayan bir ülkeye yapılacak kişisel veri aktarımlarının hukuka uygun olabilmesi için söz konusu veri aktarımından sorumlu olan veri sorumlusu tarafından taahhüt edilen ve yetkili otorite tarafından taahhüt edilen bu koruma tedbirlerinin iç hukuk kurallarına göre uygun bulunması veya başta kamu menfaati olmak üzere ilgili kişinin üstün gelen meşru menfaatleri sebebiyle iç hukuk kurallarının izin vermesi gerekmektedir. Bu bakımdan 108 sayılı Sözleşme ile özellikle aktarıma tabi tutulacak kişisel veriler için ilgili grup üyesi şirket tarafından yeterli güvenlik tedbirlerinin sağlanmış olması şartının aranması, Tüzük uyarınca söz konusu grup üyesi şirketin AB üyesi olmayan üçüncü ülkelerde yer alan diğer bir grup üyesi şirkete yapacağı kişisel veri aktarımlarında da bu grup üyesi şirketin kurulduğu üçüncü ülkenin 108 sayılı Sözleşme'ye taraf olup olmadığının göz önünde bulundurulacak bir kıstas olduğunu göstermektedir. Diğer taraftan 108 sayılı Sözleşme'nin kişisel verilerin korunması adına daha üst düzey bir koruma sağlanması amacıyla güncellenerek 10 Ekim 2018 tarihinde Sözleşme 108+ olarak modernize edilmesi ve Tüzük'te düzenlenen ilgili kişiden temin edilecek rıza, ilgili kişiye tanınan yeni haklar, gizlilik ve profilleme gibi konuları da içerecek şekilde yeniden düzenlenmesiyle birlikte Tüzük ile büyük oranda uyumlu hale getirilmiştir.

1.3.1.1. Avrupa Genel Veri Koruma Tüzüğü

Mayıs 2018'de yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğü ("Tüzük") AB bünyesinde kişisel verilerin korunmasına ilişkin temel mevzuat niteliğindedir.

Tüzük çerçevesinde kişisel verilerin işlenmesine, aktarımına, saklanmasına ve korunmasına ilişkin gerek AB sınırları içerisinde faaliyet gösteren gerekse AB dışında olmasına rağmen AB'de bulunan gerçek kişilere ilişkin kişisel veri işleme faaliyetleri yürüten veri sorumluları ve veri işleyenler için önemli düzenlemeler getirilmiş ve kişisel verilerin AB dışında işlenmesi ve sınır ötesine aktarımı halinde yeterli veri koruma düzeninin sağlanamayacağı kaygısıyla ilgili kişilerin kişisel verilerine ilişkin temel haklarını koruyabilmek adına sınırlayıcı belirli hükümler öngörülmüştür. Tüzük kapsamında AB sınırları dışına veri aktarımı sınır ötesi veri aktarımı olarak tanımlanmış[48] ve Tüzük'ün m. 44 ila 50 arasında getirdiği yurt dışına veri aktarımı için sınırlandırılmış aktarım prensibini gözeterek Tüzük'e tabi olmayan ve fakat Tüzük kapsamında korunması gereken veri işleme faaliyetleri için dereceli bir sistem benimsenmiştir. Bu kapsamda örneğin Almanya'da kurulu grup üyesi bir bağlı şirketin ABD'deki hakim şirketinin sağladığı muhasebe yazılımını kullanarak bu yazılım üzerinden bağlı şirket müşterilerine ilişkin kişisel verileri ABD'deki hakim şirketine aktarması halinde söz konusu veri aktarım faaliyetinin Tüzük hükümlerine uygun olması gerekmektedir. Diğer taraftan Tüzük uyarınca Tüzük Çalışma Grubu tarafından hazırlanan rehberde transit aktarımların Tüzük uyarınca yurt dışına veri aktarımı kapsamında değerlendirilmeyeceği belirtilmiştir. Bu noktada İtalya'daki grup üyesi şirketin Macaristan'daki diğer bir grup üyesi şirkete yönelik aktaracağı kişisel verileri AB dışındaki bir ülkede yer alan sunucular aracılığıyla gerçekleştirilmesi halinde yalnızca sunucuların bulunduğu AB dışındaki ülkeden aktarıma tabi tutulan kişisel verilere erişim sağlanıyor olması Tüzük kapsamında yurt dışına aktarım olarak kabul edilmeyecektir. Ancak İtalya'daki bir grup üyesi şirketin topluluğun internet sitesi üzerinden oluşturduğu iş ilanına AB'de bulunan kişilerin başvuruda bulunması sonucu bu kişilere ait kişisel verilerin topluluğa ait internet sitesinin sunucularının bulunduğu Kanada'daki grup üyesi şirketin de erişim sağlaması halinde burada transit aktarımdan bahsedilemeyeceği için bu aktarımın Tüzük kapsamında değerlendirilmesi gerektiğini unutulmamalıdır.

[48] Paul Lambert, Understanding the New European Data Protection Rules, Taylor & Francis, 2017, s.341.

Tüzük kapsamında yurt dışına kişisel veri aktarımı için üç temel yol öngörülmüştür. Bu yolların aktarımı gerçekleştirecek veri sorumlusu ya da veri işleyen tarafından bir öncelik sırasına göre izlenmesi gerekmektedir. Bu sıralamaya göre yurt dışına kişisel veri aktarımında bulunulurken ilk olarak aktarımın gerçekleşeceği ülkenin Komisyon tarafından aktarıma tabi kişisel veriler için yeterli korumayı sağlayan bir ülke olarak kabul edilip edilmediğine bakılması gerekmektedir[49]. Şayet Komisyon'un yeterlilik kararının bulunması halinde bir sonraki mekanizmaların işletilmesine gerek olmaksızın yurt dışına kişisel veri aktarımı gerçekleştirilebilecektir. Bu noktada Komisyon, Tüzük m. 45 ve Direktif m. 25 uyarınca kişisel verilerin aktarılacağı AB üyesi olmayan üçüncü ülkelerde aktarıma tabi kişisel veriler için yeterli korumanın sağlanıp sağlanmayacağını değerlendirmek ve bu değerlendirmesi sonucunda tüm AB üyesi ülkeler için hukuken bağlayıcı olan bir karar vermektedir. Belirli durumlarda Komisyon kısmi yeterlilik kararı şeklinde de bilinen ve AB üyesi olmayan üçüncü ülkenin yalnızca belirli bölgesinin aktarılacak kişisel verilerin güvenliğinin sağlanması adına yeterli olduğuna yönelik kararlar da verebilmektedir.

Komisyon bir ülke için yeterlilik kararı verirken o ülkedeki temel veri koruma ilkelerini (verinin belirli bir amaçla sınırlı olarak ve amacıyla orantılı bir biçimde hukuka uygun, adil ve meşru bir şekilde işlenmesi, işlenen verilerin güncel ve doğru olması ve amacını aşan süreden fazla saklanmaması gibi), veri güvenliğinin sağlanabilmesi adına alınabilecek idari ve teknik tedbirleri, aktarıma tabi kişisel verilerin sahibi olan ilgili kişi için bu ülkede tanınan yasal hakları, bu ülkede kişisel verilerin korunması konusunda yetkili bir otoritenin bulunup bulunmadığı ve kişisel verilerin korunmasına ilişkin iç hukuktaki mevzuat hükümleri ile taraf olduğu uluslararası anlaşmaları gibi kriterleri göz önünde bulundurmaktadır[50]. Komisyon

[49] Doğan Yörük, AB 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü doğrultusunda kişisel verilerin korunması s.108 /Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi.

[50] AB Komisyonu üçüncü ülkelere veri aktarımında yeterlilik kararı, https://ec.europa.eu/info/law/lawtopic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Erişim Tarihi:09.12.2021.

tarafından verilen söz konusu yeterlilik kararları belirli dönemlerde Komisyon tarafından tekrar gözden geçirilebilmekte ve Komisyon'un daha önce yeterlilik kararı verdiği ülkede kişisel verilerin korunmasına ilişkin gerçekleşen değişiklikler üzerine Komisyon'un söz konusu yeterlilik kararlarını iptal etme yetkisi bulunmaktadır. Komisyon, yeterli veri koruma temin eden üçüncü ülkelerin, bu ülkelerin sektörleri veya uluslararası örgütlerinin bir listesini AB Resmî Gazetesi'nde ve internet sayfasında yayınlamaktadır (Tüzük m.45/8). 2018 yılında Andorra, Arjantin, ticari işletmeler yönünden Kanada, İsrail, Yeni Zelanda, Uruguay, İsviçre, Guernsey, Faroe Adaları ve Man Adaları hakkında geçerli yeterlilik kararları vardır[51]. Yeterlilik kararının sadece belirli bir bölgeyle ya da üçüncü ülkedeki belli bir sektörler kısıtlanması mümkündür. Bu çerçevede AB ve ABD arasında ABD kararı ile iptal edilen Safe Harbor ve Privacy Shield düzenlemeleri örnek olarak verilebilir.

Aktarımın gerçekleştirileceği ülkenin Komisyon tarafından yeterli korumanın sağlandığı bir ülke olarak açıklanmamış olması halinde aktarımı gerçekleştirecek veri sorumlusu veya veri işleyenin ikinci mekanizmaya başvurması gerekmektedir. Tüzük uyarınca hakkında yeterlilik kararı bulunmayan bir ülkeye kişisel veri aktarımının ikinci yolu aktarımı gerçekleştirecek olan veri sorumlusu veya veri işleyen tarafından aktarıma tabi tutulacak kişisel veriler için gerekli güvenlik tedbirlerinin alınmış olmasıdır. Bu tedbirler, veri aktarım sürecinin AB üyesi ülkelerdeki yetkili veri koruma otoritelerince takip edilmesi ve denetlenmesini öngörmektedir. Tüzük bu noktada aktarımın hukuka uygunluğunun sağlanabilmesi için alınabilecek güvenlik önlemlerini sıralamaktadır[52]. Bu önlemler (i) bir kamu kurum veya kuruluşu arasında oluşturulan ve yasal olarak bağlayıcı ve uygulanabilir bir mekanizmanın oluşturulması, (ii) çok uluslu grup şirketler için büyük bir kolaylık sağlayacak bağlayıcı şirket kurallarının hazırlanması, (iii)

[51]European Union Agency For Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, 2018, s.255, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, Erişim Tarihi:10.12.2021.

[52] Christopher Kuner, Transborder Data Flow and Data Privacy Law, Oxford, Oxford University Publishing, 2013, sf. 175-180.

aktarımın taraflarınca imzalanarak taraf olunacak ve Komisyon tarafından kabul edilen standart veri koruma maddeleri ya da (iv) bir denetleyici otorite tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma maddeleri, (v) AB dışındaki alıcının bağlayıcı ve uygulanabilir onaylanmış davranış kurallarını taahhüt etmesi veya (vi) AB dışındaki alıcının bağlayıcı ve uygulanabilir taahhütleri ile onaylanmış bir sertifikanın bulunması, (vii) denetleyici otorite tarafından onaylanmış sözleşme hükümleri, (viii) kamu kurum veya kuruluşları arasında yapılan ve kişisel verileri aktarılan ilgili kişilere dair uygulanabilir ve etkili haklar içeren ve AB üyesi bir ülkenin yetkili denetleyici otoritesi tarafından onaylanmış olan idari anlaşmanın bulunması şeklindedir. Aktarıma tabi tutulacak kişisel verilerin güvenliğinin ve gizliliğinin sağlanmasına yönelik Tüzük m. 46 ve m. 47 uyarınca alınacak bu tedbirlerin Tüzük uyarınca gerek kişisel veri aktarımında bulunan AB üyesi ülkedeki gerekse AB üyesi olmayan üçüncü ülkedeki veri sorumlusu ve veri işleyenlerce alınması gerekmektedir.

Aktarımın taraflarınca alınması gereken söz konusu güvenlik tedbirleri ile esasında aktarıma tabi tutulacak kişisel verilerin sahibi olan ilgili kişiler için kişisel verilerin korunmasından doğan haklarını etkili ve uygulanabilir bir şekilde kullanabilecekleri tarafları bağlayıcı ve geçerli mekanizmalar ortaya konması gerekmektedir. Güvenlik tedbirleri arasında yer alan bağlayıcı şirket kuralları özellikle çok uluslu grup şirketler arasındaki kişisel veri aktarımları için büyük bir öneme sahiptir. Bu kuralların hazırlanması ile kişisel veri aktarımının gerçekleşeceği toplulukta uygulanacak temel veri ilkeleri ve kuralları ortaya konmakta ve topluluk bünyesinde bulunan ve aktarımın tarafı olan tüm grup üyesi şirketler için geçerli olacak davranış kuralları oluşturulmaktadır. Aktarımı gerçekleştirecek olan grup üyesi şirketler tarafından hazırlanan bağlayıcı şirket kurallarının grup üyesi şirketlerden herhangi birinin kurulduğu AB üyesinde yetkili veri koruma otoritesi tarafından onaylanması gerekmektedir. Bağlayıcı şirket kuralları ile topluluk içi aktarımın konusu olan kişisel verilerin ilgili kişilerinin aktarıma ilişkin olarak gereğine uygun bir şekilde bilgilendirilmesi ve ilgili kişilere bu aktarıma bağlı olarak şikâyet hakkı ve diğer yasal hakların tanınması ile bunları

etkili bir şekilde kullanmalarına imkân tanınması beklenmektedir. Bununla birlikte bağlayıcı şirket kurallarının aktarımın tarafı olan tüm grup üyesi şirketlerce etkin bir şekilde uygulandığının belirli mekanizmalarla ispatlanabilir olması ve hesap verilebilirliğin sağlanması gerekmektedir.

Diğer taraftan Komisyon tarafından kabul edilmiş standart veri koruma maddeleri de yurt dışına veri aktarımında sıklıkla başvurulan güvenlik tedbirleri arasında yer almaktadır. Bu hükümler, başka sözleşmesel yükümlülüklerden daha önce uygulanmakta ve üçüncü ülkelerde Tüzük kapsamına göre verilerin korumasını sağlamaktadır[53]. Standart veri koruma hükümleri için, Komisyon tarafından hazırlanmış sözleşmeler veya üçüncü kişiler tarafından önerilerek Komisyonca onaylanan sözleşmeler kullanılabilir. Standart veri koruma maddeleri ile aktarımın tarafı olan veri sorumlusu veya veri işleyenler sözleşmesel bir ilişki altına girerek yapılacak veri aktarımına ilişkin belirli taahhütler altına girmektedir. Standart veri koruma maddeleri veri sorumluları arasında imzalanabileceği gibi veri sorumlusu ile veri işleyen arasında da imzalanabilmektedir, öyle ki Türk hukukundan farklı olarak Tüzük uyarınca standart veri koruma maddelerinin iki veri işleyen arasındaki aktarım özelinde de kullanılması ve tarafları veri işleyenler olarak düzenlenmesi mümkündür; ancak tarafların bu maddeleri değiştirme yetkileri bulunmamaktadır. Taraflar yalnızca aralarındaki aktarıma dayanak oluşturan ilişki uyarınca bu maddelerin amacıyla çelişmeyecek eklemelerde bulunabilirler. Söz konusu maddeler ile taraflar aktarıma tabi kişisel verilerin korunmasına ilişkin olarak Direktif'te öngörülen hükümlere bağlı karşılıklı ve ilgili kişiye yönelik belirli yükümlülükler üstlenmektedir. Öte yandan Komisyon, Direktif hükümleri uyarınca hazırlanan standart veri koruma maddelerini Tüzük'e uygun bir şekilde güncellenmesi konusunda çalışmalar yürütmektedir.

[53] Develioğlu, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017, s. 65.

Standart veri koruma sözleşmeleri, Direktif'in yürürlükte olduğu dönemden bu yana mevcuttur. Bu sözleşmeler, veri aktarımının hukuka uygun şekilde yapıldığının yetkili merciler tarafından onaylandığını göstermektedir. Standart veri koruma hükümleri, hızlı uygulanabilme ve idari aşamaların belirsizliğine son verme özelliğinden dolayı taraflara yüksek bir koruma temin etmektedir. ABAD'ın 16 Temmuz 2020 tarihinde verdiği *Schrems II* kararında, standart sözleşme hükümlerinin uygulamasına ilişkin önemli ibareler bulunmaktadır. Bu karardan sonra, standart sözleşme hükümleri içeren sözleşmeleri imzalayan taraflara, üçüncü ülkelerdeki veri koruma kurallarını araştırma sorumluluğu yüklenmiştir. Ayrıca taraflar, üçüncü ülkedeki kamu makamlarının aktarılan veriler üstündeki denetim yetkisini araştırmakla da yükümlü kılınmıştır. Yapılan inceleme neticesinde standart sözleşme hükümlerinin yerine getirilemeyeceği tespit edilirse, sözleşme feshedilmeli veya aktarım durdurulmalıdır[54]. Bununla birlikte, bu kararın AB'deki veri koruma otoritelerinin de denetim yetkisini kuvvetlendirdiği söylenebilir. AB veri koruma otoriteleri de üçüncü ülkede standart sözleşme hükümlerinin korunmadığını belirlerlerse, veri aktarımını durdurabilir ya da yasaklayabilirler[55].
Ayrıca uygulamada sıklıkla başvurulmasa da Tüzük uyarınca aktarımın taraflarının faaliyet gösterdiği sektördeki meslek birlikleri tarafından hazırlanmış ve Tüzük ile uyumlu bir veri koruma mekanizması sunduğu ilgili veri koruma otoritesi veya gerektiğinde Avrupa Veri Koruma Kurulu tarafından onaylanan mesleki davranış kuralları ile de yurt dışına aktarım gerçekleştirilebilmektedir. Davranış kuralları; veri sorumlusu veya işleyen üyeleri temsil eden sektör ya da ticari birliklerin o sektörün gereksinimlerini dikkate alarak düzenledikleri onaydan geçmiş araçları ifade etmektedir[56]. Bir davranış kuralının Tüzük'e göre uygun güvenlik tedbiri olarak kabul edilebilmesi için üç koşula sahip olması gereklidir. Bu koşullar; Tüzük m.40'da yer alan veri koruma ilkelerini taahhüt etmesi, Tüzük m.55 gereğince yetkili veri koruma otoritesi ya da AB Komisyonunca onaylanması ve hukuki bağlayıcılığının bulunmasıdır[57]. Bu kuralları hazırlayan Birlik içindeki veri

[54] C-311/18, para. 140.
[55] C-311/18, para.113, 114.
[56] Çekin, 2020, s.179.
[57] Toparlak, s.40.

sorumluları ya da işleyenler, isterlerse bunlara uymayı tam olarak taahhüt edip kendileri açısından bu kurallara hukuki bağlayıcılık kazandırabilirler. Bu özelliği nedeniyle davranış kuralları, hesap verebilirliği arttıran isteğe bağlı yürürlüğe konulan uyum araçları olarak görülmektedir. Davranış kuralları, veri aktarma da dâhil olmak üzere bütün veri işleme süreçlerini içerecek biçimde hazırlanmaktadır. Davranış kuralları, meslek odaları ya da birlikler gibi sektörel bazda düzenlendiğinden ilgili sektörün gereksinimleri kapsamında oluşturulurlar. Bu kurallar, oluşturuldukları ticari birliğin üyeleri, veri sorumluları veya işleyenleri açısından hızlı ve nispeten hesaplı bir uyum yöntemidir. Yetkili veri koruma otoritesi tarafından onaya tabi tutulduklarından bu kurallara uymayı vaat eden veri sorumluları ya da işleyenler, yetkili otorite gözünde güvenilir olarak kabul edilmektedir[58]. Bu anlamda davranış kuralları, hesap verebilirlik ve şeffaflık ilkelerinin de gerçekleşmesine katkıda bulunmaktadır. Yalnızca belirli bir ülkede uygulanacak davranış kuralları açısından o üye ülkenin veri koruma otoritesine başvuru yeterlidir. Ancak davranış kuralları AB içinde geçerli olacaksa üye ülke otoritesi, kendisine verilen davranış kurallarını Tüzük m.63 kapsamında düzenlenen uyum mekanizması çerçevesinde AB Veri Koruma Kurulu'na sunmaktadır[59]. Veri sorumlusu ya da işleyenin üye olduğu meslek odaları veya birlikler tarafından hazırlanan davranış kurallarının veri sorumlusu şirket tarafından taahhüt edilmesi birçok bakımdan yararlı görülmektedir. Ancak veri sorumlusu veya işleyenin bilhassa sürdürmeyi istediği yerleşik kuralları ya da özel bir teşkilatlanması varsa, veri aktarımı amacıyla farklı güvenlik tedbirleri dikkate alınabilecektir.

Kişisel verilerin alıcısı olan AB dışındaki şirketin yetkilendirilmiş kuruluşlara ya da gerekmesi halinde Avrupa Veri Koruma Kurulu'na başvuruda bulunması üzerine aktarıma dair yeterli ve uygun güvenlik tedbirlerini aldığına dair değerlendirme sonrası düzenlenecek sertifikalar sayesinde de Tüzük uyarınca hukuka uygun sınır

[58]Information Commissioner's Office, Guide to Codes of Conduct, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-thegeneral-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/ Erişim Tarihi: 11.12.2021.
[59] Çekin, 2020, s.179-180.

ötesi kişisel veri aktarımları gerçekleştirilebilmektedir. Sertifikalar (certificate), veri sorumlusu ya da işleyenin yaptığı faaliyetlerin Tüzük'e uyumlu olduğunu gösteren damga veya mühürlerdir. Sertifikalar; Tüzük m.42/5 gereğince AB üyesi devletlerin veri koruma otoriteleri, Tüzük m.43 gereğince yetkili sertifika kuruluşları[60] ya da Tüzük m.63 gereğince AB Veri Koruma Kurulu tarafından verilebilmektedir[61]. Üçüncü ülkelerdeki veri sorumlusu ya da işleyenlerin sertifika alması durumunda bu sertifika, AB'den bu ülkeye gerçekleştirilecek veri aktarımlarında Tüzük m.46/2-f gereğince uygun güvenlik tedbiri niteliğine sahiptir[62].

Sertifika almayı talep eden üçüncü ülkelerdeki veri sorumluları ya da işleyenlerin, yerine getirmeleri gereken dört yükümlülük bulunmaktadır[63]. Birinci olarak sertifika kıstasları, Komisyon tarafından onaylanan ve tespit edilen veri koruma ilkelerini kapsamalıdır. İkinci olarak sertifika, Tüzük'ün yetkili kıldığı bir kuruluş ya da AB Veri Koruma Kurulunca verilmelidir. Üçüncü olarak üçüncü ülkedeki veri sorumlusu veya işleyen, Tüzük'ün getirdiği yükümlülüklere ilişkin taahhüt vermelidir. Dördüncü ve son olarak ise sertifika kıstaslarının, üçüncü ülkede bulunan veri sorumlusu ya da işleyenler açısından hukuki bağlayıcılığının bulunması gerekmektedir. AB'de kurulu bir veri sorumlusu ya da işleyen için sertifikanın getirdiği en önemli fayda, olası kontrol ve denetim giderlerinin düşürülmesidir. Bununla birlikte veri sahiplerinde oluşturulan güven, pazarlama yararını da beraberinde getirebilir[64]. Üçüncü ülkelerde bulunan veri sorumluları ya da işleyenleri açısından sertifikanın getirdiği fayda daha büyüktür. AEA'dan üçüncü ülkeye gerçekleştirilecek veri aktarımları için uygun bir güvenlik tedbirinin bulunması, üçüncü ülkedeki sorumluları tercih edilebilir bir alternatif durumuna getirmektedir. Veri işleme aşamalarında maliyetleri düşürmek için dıştan hizmet

[60]Dove, s.1025.
[61]European Data Protection Seal, https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en, Erişim Tarihi: 11.12.2021.
[62]Çekin, 2020, s.181.
[63] Toparlak, s.41-42.
[64] GDPR Certification, https://www.eugdpr.institute/gdpr-certification/, Erişim Tarihi:14.07.2021.

alındığı (outsourcing) hallerde, üçüncü ülkelerdeki sorumlu ve işleyenler açısından sertifikaların ticari önemi de bulunmaktadır.

Bunlar dışında ilgili AB üyesi ülkesindeki yetkili veri koruma otoritesi tarafından onaylanan ve veri aktaran ile veri alıcısı arasında düzenlenen sözleşmeye ek veri koruma hükümleri uyarınca veyahut ilgili AB üyesi ülkenin veri koruma otoritesi veya aktarımın birden fazla AB üyesinden yapılacak olması halinde Avrupa Veri Koruma Kurulu tarafından onaylanan ve iki idari otorite arasında imzalanan mutabakat aracılığıyla da kişisel verilerin AB üyesi olmayan üçüncü bir ülkeye aktarımı yeterli güvenlik tedbirinin alındığından bahisle uygun görülebilecektir. Görüldüğü üzere üçüncü ülkelere kişisel veri aktarılması amacıyla Tüzük'te farklı güvenlik tedbirleri belirlenmiştir. Veri sorumluları ve veri işleyenler ve özellikle çok uluslu grup şirketler kendi özel durumları kapsamında gerekli değerlendirmeleri yaparak kendi ihtiyaçlarını karşılayan güvenlik tedbirlerini seçerek aktarımların hukuka uygunluklarını temin etmekle yükümlüdür.

Yeterlilik kararının bulunmadığı ve yeterli güvenlik tedbirlerinin sağlanması şartının da karşılanamadığı hallerde AEA sınırları dışındaki üçüncü bir ülkeye kişisel veri aktarımına izin verilebilmesi için bu aktarımın Tüzük m. 49 uyarınca öngörülen istisnai hallerden birine girmesi gerekmektedir. Söz konusu istisnai hallerin geçerli olabilmesi için AEA sınırları dışındaki üçüncü ülkeye kişisel veri aktarımında bulunan veri sorumlusunun gerçekleştirdiği aktarımın devamlı ve geniş kapsamlı olmaması ve Tüzük uyarınca öngörülen diğer veri işleme ve aktarım şartlarını karşılaması aranmaktadır. Bu istisnalar arasında en sıklıkla başvurulan yöntem Tüzük m. 49/1 (a) uyarınca ilgili kişiden alınacak açık rıza beyanıdır. Açık rızanın geçerli olabilmesi için bu rızanın belirli bir amaca özgü olması ve ilgili kişinin aktarıma ilişkin gereğine uygun bir şekilde bilgilendirilmiş olmalıdır[65]. Bu bilgilendirmede aktarımı gerçekleştirecek veri sorumlusu aktarıma tabi kişisel verilerin ilgili kişileri için aktarımdan doğabilecek riskleri ve beyan etmiş oldukları

[65] Yörük, s.61; Turan, s.177.

açık rızalarını herhangi bir zamanda geri alma haklarının olduğunu da ilgili kişilere bildirmelidir[66]. Ayrıca Tüzük'te rıza beyanının açıklanmasına ilişkin belli bir koşul da öngörülmemiştir. Bu nedenle açık rıza sözlü, yazılı veya elektronik vasıtalarla açıklanabilir. Diğer taraftan1 Ekim 2019 tarihinde yayımladığı Planet kararında ABAD hukuka uygun bir rıza için ilgili kişinin özgür iradesini ortaya koyan aktif bir hareketinin bulunması gerektiğini belirtmektedir[67]. Bu kapsamda çevrimiçi alışveriş sitelerinde yer alan ve önceden işaretlenmiş kutucuklar ile ilgili kişinin rıza verdiğinin kabulü de hukuka aykırı olacaktır ve açık rızanın mümkünse ilgili kişiye doğrudan boş bir kutucuğun sunulmasıyla alınması gerekmektedir. Öte yandan açık rıza, bir hizmetten yararlanma bakımından ön şart olarak düzenlenmişse özgür irade sakatlanacağından rıza geçersiz kabul edilmektedir[68].

Bununla birlikte Tüzük m. 49/1 (b) uyarınca ilgili kişi ile aktarımı gerçekleştirecek veri sorumlusu arasındaki bir sözleşmenin ifası ya da ilgili kişinin bir sözleşmenin kurulması öncesi dile getirdiği talebin yerine getirilmesi için gerekli olması halinde de ve sıklıkla gerçekleşmemesi şartıyla aktarımın sözleşmenin ifası sebebiyle yurt dışına veri aktarımında bulunulabilmektedir. Bu istisnaya dayanılabilmesi için aktarımı yapacak veri sorumlusunun sözleşme veya ilgili kişinin talebi için aktarımın hangi sebeplerle ve hangi kapsamda zorunlu olduğuna ilişkin gerekli incelemeleri yapması faydalı olacaktır. Ayrıca bu istisnanın farklı bir görünümü olan ve Tüzük m. 49/1 (c) uyarınca ilgili kişi yararına üçüncü taraf sözleşmelerinin kurulması veya ifası için gerekli olması halinde de kişisel verilerin yurt dışına aktarımı gerçekleştirilebilecektir.

Diğer taraftan Tüzük m. 49/1 (d) uyarınca aktarımı yapacak veri sorumlusunun bulunduğu AB üyesi ülkenin hukukuna veya AB hukukuna göre kamu yararının gerektirdiği durumlarda veya Tüzük m. 49/1 (e) uyarınca aktarımı gerektiren ve

[66] Çekin, 2020, s.84.
[67] C - 673/17, para.62.
[68] Tüzük, Gerekçe, m.42; Kişisel Verileri Koruma Kurulu, Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili 27/02/2020 Tarihli ve 2020/173 Sayılı Karar, https://www.kvkk.gov.tr/Icerik/6739/2020-173, Erişim Tarihi: 13.07.2021.

geçerli bir dayanağı bulunan yasal talebin varlığı halinde bu talebin yerine getirilmesi için gerekli ise de AEA sınırları dışında üçüncü ülkelere veri aktarımında bulunulması uygun bulunabilmektedir. Bununla birlikte yine Tüzük m. 49/1 (f) uyarınca ilgili kişi veya diğer kişilerin hayati menfaatlerinin korunması bakımından gerekli olması ve ilgili kişinin fiziksel veya hukuki imkansızlıklar nedeniyle rıza veremeyecek durumda olması halinde, Tüzük m. 49/1 (g) uyarınca ilgili AB üyesi ülkenin ya da AB'nin hukukuna göre kamuoyuna ya da meşru bir menfaati bulunan kişilere açık olan sicillerden kamuoyuna bilgi vermek amacıyla aktarımın yapılmasının gerekli görülmesi halinde ve Tüzük m. 49/2'de belirtilen ve veri sorumlusunun zorlayıcı meşru menfaatlerinden en az birinin bulunması ve bu aktarımın ilgili kişinin temel hak ve özgürlüklerini ciddi bir şekilde ihlal etmemesi halinde de Tüzük uyarınca AEA dışında üçüncü bir ülkeye kişisel veri aktarımında bulunabileceği kabul edilmektedir. Söz konusu aktarım için Tüzük m. 49'da düzenlenen bu istisnai durumlardan en az birinin sağlanmış olmasının yanı sıra Tüzük kapsamında düzenlenen genel veri işleme ve aktarım ilkeleri ile şartlarına da itibar edilmesi gerektiği unutulmamalıdır.

1.3.1.2. Avrupa Birliği Adalet Divanı Kararları

AB mevzuatında yer alan AB dışına kişisel verilerin aktarımına ilişkin 108 sayılı Sözleşme, Tüzük, uluslararası anlaşmalar ve iç hukuk hükümlerinin yanı sıra bu hükümlerin yorumlanmasına ilişkin ABAD kararları da AB mevzuatının ayrılmaz ve bağlayıcı parçalarından biridir[69] ve ABAD'ın AB üyesi olmayan üçüncü ülkelere kişisel veri aktarımına ilişkin uygulamaya ve mevzuat hükümlerinin yorumlanmasına yön veren önemli kararları mevcuttur. Bu kararların başında AB ile ABD arasında yapılan kişisel veri aktarımlarına ilişkin hüküm verdiği *Schrems I ve II kararları* çok uluslu grup şirketler arasındaki kişisel veri aktarımları için de önemli bir yere sahiptir. Öyle ki Schrems I ve II kararları esasında AB'de bulunan ve Facebook'a kayıtlı olan kişilerin kişisel verilerinin Facebook'un İrlanda'daki

[69] Kerim Anadolu, "Avrupa Birliği Adalet Divanı", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C.11, S.3, 2003, s.360.

grup şirketinden ABD'de bulunan diğer bir grup üyesi şirkete aktarımını konu almaktadır. Avusturya'da yaşayan ve Facebook kullanıcısı olan başvurucunun ABD'ye aktarılan kişisel verilerinin ABD'deki mevzuat hükümlerinin soruşturma ve gözetleme faaliyetleri amaçlarıyla kamu kurumlarına verdiği kişisel verilere erişim hakkının oldukça geniş bir şekilde düzenlenmesi gerekçesiyle kişisel verilerinin İrlanda'dan ABD'ye aktarımının hukuka aykırı sonuçlara yol açacağı iddiasıyla İrlanda Veri Koruma Otoritesi'ne başvuruda bulunmaktadır. İrlanda Veri Koruma Otoritesi ise Komisyon tarafından ABD'nin yeterli koruma seviyesini sağladığına ilişkin 2000/520 sayılı Güvenli Liman Kararı'nı ileri sürerek başvuruyu reddetmiştir. Bunun üzerine İrlanda Yüksek Mahkemesi'ne giden başvurucunun bu başvurusu üzerine İrlanda Yüksek Mahkemesi Güvenli Liman Kararı'nın söz konusu aktarım faaliyetlerinin hukuka uygunluğu konusunda geçerli bir gerekçe olup olmadığının incelenmesi için konuyu ADAB'a taşımıştır. ABAD 6 Ekim 2015 tarihinde verdiği karar ile başvurucuyu haklı bularak bu aktarımların hukuka uygunluklarının sağlanması konusunda yeterli koruma tedbirlerine tabi tutulmadığı gerekçesiyle Komisyon tarafından verilen dayanak Güvenli Liman Kararı'nın geçersiz olduğunu belirtmiştir[70]. ABAD'ın bu kararındaki hareket noktası Facebook grup şirketleri arasındaki aktarımların standart sözleşme maddelerine dayanılarak yapılmasına rağmen aktarılan söz konusu kişisel verilerin Avrupa Birliği Temel Haklar Bildirgesi'ne ("Bildirge") aykırı bir şekilde ABD'deki kamu kurumları tarafından gözetleme amacıyla takdiri geniş bir şekilde erişimi ve kullanılmasının kişisel verilerin hukuka aykırı olarak işlenmesi sonucuna yol açmasıdır. ABAD'ın Schrems I adı verilen bu kararı üzerine Güvenli Liman Kararı'nın geçersiz kılınmasıyla Komisyon AB ile ABD arasındaki kişisel verilerin aktarımının hukuka uygunluk dayanağını teşkil edecek Gizlilik Kalkanı Anlaşması'nı imzalamıştır. Gizlilik Kalkanı ile özellikle ABD'de bulunan kamu kurum ve kuruluşlarının yeterli gerekçeleri bulunmadıkça AB'den aktarılan kişisel verileri işlememeleri, aksi halde ilgili kişilerce kişisel verilerinin kötüye kullanıldığına dair herhangi bir şüphenin bulunması halinde ABD'deki

[70] Gülçin Gümüş, Dülger ''Schrems II Kararı ve Sonuçları'', s.2

mahkemelere başvurma hakkı gibi belirli kontrol yetkileri verilerek Güvenli Liman Kararı'nın Schrems I kararıyla tespit edilen eksiklerinin doldurulması amaçlanmıştır. Gizlilik Kalkanı Anlaşması'na Çalışmamızın 1.3.3. ABD'de Kişisel Veri Aktarımları başlığı altında yer verilecektir.

ABAD Gizlilik Kalkanı Anlaşması ile ABD'deki kamu kurum ve kuruluşlar tarafından AB'den aktarılan kişisel verilerin hukuka aykırı bir şekilde gelişi güzel kullanılmasının önüne geçilemediği gerekçesiyle 16 Temmuz 2020 tarihinde Schrems II kararı ile Gizlilik Kalkanı Anlaşmasını da geçersiz kılmıştır[71]. Schrems II kararıyla ABAD, AB ile ABD arasında kişisel veri aktarımında bulunan çok uluslu grup şirketlerce kullanılan standart sözleşme maddelerinin kullanılmasının gerekli veri koruma düzeyini sağlamakta yeterli olmadığını belirterek aktarımın tarafı olan grup şirketlerce standart sözleşme maddelerinin ötesinde gerekli tedbirlerin alınması gerekliliğine işaret etmektedir. Aksi halde ABAD, aktarım için alınan tedbirlerin aktarılan ülkedeki mevzuat hükümleri uyarınca gerçekleşen veri işleme faaliyetlerinin hukuka aykırılığını önleyememesi ve aktarılan ülkenin mevzuat hükümlerinin aktarım için alınan güvenlik tedbirlerini aktarımın taraflarına ihlal edecek yükümlülükler yüklemesi halinde söz konusu güvenlik tedbirinin yeterli kalmayacağından hareketle aktarımın durdurulması ya da yetkili veri koruma otoritesinin bu aktarımı yasaklaması gerektiğini belirtmektedir.

ABAD tarafından Schrems II kararında dayanılan gerekçede de tıpkı Schrems I'de olduğu gibi kişisel verilerinin ABD'deki kamu otoritelerince Bildirge'de[72] düzenlenen temel haklara aykırı şekilde kullanılmasıdır. Öyle ki ABAD Bildirge'de yer alan temel hak ve özgürlüklere yönelik müdahalelerin ancak kanunda öngörülmüş ve orantılı[73] olması halinde gündeme gelebileceği, ancak ABD'nin milli güvenlik gerekçesiyle istihbarat örgütlerince uygulamada benimsediği gelişi

[71]Toparlak, s.35.
[72]European Data Protection Board, Frequently Asked Questions Aboutthe Judgement C-311/18 https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf, Erişim Tarihi: 01.12.2021.
[73] AAD C-311/18, 178, 179, 180.

güzel veri işleme faaliyetleri ile kısıtlanamayacağını belirtilmektedir[74]. Schrems II kararıyla Gizlilik Kalkanı Anlaşması'nın iptal edilmesi üzerine AB'den ABD'ye yapılacak kişisel veri aktarımlarının hangi yasal düzenleme ile hukuka uygun bir zemine oturtulabileceği konusunda akıllarda soru işaretlerine sebep olmaktadır. Bu noktada çok uluslu grup şirketler arasında yapılacak kişisel veri aktarımları için bağlayıcı şirket kurallarına başvurulması değerlendirilebilecek mekanizmalar arasında yer alabilir. Bu kurallar ile özellikle Tüzük kapsamında da koruma altına alınan ve ilgili kişilere yönelik etkili ve yasal olarak uygulatılabilir hakların gözetilmesi büyük önem taşımaktadır. Görüldüğü üzere Schrems I ve II kararıyla ABAD, AEA'dan AEA sınırları dışında bulunan üçüncü ülkelere kişisel veri aktarımında taraflarca hazırlanması gereken ve bir güvenlik tedbiri yerine geçen standart veri koruma hükümlerine ilişkin önemli tespitlerde bulunmakta ve "*kişisel veri aktarımının yapıldığı ülkede yeterli veri koruma güvenlik seviyesinin bulunması*" kavramına açıklık getirmektedir[75]. ABAD'a göre yeterli güvenlik seviyesi, AEA sınırları dışındaki üçüncü ülkenin aktarılan kişisel verilerin korunmasına, güvenliğine ve gizliliğinin sağlanmasına yönelik etki taşıyan mevzuat düzenlemeleri ve aktarım için alınan güvenlik önlemlerinin veri güvenliğini ne derece sağladığıdır. Bununla birlikte ABAD kişisel verileri aktarılan ilgili kişilerin aktarılan ve işlenen kişisel verileri ile ilgili olarak kendileri tanınan ve faydalanabilecekleri haklar ile bunları etkin bir şekilde kullanmalarına imkan tanıyan mekanizmaların o ülkede bulunup bulunmadığının incelenmesi ile de yeterli korumanın varlığının tespit edilebileceğini ifade etmektedir.

Schrems kararı sonrası AEA sınırları dışındaki üçüncü ülkelere kişisel veri aktarımları için gerekli önlemlerin alınması kapsamında getirilen bir diğer mekanizma da aktarım etki değerlendirmesidir (transfer impact assessment). Yeterlilik kararının bulunmadığı ülkelere standart sözleşme hükümlerinin oluşturulması ile yapılacak aktarımların aktarımın yapıldığı ülkede de yeterli korumadan faydalanıp faydalanmayacağının tespiti için aktarım etki

[74] AAD C-311/18, 164, 165.
[75] Gülçin Gümüş, Dülger ''Schrems II Kararı ve Sonuçları'', s.1

değerlendirmeleri büyük önem arz etmektedir. Aktarım etki değerlendirmesi ile aktarımın yapılacağı alıcı ülkenin mevzuat düzenlemelerinin ve mahkemeler ile yetkili kurum ve kuruluşların uygulamalarının aktarıma tabi tutulan kişisel veriler için ne oranda koruma teşkil edebileceği analiz edilir. Bu kapsamda alıcı ülkede kişisel veri mevzuatının olup olmadığı, böyle bir mevzuat varsa bu mevzuatın ne denli ayrıntılı ve kişisel verileri tam bir şekilde korumaya yönelik olarak düzenlendiği, bu kuralların mahkeme ve diğer yetkili kurum ve kuruluşlarca etkili bir şekilde uygulanıp uygulanmadığı, kişisel veri sahiplerinin haklarını kullanma imkanları ve alıcı ülkede kişisel verilerin korunmasına dair yeterli güvenlik önlemlerinin alınıp alınmadığı incelenir. Aktarım etki değerlendirmesinde yapılan incelemelerden bir tanesi de alıcı ülkedeki yetkili kurum ve kuruluşların aktarıma tabi tutulan kişisel veriler üzerinde hangi oranda erişim ve/veya işleme yetkisinin bulunduğu ve bu erişim ve/veya işleme yetkisinin AEA sınırları içerisinde kişisel verilerin korunması için belirlenen kurallara ve sınırlamalara ne ölçüde uygun olduğudur. Yapılacak aktarım etki değerlendirmesi sonrasında alıcı ülkenin mevzuat düzenlemeleri ve uygulamasının aktarıma tabi tutulacak kişisel verilerin korunması ve gizliliğinin sağlanması için AEA standartlarına uygunluğunu tespit edilir ve bu inceleme sonrasında yeterli korumanın sağlanmadığı sonucuna varılan alıcı ülkeye kişisel verilerin aktarılmaması ya da alınabilecek ek güvenlik önlemlerinin sağlanarak kısmi ya da geçici aktarımların yapılması AEA mevzuatıyla uyumlu hareket edilmesi açısından kritik önem teşkil etmektedir.

1.3.2. Türk Hukukunda Kişisel Veri Aktarımları

1.3.2.1. Genel Olarak

Türk Hukukunda kişisel verilerin aktarımı, kişisel verilerin işlenmesi ve korunması kapsamında 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve alt mevzuat hükümlerinde düzenleme altına alınmıştır. Bir veri işleme faaliyeti olarak kişisel verilerin aktarımı yurt içi aktarım ve yurt dışı aktarımlar olarak KVKK m.8 ve m.9 uyarınca düzenlenmiştir. KVKK m.8 ve m.9'da kişisel veri aktarımının

hukuka uygunluğunun sağlanması için taşıması gereken şartlara yer verilmiştir[76]. Bu şartlar esasında KVKK m.5 ve m.6'da yer verilen kişisel verilerin işlenmesinin hukuka uygunluk şartlarıdır ve bu şartlardan en az birinin bulunması aktarımı hukuka uygun hale getirmektedir. Söz konusu veri işleme şartlarına Bununla birlikte aktarımın yurt dışına yönelik olması halinde KVKK, bu şartlara ek olarak farklı şartların da öngörmekte ve aktarımın daha güçlü veri koruma önlemleri alınarak gerçekleşmesi gerektiğini öngörmektedir. Çalışmamızın 1.2.1. Yurt İçinde Kişisel Veri Aktarımı ve 1.2.2. Yurt Dışına Kişisel Veri Aktarımı başlığı altında bu şartlara ayrıntılarıyla yer verilmiştir. Bu şartların dışında çok uluslu grup şirketler arasındaki kişisel veri aktarımlarında önemli bir yer tutan taahhütname ve bağlayıcı şirket kuralları mekanizmalarından bahsetmek faydalı olacaktır. Aktarımın hukuki bir zemine oturtulmasında büyük bir rol oynayan bu kurallar Tüzük'te yer alan yurt dışına aktarım için alınabilecek güvenlik tedbirleri arasında görülen standart sözleşme maddeleri ve bağlayıcı şirket kurallarından hareketle Türk hukukuna dahil edilmiştir. Kurum tarafından muhtelif zamanlarda yayımlanan duyurular ile birlikte uygulamaya dahil edilen bu mekanizmalar, yeterli korumanın bulunmadığı ülkelere kişisel veri aktarımında bulunacak çok uluslu grup şirketler belirli kolaylıklar getirmektedir. Kişisel verilerin yurt dışına aktarımı için ilgili kişinin açık rızasının bulunmadığı durumlarda çok uluslu grup şirketler Kurum belirtilen standartlara uyarak Kurum'un internet sitesinde yayımladığı bu taslakları kullanarak topluluk dinamiklerine uygun metinler hazırlayabilmekte ve bunları Kurul'un incelemesine sunarak alacakları onay ile birlikte hukuka uygun bir şekilde yurt dışına kişisel veri aktarımı gerçekleştirebilecektir.

Diğer taraftan KVKK dışında Türk Hukuku'nda yurt dışına kişisel veri aktarımının düzenlendiği farklı mevzuat düzenlemeleri de bulunmaktadır. 5411 sayılı Bankacılık Kanunu'nun müşteri sırlarının yurt dışına aktarımını düzenleyen 73.maddesi bu kapsamda değerlendirilebilecektir. Söz konusu madde uyarınca

[76] KVKK, "Kişisel Verilerin Yurt Dışına Aktarılması" (Çevrimiçi) http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20YURTDI%C5%9EINA%20 AKTARILMASI.pdf (Erişim Tarihi:17.12.2021)

BDDK'nın denetimine tabi kurumların BDDK'nın muadili olabilecek yurt dışındaki denetim otoritelerinin talepleri üzerine ortaklarına, faaliyetlerine ve müşterilerine ilişkin müşteri sırları yurt dışına aktarabilmektedir ve bu aktarımın müşteri sırlarına ilişkin sır saklama yükümlülüğünün istisnası olduğu belirtilmektedir. Bu kapsamda gerekli tedbirlerin alınması şartıyla Türkiye'de bulunan veri sorumlusu şirket, söz konusu kanuni hükme dayanarak yurt dışına kişisel veri aktarımında bulunabilecektir. Bu madde uyarınca düzenleme altına alınan finansal kuruluşların kendi aralarında veya doğrudan doğruya ya da risk merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapacakları yurt dışına veri aktarımını kapsayan her türlü bilgi ve belge alışverişleri, paylarının satışı amacıyla muhtemel alıcıların yapacakları değerleme çalışmaları, konsolide finansal tablo hazırlama çalışmaları, risk yönetimi ve iç denetim uygulamaları, derecelendirme veya destek hizmetleri alınması faaliyetleri de hükümde anılan diğer şartların sağlanması halinde aynı kapsamda değerlendirilebilecektir[77]. Öte yandan 7201 sayılı Tebligat Kanunu'nun kişisel veri teşkil eden bilgileri ihtiva eden belge ve kayıtların farklı ülkelere tebliğ edilmesi halinde T.C. Dışişleri Bakanlığı'nın söz konusu yabancı ülkedeki yetkili makama tebliğde bulunması ve bu makamın da ilgili ülkedeki kişiye tebligatı yönlendirmesi yine yurt dışına kişisel veri aktarımının yapılmasına dayanak oluşturan mevzuat düzenlemeleri arasında yer almaktadır. Ayrıca 6706 sayılı Cezaî Konularda Uluslararası Adlî İş Birliği Kanunu'nun uluslararası adli iş birliği kapsamında ilgili kişilere ait özel nitelikli kişisel verileri de içeren verileri yurt dışındaki yetkili makamlara sunulmasını düzenlemesi, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun uyarınca yurt dışındaki yetkili kurum ve kuruluşlara yönelik Malî Suçları Araştırma Kurulu Başkanlığı tarafından mali ve mesleki bilgiler başta olmak üzere çeşitli bilgilerin aktarılması ve 2920 sayılı Türk Sivil Havacılık Kanunu uyarınca güvenlik ve risk değerlendirmelerinin yapılabilmesi amacıyla havayolu ile seyahat eden kişilere ait kişisel verilerin toplanması ve T.C. İçişleri Bakanlığı'nın onayı ile yurt dışına aktarılması da yine yurt dışına kişisel

[77] Mert Karamustafaoğlu ''Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği'', s. 27 vd.

veri aktarımı konusunda KVKK m.9/6'daki saklı tutulan diğer kanun hükümlerine örnek gösterilebilecektir.

1.3.2.2. Bağlayıcı Şirket Kuralları

Türk hukukunda KVKK ve alt mevzuat hükümleri başta olmak üzere çok uluslu grup şirketlerin kendi aralarında kişisel veri aktarımlarını düzenleyen ve bağlayıcı şirket kurallarına değinen açık bir kanuni düzenleme bulunmamaktadır. Buna karşılık AB hukukunda uzun bir süre önce düzenlenmiş bulunan bağlayıcı şirket kurallarının birden fazla ülkede üyesi bulunan şirket toplulukları açısından kişisel veri aktarımında büyük kolaylıklar sağladığı görülmektedir[78]. Türk hukukunda da bu yönde açık bir düzenlemenin bulunmaması ve bu kuralların uygulamada sağladığı yararlar gözetilerek Kurum tarafından 10.04.2020 tarihinde "bağlayıcı şirket kuralları"na ilişkin bir duyuru yayımlamıştır[79]. Bu duyuru çerçevesinde, çok uluslu grup şirketlerin, bu duyurunun ekinde yer alan formu doldurarak ve gerekli talimatları izleyerek Kurum'a bağlayıcı şirket kuralları başvurusu yapması gerektiği ifade edilmiştir. Kurum tarafından çok uluslu grup şirketlere tanınan bu imkân ile esasında kişisel verilerin yurt dışına aktarımı için gerekli olan izin başvurusuna halel getirilmemiş, yine KVKK m.9/2 (b) gereğince yurt dışına kişisel veri aktarımı farklı bir görünümde Kurul'un iznine tabi kılınmıştır[80].

Kurum'un yayınladığı ve bağlayıcı şirket kurallarına ilişkin yegâne resmi bir açıklama olarak kabul edilebilecek olan bu metin ayrıntılı olarak incelendiğinde esasında aynı konuda Çalışma Grubu'nun oluşturduğu belgelerle içerik olarak oldukça benzer olduğu anlaşılmaktadır. İki metin arasında belirli küçük farklılıklar

[78] Claire Sullivan, 'EU GDPR Or APEC CBPR? A Comparative Analysis Of The Approach Of The EU And APEC To Cross Border Data Transfers And Protection Of Personal Data İn The Iot Era', Computer Law and Security Review, C. 45, s. 380-397

[79] Kişisel Verileri Koruma Kurulu, Bağlayıcı Şirket Kuralları https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, Erişim Tarihi: 01.12.2021

[80] Ezgi Çabuk, Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması, Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, İstanbul 2020, s.104.

olsa da Kurum'un çok uluslu grup şirketler arasındaki kişisel verilerin aktarımında getirdiği düzenlemelerde aslında uluslararası kaynakları takip ettiği ve bunlarla uyumlu bir sistem kabul etmeye çalıştığı gözlemlenmektedir. Buna karşılık Kurul'un kendisine yapılan bağlayıcı şirket kuralları başvurularını kabul ettiğine dair yayımlamış olduğu bir kararı henüz bulunmamaktadır. Kurum tarafından yayımlanan metin, özgünlüğü bakımından eleştirilebilecek olsa da ve henüz Kurum'un bu mekanizmayı etkin olarak uygulamaya koyduğuna dair herhangi bir karar örneği bulunmasa da bağlayıcı şirket kurallarının kabulü, Türk hukukunda grup şirketlerin kişisel verileri yurt dışında kurulu olan diğer grup üyesi şirketlere aktarımının hukuki bir zemine oturtulması sürecinde önemli bir başlangıç teşkil etmektedir[81]. Diğer taraftan Kurul tarafından henüz güvenli kabul edilen ülkelerin listesi yayımlanmamış olsa da bağlayıcı şirket kurallarının hazırlanarak Kurul'un onayının alınması ile Türkiye dışında yabancı bir ülkede kurulu grup üyesi şirkete kişisel veri aktarımı mümkün hale gelecektir.

Bağlayıcı şirket kuralları Türkiye'de bulunan ve veri sorumlusu sıfatıyla aktarımda bulunacak olan grup üyesi şirket tarafından yeterli veri koruması bulunmayan ülkelerdeki veri sorumlusu veya veri işleyen olarak hareket eden diğer grup üyesi şirketlere yapılacak aktarımlar için hazırlanmakta ve bu kurallar ile aktarımın yapılacağı yabancı ülkede de aktarıma tabi tutulan kişisel veriler için güvenliklerinin sağlanması için yeterli korumanın tesis edileceği yazılı olarak aktarımın tarafı olan grup üyesi şirketlerce taahhüt edilmektedir. Kurul tarafından incelenen bağlayıcı şirket kurallarının Kurul tarafından onaylanabilmesi için bu kuralları hazırlayan grup üyesi şirketlerin Kurum'un internet sitesinde yayımladığı duyuruda yer alan başvuru ve içerik şartlarını eksiksiz bir şekilde yerine getirmesi ve varsa bu kurallara dayanak teşkil eden ek bilgi ve belgeleri de Kurul'a sunmalıdır. Bağlayıcı şirket kurallarının hazırlanmasının ardından Kurul'a yapılacak başvurular şirketler topluluğunun merkezinin Türkiye'de bulunması

[81]Murat Volkan Dülger, KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, 11 Nisan 2020, s. 6, https://www.hukukihaber.net/kvkkdan-kisisel-verilerin-yurt-disina-aktariminda-onemli-bir-adim-baglayici-sirket-kurallari-makale,7685.html, Erişim Tarihi: 01.12.2021.

halinde söz konusu grup üyesi şirketin başvuruda bulunması gerekmektedir. Grup şirketlerin Türkiye'de bulunan bir merkezinin bulunmaması halinde ise Türkiye'de bulunan bir grup üyesi şirketin kişisel verilerin korunması konusunda yetkilendirilmesi gerekir. Öyle ki başvuruda bulunacak söz konusu grup üyesi şirket ayrıca kişisel veri aktarımına taraf olan yurt dışındaki diğer grup üyesi şirketlerin bağlayıcı şirket kuralları ile bağlı olmasını, bu kurallara uygun hareket etmeleri için gerekli önlemlerin alınmış olduğunu ve bu kuralların ihlal edilmesi halinde kişisel verileri aktarılan ilgili kişilerin maruz kalacağı zararların tazmin edilmesini taahhüt etmelidir.

Bağlayıcı şirket kuralları kapsamında sorumluluk altına giren grup üyesi şirketlerin veri güvenliğinin sağlanması için alacakları güvenlik önlemlerine de ayrıntılı bir şekilde bağlayıcı şirket kuralları dahilinde belirtmeleri gerekmektedir[82]. Bu noktada topluluk içindeki grup şirketlerin kişisel verilerin korunması konusunda varsa yürüttükleri eğitim ve farkındalık çalışmalarının detaylarına yer vermesi faydalı olabilecektir. Bununla birlikte bu kurallar dahilinde yapılacak kişisel veri aktarımları karşısında ilgili kişilere tanıdıkları haklar ve ilgili kişilerce bu hakların etkili bir şekilde kullanımı için topluluk dahilinde oluşturulan mekanizmalara, şikâyet yönetim süreçlerine, topluluk üyesi şirketler nezdinde varsa belirli aralıklarla gerçekleştirilecek denetim faaliyetlerine ve bu denetimlerin kapsamına da yer verilmesi büyük önem arz etmektedir. Ayrıca bağlayıcı şirket kurallarında aktarıma taraf grup üyesi şirketlerin aktarımda bulunacağı kişisel verilerin türlerinin, aktarımın amaçlarının, süresinin, aktarımın hukuki dayanaklarının, hangi yöntemlerle aktarımın gerçekleşeceğinin, aktarıma tabi kişisel verilerin konusu olan ilgili kişi gruplarının, aktarımın grup şirketler dışında farklı alıcı gruplarını da kapsayıp kapsamadığının, kapsıyorsa söz konusu diğer alıcı grupların da belirtilmesi gerekmektedir. Bununla birlikte bu kurallar dahilinde Kurul'a bildirilmiş hususlarda gündeme gelecek değişiklik ve güncellemelerin de aynı şekilde gecikmeksizin Kurul'a bildirilmesi gerektiği unutulmamalıdır. Çok uluslu

[82] Martin Selmayr Datenschutz-Grundverordnung Kommentar, 2. Auflage C.H. Beck, München, Almanya, s. 783.

grup şirketlerde kişisel veri aktarımlarının en temel mekanizmalarından birini oluşturan bağlayıcı şirket kurallarına ve içeriğine, Çalışmamızın üçüncü bölümünde ayrıntılı bir şekilde yer verilecektir.

1.3.2.3. Taahhütnameler

Kurul'un 02/04/2018 tarih ve 2018/33 sayılı kararı ile kişisel verilerin korunması hukukuna giren "*Taahhütnameler*", Türkiye'de kurulu olan veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerdeki veri sorumlusu ya da veri işleyen kişiye kişisel veri aktarımında izlenebilecek yollardan bir tanesidir ve çok uluslu grup şirketler tarafından da kendi aralarında yapacakları aktarımlarda kullanılabilecek önemli bir veri aktarım yöntemidir. Yeterli korumanın bulunmadığı bir ülkeye yapılacak kişisel veri aktarımlarında aktarıma tabi kişisel verinin ilgili kişisine ait açık rızanın bulunmaması ve fakat KVKK m. 5 veya m.6'da yer alan veri işleme şartlarından en az birisinin bulunması halinde kişisel veri aktarımı taahhütleri uygulama alanı bulmaktadır. Aktarımın tarafı olan şirketlerin yeterli korumayı yazılı şekilde taahhüt etmeleri ve bu taahhüdün Kurul tarafından yeterli ve etkili bulunması halinde kişisel verilerin Türkiye'den yurt dışına aktarımı taraflarca hazırlanacak söz konusu veri sorumlusu-veri sorumlusu ya da veri sorumlusu-veri işleyen taahhütnameleri ile mümkün kılınmıştır. Taahhütnamelerde Türkiye'de yerleşik veri sorumlusu tarafça asgari olarak kişisel veri aktarımında bulunan veri sorumlusu tarafın kimliği ve yükümlülükleri, aktarılan söz konusu kişisel verilerin alıcısı olan yurt dışındaki veri sorumlusu veya veri işleyen tarafın kimliği ve yükümlülükleri ile tarafların tabi olacağı KVKK m. 9/2 (b) ve 12/2'de yer alan ortak koruma maddelerinin bulunması zorunlu tutulmaktadır[83]. Taraflarca hazırlanan taahhütnamenin her iki tarafın yetkili kişilerince imzaya verilerek Kurul'un onayına sunulması gerekmektedir. Bağlayıcı şirket kuralları başvurularının aksine Kurul'un sayısı az da olsa kendisine sunulan söz konusu

[83] Turan, s.147.

taahhütnameleri onayladığına ve bu kapsamda yurt dışına kişisel veri aktarımı yapılmasına imkân tanıdığına yönelik kararları bulunmaktadır[84].

Çok uluslu grup şirketler arasında yapılacak kişisel veri aktarımlarında iki grup üyesi şirket tarafından hazırlanacak taahhütnamelerde gerek usul gerekse içerik hususlarında Kurul'un belirttiği şartların eksiksiz bir şekilde yerine getirilmesi gerekmektedir[85]. Aksi halde taahhütname başvurularının reddedilmesi gündeme gelecektir. Bu noktada başvurunun usulen uygun bir şekilde gerçekleştirilmesi, taahhütnamenin tarafların yetkili kişilerince imzalanmış olması, taahhütnamenin ekine söz konusu kişilerin imzaya yetkili belgelerinin ve gerekirse diğer ek bilgi ve belgelerin eklenmesi büyük önem arz etmektedir. Bununla birlikte Kurul, taahhütnamede yer alan hükümlerin tıpkı Tüzük kapsamında öngörülen standart sözleşme maddeleri gibi değişikliklere yer verilmeden taraflarca kabul edilmesini ve varsa ilave hükümler altında tabi olacakları ek düzenlemelere yer vermelerini beklemektedir. Diğer taraftan Kurul, aktarıma tabi tutulacak kişisel verilerin ve kategorilerinin, bu verilerin sahibi olan ilgili kişi gruplarının, aktarımın amaçlarının ve hukuki sebeplerinin, aktarımın grup üyesi şirketler dışında farklı alıcı gruplarına da sirayet etmesi halinde bu alıcı grupların ve alıcı gruplarına aktarım amaçlarının da taahhütname kapsamında belirtilmesi gerektiğini belirtmektedir. Öte yandan aktarımın tarafı olan grup üyesi şirketlerce veri güvenliğine ilişkin alınan tedbirlerin de varsa tarafların VERBİS kayıt bilgilerinin de taahhütnamede yer alması aranmaktadır.

---

[84] Kurul, veri sorumluları Amazon Turkey Perakende Hizmetleri Ltd. Şti. ve Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti. tarafından yurtdışına kişisel veri aktarımı yapılması hususundaki Taahhütname başvurularına Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2. fıkrasının (b) bendi kapsamında 04.03.2021 tarihinde izin vermiştir.
https://www.kvkk.gov.tr/Icerik/6898/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU, erişim tarihi: 01.12.2021.

[85] KVKK, "Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru", 7 Mayıs, 2020,
https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU

1.3.3. ABD'deki Mevcut Düzenlemeler

1.3.3.1. Genel Olarak

ABD hukukunda tıpkı diğer pek çok alanda olduğu gibi yazılı olarak kanun yapma tekniği yaygın olmadığından kişisel verilerin korunması adıyla çıkarılmış henüz herhangi bir yasal düzenleme bulunmadığı görülmektedir. Öyle ki ABD Anayasası'nda dahi kişisel verilerin korunması hakkını içeren özel yaşamın gizliliği hakkı düzenlenmemiştir. Bu hak, 19. yüzyılın sonlarında tartışılmaya başlanmış ve ilerleyen yıllarda ancak içtihatlarla kabul görmüştür[86]. Mahkemelerce kabul edilen içtihatlar da kişisel verilerin korunması kavramının genellikle kişinin mahremiyet hakkı kapsamında ele alındığı görünmektedir. Kişisel verilerin gizliliği açısından verilen mahkeme kararlarına bakıldığında bunlardan uzun bir süre kişisel veri uygulamalarını ciddi şekilde etkileyen U.S. v. Miller davası önem arz etmektedir. Amerikan Federal Temyiz Mahkemesi[87] 1976 yılında kişilerin üçüncü kişilere kendi rızalarıyla aktardığı veriler üzerinde herhangi bir gizlilik beklentisi (reasonable expectation of privacy) içinde olmalarının haklı bir beklenti olmadığına karar vererek "üçüncü taraf doktrini" olarak kabul edilen bir karar vermiştir. Bu karar ile mahkeme ABD'deki yasal makamların bir mahkeme kararına gerek bulunmaksızın kişilerin internet veya e-posta hizmeti sunucularında bulunan kişisel verilere erişim sağlayabilme hakkının olduğunu ifade etmektedir[88].

Bununla birlikte ABD'de kişisel verilerin korunması daha çok yargı kararları ile ilerlese de ve kişisel verilerin korunmasına ilişkin bağımsız bir ulusal otorite ya da hukuki düzenlemelerde tek ve birleşik bir yasa bulunmasa da farklı yasalarda yer

[86]Küzeci, s.61.
[87] Yüksek Mahkemenin 1967 tarihli Katz v. US kararında, kamusal alandaki görüntü kayıtlarının mahremiyet kapsamında kabul edilemeyeceğini ve özel hayatın gizliliğini ihlal etmeyeceği kararını vermiş ve bu anlamda kişisel verilerin korunmasına ilişkin bir karar vermiştir, bkz. Bozlak, Ayhan, "Kamusal Bağlamda Özel Hayatın Korunması: ABD Federal Yüksek Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Uygulaması Arasında Mukayeseli Bir İnceleme, Türkiye Barolar Birliği Dergisi, (109), ss.55-92, 2013, s.77.
[88] United States v. Miller, 425 U.S. 435, 1976; Ata Umur Kalender, Parçalı Bulutlar: Cloud Act ve Etkileri, Kişisel Verileri Koruma Dergisi, S. 2(2), ss.73-106, 2020, s.76.

alan ve kişisel verilerin korunmasına ilişkin pek çok sektörel düzenleme bulunduğu görülmektedir. Öyle ki ABD'de de yazılı kanun yapma tekniğinin yaygın olmaması ve yargı kararlarının ülke genelinde adaletin tesisi açısından önemli bir yer teşkil ediyor olması ülkede kişisel verilerin korunması alanında gerekli ve yeterli düzenlemelerin bulunmadığı şeklinde yorumlanmamalıdır. Her ne kadar kişisel verilerin korunması adıyla tek bir kanunun bulunmaması ve kişisel verilerin korunmasında birçok alana özgü kişisel veri düzenlemesinin yapılması bu alanın dağınık bir yapıya sahip olmasına yol açsa da kişisel verilerin korunmasına yönelik pek çok sektörel düzenleme bulunmaktadır. Özellikle belirli Kaliforniya (Kaliforniya Tüketici Gizliliği Kanunu gibi), Kolorado (Kolorado Gizlilik Kanunu gibi), Virginia (Virginia Tüketici Verilerini Koruma Kanunu gibi) başta olmak üzere belirli eyaletlerde kişisel verilerin korunması alanında ayrıntılı düzenlemelerin yer aldığı görülmektedir. ABD'deki kişisel verilerin korunması alanındaki bu yasalara örnek olarak mali bilgilerin korunmasına yönelik 1978 tarihli Mali Mahremiyet Kanunu (Financial Privacy Act), 1986 tarihli Elektronik Ticarette Gizlilik Kanunu, 1996 tarihli İletişim Ahlak Yasası (Communications Deceny Act), 1998 tarihli Çocukların Çevrimiçi Korunması Yasası (Child Online Protection Act), 1988 tarihli Video Gizlilik Koruması Kanunu (Video Privacy Protection Act) 2018 tarihli Yurtdışındaki Verilerin Yasal Kullanımı Kanunu (Clarifying Lawful Overseas Use of Data Act) verilebilir.

Öte yandan, *Schrems I* kararından sonra ABD Kongresi'nin onayı ile 23 Mart 2018 tarihinde kısaca Bulut Kanunu (Clarifying Lawful Overseas Use of Data Act-CLOUD) olarak bilinen bir yasa kabul edilmiştir ve Bulut Kanunu ile iletişim ve bulut hizmeti sağlayıcılarının sunucularında tutulan kişisel verilere ABD kolluk kuvvetlerinin erişim yetkisi düzenleme altına alınmıştır. Bulut Kanunu'na göre ABD kolluk kuvvetleri ABD sınırları içinde ve ABD dışındaki ülkelerde tutulan kişisel verilere ilişkin herhangi bir talepte bulunursa bu kanunda belirtilen şartlara uygun olarak söz konusu kişisel verilere erişim sağlayabilmektedir. Bulut Kanunu, ABD'ye kişisel veri aktarımında ABD tarafından sağlanacak güvenliğe ilişkin belirli sorunları gün yüzüne çıkarmıştır. ABD Adalet Bakanlığı, Bulut Kanunu'na

ilişkin 2019 yılında yaptığı yazılı bir bilgilendirmede, bu düzenlemenin siber suçlar ve çocukların cinsel istismarı suçlarına daha hızlı müdahale amacıyla getirildiğini ve bu çerçevede Türkiye'nin de 22.4.2014 tarihli ve 6355 sayılı Kanunla[89] taraf olduğu Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ("Budapeşte Sözleşmesi") ile uyumlu olduğunu belirtse de hizmet sağlayıcı şirketlerin bu yönde bir talep üzerine kişisel verileri ABD'ye aktarırken merkezlerinin bulunduğu ülkenin kanunlarına göre hareket etmelerinin gerekecek olması ve bu sebeple belirli durumda kişisel verileri ABD'ye aktaramayacak olmaları bir sorun teşkil etmektedir.

Her ne kadar Bulut Kanunu'nda hizmet sağlayıcı şirketlerin farklı ülkelerde yer alan veri merkezlerinin de bu kanuna tabi olduğu belirtilerek bu soruna bir çözüm getirilmeye çalışılsa da bu kanun ile birlikte ortaya çıkan uygulanacak hukuk sorunu tam olarak çözümlenmiş değildir. Bununla birlikte, Bulut Kanunu'nun 2523 sayılı bölümünde belirtilen ve yabancı devletler ile kişisel verilerin paylaşımı hususunda uluslararası anlaşmalar yapılabileceği hükmü kanunun uygulanmasından doğan uygulanacak hukuk sorununun çözümünde yardımcı olabilecektir. Bu hükme dayanarak akdedilen anlaşmalar çerçevesinde hizmet sağlayıcı şirketin veri merkezlerinin bulunduğu ülkeler ile ABD arasında hukuka uygun bir şekilde kişisel veri aktarımı gerçekleştirilebilecektir[90]. Ancak bu anlaşmaların akdedilmesi uzun süren müzakere dönemlerini de beraberinde getirdiğinden kısa vadede kişisel verilerin aktarımına ilişkin kanundan doğan uygulanacak hukuk sorununa çözüm bulması pek olası gözükmemektedir. Bununla birlikte söz konusu hükme dayanarak ABD ile kişisel verilerin aktarımına ilişkin uluslararası anlaşmalar akdeden ülkeler de bulunmaktadır. İngiltere ile 3 Ekim 2019 tarihinde ABD arasında imzalanan uluslararası veri aktarımına ilişkin anlaşma buna örnek niteliğindedir. Ancak her ne kadar İngiltere ABD ile bu anlaşmaya taraf olsa da kişisel verilerin ABD'ye aktarımı sonrası yeterli koruma tabi olmadığı şeklindeki Schrems I ve II kararlarında belirtilen gerekçelere bakıldığında AB'nin ABD ile bu yönde bir

[89] RG Tarih: 02.05.2014, Sayı: 28988.
[90] Hocaoğlu / Doğan / Saltık, s.367.

uluslararası anlaşmaya taraf olması yakın dönemde pek de muhtemel görünmemektedir.

1.3.3.2. Gizlilik Kalkanı Anlaşması

ABAD tarafından verilen Schrems II kararıyla AB ile ABD arasında hukuka uygun bir veri aktarım faaliyetinde yeterli güvenlik tedbiri teşkil etmediği gerekçesiyle iptal edilmiş olsa da AB ile ABD arasındaki kişisel veri aktarımına ilişkin getirdiği düzenlemeler ile 12 Temmuz 2016 tarihinde yürürlüğe giren Gizlilik Kalkanı Anlaşması önemli bir yere sahiptir[91]. Gizlilik Kalkanı Anlaşması öncesinde AB ile ABD arasındaki aktarımlar 6 Ekim 2015 yılında Schrems I kararıyla geçerliliğini yitiren Güvenli Liman Anlaşmasına dayanarak gerçekleştirilmekteydi[92]. Gizlilik Kalkanı Anlaşması uyarınca veri işleyen şirketler bildirim, seçim, gelecek aktarımlar için hesap verilebilirlik, güvenlik, veri bütünlüğü ve amaçla sınırlı olma, erişim, başvuru, uygulama ve sorumluk olarak kabul edilen ilkelere[93] uyum sağlamayı taahhüt etmektedir. Bu taahhüdü gereğine uygun bir şekilde yerine getiren şirkete de Gizlilik Kalkanı uyarınca Tüzük'teki güvenlik tedbirlerine benzer bir mekanizma olan sertifika verilmektedir.

Gizlilik Kalkanı Anlaşması uyarınca şirketler tarafından yerine getirilmesi gereken bildirim yükümlülüğü şirketlerin her bir veri işleme faaliyetlerine göre ilgili kişileri açık bir şekilde bilgilendirmesi[94] ve bu kapsamda gerekli metinleri oluşturması anlamına gelir. Bununla birlikte seçim ilkesi ise mevcut veri işleme amaçlarından farklı bir amaçla veri işleme başlayan şirketlerin yeni işleme amacına istinaden ilgili

[91] Yeterlilik kararının tam metni: Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EUU.S. Privacy Shield, 2016, Official Journal of the European Union L 207/1, https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

[92] "Maximillian Schrems v Data Protection Commissioner" kararının İngilizce metnine (https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62014CJ0362) adresinden ulaşılabilir

[93] "Privacy Shield Framework," The International Trade Administration (ITA)- U.S. Department of Commerce, erişim 18 Şubat, 2020, https://www.privacyshield.gov/EU-US-Framework.

[94] "Notice," The International Trade Administration (ITA)- U.S. Department of Commerce, Erişim 18 Şubat, 2020, https://www.privacyshield.gov/article?id=1-NOTICE.

kişiye başvurması ve söz konusu yeni amaca istinaden veri işlenmesine onay verip vermediğinin sorulmasıdır. Bu noktada ilgili kişiye şirket tarafından planlanan yeni veri işleme amacı ve faaliyeti için bir seçim imkânı sunulmuş olur ve bu sayede ilgili kişinin rızası dışında bir veri işleme faaliyeti gerçekleştirilmesinin önüne geçilmesi amaçlanmaktadır. Ayrıca Gizlilik Kalkanı Anlaşması uyarınca ilgili kişilerin şirketlere başvuruda bulunması için şirket tarafından etkili mekanizmaların oluşturulmuş olması ve veri işleme faaliyetlerinden doğabilecek olası uyuşmazlıkların hızlı bir şekilde çözümü için etkin yolların öngörülmüş olması beklenmektedir. Bu kapsamda şirketin ortaya çıkabilecek uyuşmazlıklar ve kendisine yöneltilen ilgili kişi taleplerine karşı arabuluculuk gibi bağımsız bir başvuru mekanizması kabul etmesi, tahkim gibi alternatif uyuşmazlık çözümlerine yer vermesi, yerel veri koruma otoritelerine şirket için başvuruda bulunulmasına imkan tanınması, söz konusu veri koruma otoritelerinin ABD'deki ilgili kurumlar[95] ile koordinasyon içerisinde olması ve bu yolların ücretsiz bir şekilde işletilebilmesi ile şirketlerin tüm bu süreçte ilgili kişi ile uzlaşmacı bir şekilde hareket etmesi ve iş birliğine gitmesi büyük önem arz etmektedir.

Bununla birlikte Gizlilik Kalkanı Anlaşması uyarınca veri sorumlusu olan bir şirketin veri sorumlusu olan başka bir şirkete aktarımda bulunması için alıcı tarafta bulunan şirketin aktarıma tabi tutulan kişisel verilerin sahibi ilgili kişinin rızası ile sınırlı olarak söz konusu verileri işleyebileceğini ve Gizlilik Kalkanı Anlaşması uyarınca veri güvenliğinin sağlanması adına gerekli olan güvenlik önlemlerini alacağına dair taahhütlerini içeren yazılı bir anlaşma yapması gerekmektedir. Diğer taraftan veri sorumlusu bir şirketin veri işleyen olarak faaliyet gösteren başka bir şirkete aktarımda bulunması halinde Gizlilik Kalkanı Anlaşması bu aktarımı tedarikçi yönetimi olarak tanımlamakta ve yine veri işleyen taraf ile veri sorumlusu arasındaki veri aktarım faaliyetine dayanak teşkil eden yazılı bir anlaşmanın bulunmasını aramaktadır. Öyle ki aktarıma dair yeterli güvenlik tedbirlerinim alınmaması ya da bir şekilde aktarıma ilişkin söz konusu taahhütlerin yerine

[95] Gizlilik Kalkanı programı ABD Ticaret Bakanlığı içerisindeki Uluslararası Ticaret İdaresi tarafından yürütüldüğü için ilgili otorite olarak ABD Ticaret Bakanlığı karşımıza çıkmaktadır.

getirilmemesi halinde aktarıma tabi kişisel verinin sahibi ilgili kişinin maruz kalacağı zararlardan esas olarak veri sorumlusu şirket sorumlu tutulmuştur. Sorumluluk mekanizmasının yanı sıra Gizlilik Kalkanı Anlaşması uyarınca hesap verilebilirlik ilkesi gereği şirketlerin kişisel verilerin korunması mevzuatı hükümleriyle uyumlu olduklarını doğrulaması ve yapılacak denetim sonrasında uyumluluk raporunu ilgili kurumlara ibraz etmesi beklenmektedir. Görüldüğü gibi bir sertifika programı şeklinde işleyen Gizlilik Kalkanı Anlaşması hükümleri AB ile ABD arasında aktarıma tabi tutulan kişisel veriler için olabildiğince Tüzük ile paralel güvenlik önlemleri alınması şartlarını öngörerek ilgili kişilerin verilerinin korunması adına önemli ilke ve yükümlülükler içermektedir[96]. Öte yandan Gizlilik Kalkanı Anlaşması uyarınca kişisel verileri işlemeye devam eden her bir şirket bu sertifika programından çıksa da Gizlilik Kalkanı Anlaşması'nın hükümlerine uymakla yükümlendirilmiştir. Bu sayede aktarıma tabi tutulan kişisel veriler için aktarım sonrası da sürdürülebilir koruma önlemleri alınması amaçlanmaktadır.

[96] H. Rolf Weber, Transatlantic Data Protection in Practice, Springer, BerlinHeidelberg, Almanya 2017, s. 39.

İKİNCİ BÖLÜM

ÇOK ULUSLU GRUP ŞİRKETLERDEKİ KİŞİSEL VERİ AKTARIMLARININ AMAÇLARI İLE BUNLARIN HUKUKA UYGUNLUK ŞARTLARI VE VERİ GÜVENLİĞİ TEDBİRLERİ

2.1. Çok Uluslu Şirket ve Grup Şirket Kavramları

TTK'da ekonomik gerçeklik ve maddi hukuk kurallarının çatışmaması amacıyla uygulamada sıklıkla karşımıza çıkan şirketler topluluğu kavramına ilişkin yasal düzenlemeler getirildiği görülmektedir. Şirketler topluluğunun yasal mevzuat dahilinde düzenlemesindeki temel amaçlar esasında şirketler topluluğu içerisindeki hakimiyeti diğer bir deyişle tek elden yönetimi hukuka uygun bir düzene oturtmak ve bu ilişkinin düzenli bir şekilde yürütülmesini ve diğer grup şirketlerden birinin aleyhine hakkaniyete aykırı bir işlem yapılmasının önüne geçilmesini sağlamaktır. Ayrıca bu düzenlemelerin bağlı şirketin topluluk dışında kalan pay sahiplerini ve alacaklılarını korumak, bağlı şirket yönetim kurulu üyelerinin hakkaniyete aykırı bir şekilde bağımsız bir şirketin yönetim kurulu üyesi gibi sorumlu tutulmasını önlemek ve topluluğun yönetiminde kolaylık sağlamak gibi farklı yararları da bulunmaktadır[97]. Bu düzenlemelere karşılık TTK'da doğrudan şirketler topluluğu ya da bu topluluğu oluşturan grup şirketlere ilişkin net bir tanımlamaya yer verilmemiştir. Bu yönde bir tanımlama bulunmamasına rağmen TTK m.195'te bir ticaret şirketinin diğer bir ticaret şirketinde doğrudan ya da dolaylı olarak oy haklarının çoğunluğuna ya da şirket sözleşmesi uyarınca, yönetim organında karar alabilecek çoğunluğu oluşturan sayıda üyenin seçimini sağlayabilme hakkını haiz olması veya kendi oy haklarının yanında, bir sözleşmeye dayanarak, tek başına veya diğer pay sahipleri ya da ortaklarla birlikte, oy haklarının çoğunluğunu oluşturması veyahut bir ticaret şirketinin diğer bir ticaret şirketini, bir sözleşme gereğince veya

[97] Efe Dündar, Yeni Türk Ticaret Kanunu Çerçevesinde Çok Uluslu Şirketler, Yayımlanmamış Doktora Tezi, İstanbul Kültür Üniversitesi, İstanbul 2013, s.85 vd.; Fatma Betül Çakır Çelebi, "Şirketler Topluluğunda Hâkim Teşebbüs", Ticaret ve Fikri Mülkiyet Hukuku Dergisi C.4, S.1,2018, s.20.

başka bir yolla hâkimiyeti altında tutuyor olması şeklinde belirli kriterlere yer verilerek dolaylı olarak şirketler arasında hakimiyet ve bağlılık ilişkisi tanımlanmaya çalışılmıştır. Görüldüğü üzere şirketler topluluğunun dayandığı temel araç hakimiyet ve kontrol ilişkisidir ve hakimiyetin fiili kontrol ya da sözleşmesel kontrol şeklinde ve doğrudan ya da dolaylı olması mümkündür. Doğrudan hakimiyet, hakim şirketin bağlı şirkette hakimiyeti tek başına elinde tutmasıyken; dolaylı hakimiyet ise bir hakim şirketin, bir veya birkaç bağlı şirket aracılığıyla bir diğer şirkete hakim olması anlamına gelmektedir. Ayrıca dikkat edilmesi gereken bir diğer husus ise hakim şirketin bağlı şirkete ait sermayenin çoğunluğuna sahip olması tek başına bir hakimiyet ve kontrol aracı olarak görülmemiş, hakim şirketin bağlı şirkete ait yönetimde ya da oyda imtiyazlı olması sermayesinin çoğunluğuna sahip olmayı önemsiz hale getirebilecek nitelikte kabul edilmiştir. TTK m. 195/1'de şirketler topluluğu, bu kriterlerden de anlaşılacağı üzere genel olarak ticaret şirketleri esas alınarak düzenlenmiştir. Ticaret şirketleri adi ortaklıktan farklı olarak bir tüzel kişiliğe sahip olan ve tacir sıfatını taşıyan şirketlerdir ve şahıs ya da sermaye şirketi olarak ikiye ayrılırlar. Öyle ki anonim, limited, kollektif, komandit şirket ve kooperatif bir ticaret şirketi niteliğindedir. Ancak TTK m. 195/5 ile bu kurala bir istisna konulmuş ve şirketler topluluğunun hâkiminin, merkezi veya yerleşim yeri yurt içinde veya yurt dışında bulunan bir teşebbüs olması hâlinde de, 195 ilâ 209 uncu maddeler ile TTK'daki şirketler topluluğuna ilişkin hükümlerin uygulanacağı belirtilmiştir.

Teşebbüs, TTK kapsamında şirketler hukuku bakımından yeni bir kavram olduğundan, teşebbüsün tanımı yapılırken rekabet hukuku mevzuatına bakılması faydalı olacaktır. RKHK m. 3 uyarınca teşebbüs, "Piyasada mal veya hizmet üreten, pazarlayan, satan gerçek ve tüzel kişilerle, bağımsız karar verebilen ve ekonomik bakımdan bir bütün teşkil eden birimleri ifade eder". Doktrinde de teşebbüsün tanımına ilişkin çeşitli görüşler bulunmaktadır. Tekinalp ilgili mal veya hizmet piyasasında, mal veya hizmet üreten, bunları pazarlayan, aracılık eden, danışmanlıkta bulunan, organizasyon yapan, bütün gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan ancak hukuken bağımsız ve ekonomik açıdan bir bütün

oluşturan birimlerin teşebbüs olduğunu belirtirken[98] Aslan ise teşebbüsü, üretim, dağıtım veya hizmet verme gibi ekonomik faaliyetlerde bulunan, bağımsız karar verme özgürlüğüne sahip ekonomik varlıklar olarak tanımlamaktadır[99]. Bu görüşler tahtında teşebbüsün temel unsurlarının ekonomik bağımsızlık ve ekonomik faaliyet olarak belirtmek yanlış olmayacaktır. TTK'da ekonomik faaliyetin şekli konusunda herhangi bir kısıtlama yapılmamıştır. Bu sebeple herhangi bir mal veya hizmet piyasasında üretim, satış, pazarlama ve dağıtım gibi ekonomik sürecin herhangi bir noktasında işlerlik göstermek ekonomik faaliyet yürütme unsurunun yerine getirilmesi için yeterli görülebilecektir[100]. Diğer taraftan ikinci bir unsur olarak kabul edilen ekonomik bağımsızlık ise işletmenin herhangi bir ekonomik kontrol veya egemenlik altında bulunmaması anlamına gelir. Ekonomik egemenlik işletmenin kendi yönetimsel ve muhasebesel bağımsızlığının bulunması, ticari faaliyetlerini ve politikalarını kendi ekonomik amaç ve menfaatleri uyarınca tek başına ve kendi içinde belirlemesi, bu kapsamda ekonomik planlama ve karar mekanizmalarının kendi işletmesi içerisinde kalması bu şekildedir[101]. Bu unsurları bünyesinde bulunduran gerek gerçek kişi ya da tüzel kişi veya devlet işletmeleri veyahut tüzel kişiliği bulunmayan adi şirketler de güttükleri ekonomik amaca ya da büyüklüklerine bakılmaksızın, rekabet hukuku çerçevesinde teşebbüs olarak kabul edilecektir[102].

---

[98] Ünal Tekinalp, Ünal, Grup İçi Teşebbüsler Arasındaki Birleşme ve Devralmalar İçin Rekabet Kurulunun İznine Gerek Olup Olmadığı Sorunu, Cumhuriyetin 75. Yılı Armağanı, İstanbul (Grup İçi Teşebbüsler), s. 781.

[99] Yılmaz Aslan, Rekabet Hukuku, Teori-Uygulama Mevzuat, 4. Baskı, s. 47.Efe Dündar, Yeni Türk Ticaret Kanunu Çerçevesinde Çok Uluslu Şirketler, Yayımlanmamış Doktora Tezi, İstanbul Kültür Üniversitesi, İstanbul 2013, s.85 vd.; Fatma Betül Çakır Çelebi, "Şirketler Topluluğunda Hâkim Teşebbüs", Ticaret ve Fikri Mülkiyet Hukuku Dergisi C.4, S.1,2018, s.20.

[100] Rekabet Kurulu, 13.03.2001 tarihli ve 01-12/11429 sayılı kararı, https://www.rekabet.gov.tr/Karar?kararId=c560ab01-e956-4629-baa4-637ea81281d9 (23.03.2018).

[101] Rekabet Kurulu 13.03.2001 tarihli ve 01-12/11429 sayılı kararı, https://www.rekabet.gov.tr/Karar?kararId=c560ab01-e956-4629- baa4-637ea81281d9 (23.03.2018).

[102] C-41/90, EuGH-Höffner u. Elser v. Macrotron, ECLI::EU:C:1991:16; Rekabet Kurulu, 13.03.2001 tarihli ve 01-12/11429 sayılı kararı, https://www.rekabet.gov.tr/Karar?kararId=c560ab01-e956-4629-baa4-637ea81281d9 (23.03.2018).

TTK m. 195/1 uyarınca bir ticaret şirketinin en az iki ticaret şirketinde doğrudan veya dolaylı olarak hâkimiyet sağlaması ve hâkim veya bağlı şirketlerden en az birinin merkezinin Türkiye'de olması halinde, bu şirketler hakkında TTK'daki şirketler topluluğuna ilişkin hükümler uygulanacağı belirtilmiştir. Bu hükümden yola çıkarak şirketler topluluğu hükümlerinin uygulanabilmesi için hâkim şirketin bir ticaret şirketi olması halinde, bir bağlı şirketin bulunması yeterli görülebilecekken, teşebbüs olması halindeyse bağlı en az iki ticaret şirketinin bulunması gerekmektedir[103]. Öyle ki bu görüş, şirketler topluluğu hükümlerinin uygulanabilmesi için en az iki ticaret şirketi bulunması gerektiğini savunmaktadır[104]. Ancak bizim de katıldığımız hâkim görüşe göre TTK kapsamında bir şirketler topluluğu kurulabilmesi için hâkim şirket veya teşebbüs ve ona doğrudan veya dolaylı olarak bağlı olan bir bağlı şirketin mevcudiyeti yeterli kabul edilecektir[105]. Farklı bir deyişle, şirketler topluluğunun hâkimi bir ticaret şirketi ya da bir teşebbüs de olsa bir bağlı şirketin bulunması TTK'daki şirketler topluluğu hükümlerinin uygulanmasına imkân tanıyacaktır. Çünkü şirketler topluluğunu hüküm altına alan TTK m. 195 için önemli olan, şirketler topluluğunun kaç şirketten oluştuğu değil, bir ticaret şirketinin veya teşebbüsün başka bir ticaret şirketini TTK m. 195'de belirtilen kriterlerden biriyle hâkimiyet ve kontrol altında tutup tutmadığıdır. Bu açıklamalar kapsamında kontrolü anılan yollardan en az biriyle elinde tutan şirket topluluk dahilinde hâkim ya da ana şirket olarak ve kontrol edilen şirket ise bağlı ya da yavru şirket olarak anılmaktadır.

[103] Gül Okutan Nilsson, s.67; Oruç Hami Şener, Teorik ve Uygulamalı Ortaklıklar Hukuku Ders Kitabı, Ankara, (Ortaklıklar Hukuku), s.172.
[104]Okutan Nilsson, s.67
[105]Eminoğlu, Kurumsal Yönetim, s.163-164; Hasan Pulaşlı, 6102 Sayılı Türk Ticaret Kanunu'na Göre Şirketler Hukuku Şerhi, C.1, Ankara, (Şerh), s.284; Pulaşlı, Hasan, Yeni Türk Ticaret Kanunu'na Göre Tek Ortaklı Sermaye Şirketleri ve Buna İlişkin Bazı Özel Durumlar, REGESTA (2011), S.1 (Tek Ortaklı Şirketler), s.13 vd.; Abuzer Kendigelen, Türk Ticaret Kanunu, Değişiklikler, Yenilikler, İlk Tespitler, İstanbul, s.174; Fatih Bilgili / Ertan Demirkapı, Şirketler Hukuku, Bursa, s.12; Aynı yönde, Gökmen Gündoğdu, Bir Şirketler Topluluğu En Az Kaç Bağlı Şirketten Oluşur? -Ticaret Sicil Yönetmeliği m. 105 Hükmünün Türk Ticaret Kanunu m. 195 Hükmü ile Uyumsuzluğu Sorunu, Legal Hukuk Dergisi, S.133, C.12, s.115 119; Fatih Aydoğdu, Tek Kişi Ortaklığı, İstanbul, s.276.

Uluslararası Hukuk Enstitüsü çok uluslu grup şirketleri "herhangi bir ülkede kurulu bir karar alma mekanizmasının yanı sıra birden fazla ülkede hukuki kişiliğe sahip olarak yahut olmadan faaliyette bulunan merkezlerden oluşan girişimler" şeklinde tanımlamıştır[106]. Birleşmiş Milletler de çok uluslu grup şirketleri "iki veya daha fazla ülkede birbirleriyle bağlantılı şekilde ortak bir strateji izleyen ve tek bir karar alma mekanizması altında faaliyetlerini yürüten tüzel kişilerden oluşan yapılar" olarak tanımlamaktadır[107]. Diğer taraftan Uluslararası Çalışma Örgütü (ILO) ise çok uluslu şirketi "kurulu bulundukları ülke dışında mal yahut hizmet bazında üretim ve dağıtım yapan kamu, özel yahut karma yapıdaki kuruluşlardan oluşan yapı" biçiminde adlandırmıştır[108]. Bu tanımlara bakıldığında, çok uluslu grup şirketlerin, dünya üzerinde pek çok yerde bulundukları ülkenin iç hukuklarına uygun şekilde kurulu olan tüzel kişiliklere sahip ve global olarak ticari faaliyetler yürüten kuruluşlar olduğu sonucuna varılabilecektir[109].

Grup şirket kavramı Kurul tarafından grup şirketler arasındaki kişisel verilerin aktarımına ilişkin özellikli düzenlemeler getiren ve bu aktarımların Kurul'un onayıyla hukuka uygun bir hale getirilmesi için aktarımın tarafı olan grup şirket üyeleri tarafından hazırlanacak bağlayıcı şirket kurallarına ilişkin metinlerde de tanımlandığı görülmektedir. Kurul'un 10 Nisan 2020 tarihinde internet sitesinde yayımladığı "Bağlayıcı Şirket Kuralları Hakkında Duyuru"nun ekleri olan "Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu" ve "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman'da grup "*Bir şirketler topluluğuna bağlı olarak faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularının*

[106]Merve İspirli Armağan, Uluslararası Hukukta Çok Uluslu Şirketler ve İnsan Hakları Yükümlülükleri, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi İstanbul 2019, s.22.
[107] Report of UN Center on Transnational Corporations, E/1988/39/Add.1, para.1a. için bkz. Silvia Danailov, The Accountability Of Non-State Actors For Human Rights Violations: The Special Case Of Transnational Corporations, w. place., Institut Universitaire De Hautes Études Internationales, 1998, s.11.
[108]Danilov, s.11.
[109] İspirli Armağan, s.22.

tümü" olarak ve grup üyesi kavramı ise *"Şirketler topluluğuna bağlı bir şirket ya da teşebbüs ile ortak bir ekonomik faaliyette bulunan ya da veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan bir gruptaki veri sorumluları"* olarak tanımlanmıştır. Bu tanımlamalarda grup ve grup şirket, bir şirketler topluluğuna bağlı olarak ticari faaliyetlerini sürdüren bir şirket veya teşebbüs olarak aynı zamanda kişisel verilerin işlenmesi konusunda da diğer grup şirketler ile müşterek bir ekonomik amaç güden ve bu sebeple veri işleme faaliyetlerinde bulunan bir veri sorumlusu şirket olarak ele alınmıştır.

Görüldüğü üzere grup ve grup şirket tanımlamaları şirketler topluluğunun ticari, ekonomik ve hukuki özelliklerinin ve faaliyetlerinin topluluğu oluşturan her bir grup üyesi şirketin tek başına ya da kendi aralarında yürüttükleri kişisel veri işleme faaliyetleri ışığında değerlendirilerek açıklanmıştır. Ancak her ne kadar bu tanım grup şirketlerin kendi aralarında ve üçüncü kişilere karşı yürüttükleri ticari faaliyetlerin uygulamada farklılıklar gösterebilmesi ve topluluk içerisinde belirli grup şirketlerin diğer grup üyesi şirketler için veri sorumlusu yerine veri işleyen sıfatıyla faaliyette bulunuyor olması gibi çeşitli açılardan eleştirilebilecek olsa da, ticaret hukukuna ilişkin TTK'da düzenlenen bir kavram olarak grup şirketlerin kişisel verilerin korunması hukuku perspektifinden ele alınmış olması itibariyle bu tanımlamalar önem arz etmektedir. Bu minvalde grup şirket tanımına yer veren bu metinlerde belirtilmesi gereken bir diğer düzenleme de şirketler topluluğu içerisinde hâkim şirket olarak faaliyet gösteren şirketin Türkiye'de kurulu bir merkezi bulunmaması halinde aktarıma tabi kişisel verilerin kontrolünün sağlanması ve korumasına ilişkin hazırlıkların yürütülmesi için Türkiye'de kurulu bir grup üyesi şirketin yetkilendirilmesi gerektiğidir. Bu düzenleme uyarınca belirlenecek Türkiye'de kurulu grup şirket, şirketler topluluğu dahilinde Türkiye'de "yetkili grup üyesi" olarak tanımlanmakta ve topluluk içi kişisel veri aktarıma ve işleme faaliyetlerine yönelik Kurul nezdinde ve Türkiye'de yürütülecek işlemlerin organizasyonunda önemli bir rol oynamaktadır[110]. Şirketler topluluğu bünyesinde

[110] Toparlak, s.116

faaliyet gösteren her bir grup üyesi şirketin gerçekleşen veri işleme faaliyeti özelinde gerek veri sorumlusu gerekse veri işleyen olarak hareket etmesi mümkündür, bu sebeple şirketler topluluğu içinde gerçekleşen kişisel veri aktarımları da dahil olmak üzere veri işleme faaliyetlerinin daha iyi anlaşılabilmesi için grup üyesi şirketlerin veri sorumlusu ve veri işleyen olarak ele alınması faydalı olacaktır.

2.1.1. Veri Sorumlusu Grup Şirket

Veri sorumlusu, KVKK m.3'de kişisel verinin işleme amacını ve araçlarını tespit eden, veri kayıt mekanizmasının kurulması ve idaresinden sorumlu olan gerçek ya da tüzel kişi şeklinde tanımlamıştır. Bu tanım uyarınca görüldüğü üzere gerçek kişiler haricinde şirketler, vakıf ve dernek gibi tüzel kişiler de veri sorumlusu olabilir[111]. Bu bağlamda şirketler topluluğu dahilinde faaliyet gösteren her bir grup üyesi şirket de hâkim şirket ya da bağlı şirket olduğuna bakılmaksızın somut olaydaki veri işleme faaliyetine göre veri sorumlusu olarak addedilebilecektir. Her ne kadar grup üyesi şirketler aralarındaki kişisel veri işleme ve aktarım faaliyetleri değişkenlik gösterebilse de ve bu faaliyetlerin bazılarında grup üyesi şirketlerden biri veri işleyen sıfatını haiz olabilecekse de grup şirketler açısından değerlendirildiğinde şirketler topluluğunu meydana getiren her bir grup üyesi şirketin ayrı bir tüzel kişiliği bulunduğundan, kural olarak bu şirketlerin her birinin ayrı ayrı ve kendi içlerinde veri sorumlusu olarak kabul edilmesi gerekir. Bu kapsamda her bir grup üyesi şirket kendi kontrolünde bulunan ve/veya işleme amaçlarını ve/veya araçlarını bizzat kendisinin belirlediği kişisel veriler için veri sorumlusudur ve veri sorumlusunun KVKK ve alt mevzuat hükümleri uyarınca taşıdığı yükümlülükleri üstlenmektedir. Öyle ki bir grup üyesi şirketin istihdam ettiği çalışanlarına ilişkin doğrudan ya da bir veri işleyen aracılığı ile işlediği ve sakladığı kişisel veriler için veri sorumlusu olduğunu söylemek mümkündür. Örneğin bu grup üyesi şirketin bir kredi finansman şirketi olması halinde bu şirketin

[111]Tekin Memiş, Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt:3, Sayı:6, Aralık 2017, s.9-23.

kendi çalışanı ile arasındaki iş ilişkisi uyarınca tuttuğu özlük verileri karşısında veri sorumlusu, müşterileri ile arasındaki kredi sözleşmesi ve hizmet ilişkisi uyarınca veri işleyen olarak faaliyet göstermesi de mümkündür. Bu durumda almayı tercih ettiği hizmet uyarınca kişisel verilerinin işlenmesine ve amacına karar veren kredi alan müşteriler veri sorumlusu olarak kişisel verilerinin işlenme ve aktarımına ilişkin nihai kararı verme yetkisine sahip olurlar[112]. Görüldüğü üzere veri sorumlusu sıfatı somut olay nezdinde gerçekleşen kişisel veri işleme ve aktarım faaliyetlerine göre değişkenlik gösterebilmekte ve aynı grup üyesi şirket belirli durumlarda veri sorumlusu belirli durumlardaysa veri işleyen sıfatını taşıyabilmektedir.

Somut olaydaki kişisel veri işleme faaliyetine göre ilgili grup üyesi şirketin veri sorumlusu olup olmadığının tespiti için kişisel verilerin toplanması ve toplama yöntemine, toplanacak kişisel veri türlerine, toplanan verilerin hangi amaçlarla kullanılacağına, hangi kişilerin kişisel verilerinin toplanacağına, toplanan kişisel verilerin üçüncü kişiler ile paylaşılıp paylaşılmayacağına, paylaşılacaksa kimlerle paylaşılacağına ve verilerin ne kadar süreyle saklanacağına kimin karar verdiğine bakılması gerekmektedir. Veri sorumlusu olarak her bir grup üyesi şirketin KVKK m.12 uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önleme ve kişisel verilerin muhafazasını sağlama yükümlülüğü bulunmaktadır. Bu yükümlülüklerini yerine getirmek için veri sorumlusu gerekli olan idari ve teknik her türlü tedbiri almalıdır. Kişisel verilerin bir veri işleyen tarafından işlenmesine karar verilmesi halinde de veri sorumlusunun bu yükümlülüklerini yerine getirmesi gerekmektedir. Öyle ki KVKK ve alt mevzuat söz konusu kişisel verilerin güvenliğinin sağlanmasından bizzat veri sorumlusunu sorumlu kılmaktadır. Diğere bir deyişle veri sorumlusu asli sorumluluk sahibi olarak kabul edilmektedir. Grup üyesi şirketler tarafından yapılacak kişisel veri işleme ve aktarım faaliyetlerinin de hukuka uygun olarak gerçekleşmesi ve aktarıma tabi kişisel verilerin güvenliğinin sağlanması amacıyla aktarımın tarafı

[112]Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF, s.57, Erişim Tarihi: 30.11.2021.

olan her bir grup üyesi şirket tarafından gerekli teknik ve idari tedbirin alındığından emin olunması gerekmektedir.

Veri sorumlusu sıfatının tespiti bağlayıcı şirket kurallarının hazırlanması sırasında da aktarımın gerçekleşeceği grup üyesi şirketlerin görev ve yetkilerinin belirlenmesi için önem arz etmektedir. Yukarıda da belirttiğimiz üzere ilgili kişilere ait kişisel verilerin Türkiye'de kurulu bir veri sorumlusu grup üyesi şirket tarafından yine aynı grup içindeki ve Türkiye'de ya da Türkiye dışında yabancı bir ülkede bulunan diğer bir veri sorumlusu ya da veri işleyen grup üyesi şirkete aktarımının hukuka uygun bir zemine oturtulması için hazırlanabilecek taahhütnamelerden biridir. Bu noktada veri sorumlusu şirketin belirlenmesinde de yine yukarıda belirttiğimiz kriterler esas alınarak bir değerlendirme yapılır. Bu kriterler ışığında yapılacak değerlendirmeye göre kişisel verilerin aktarım amacına ve vasıtalarına karar veren Türkiye'deki grup üyesi şirket veya şirketler veri sorumlusu olacaktır[113]. Şirketler topluluğu bünyesinde veri sorumlusu olarak kişisel veri aktarım faaliyeti gösteren grup üyesi şirket, KVKK ve alt mevzuatta yer alan düzenlemelerin doğrudan muhatabı olduğundan yukarıda da belirttiğimiz gibi gerçekleşen veri işleme ve aktarım faaliyetine karşı da doğrudan sorumluluğu doğmaktadır.[114] Bu sebeple veri sorumlusu sıfatıyla grup üyesi şirketin topluluk dahilinde ve/veya dışında gerçekleştireceği her bir veri işleme ve aktarım faaliyeti için kişisel verilerin hukuka uygun şekilde işlenebilmesi adına gerekli organizasyonu ve koordinasyonu sağlaması ve bu amaçla alınabilecek tüm teknik ve idari önlemleri tek tek temin etmesi gerekmektedir.

Veri sorumlusunun belirli durumlarda veri işleme ve aktarım faaliyetinden doğan hak ve yükümlülüklerini veri işleyene devretmesi mümkündür. Öyle ki veri sorumlusu veri işleyen ile yapacağı bir veri işleme ve aktarım sözleşmesi ile kişisel verilerin toplanmasında kullanılacak bilgi teknolojileri ve yöntemlerini veri işleyen tarafından belirlenmesine karar verebilir ya da kişisel verilerin nasıl saklanacağı,

[113] Dülger, s.17; Çekin, 2020, s.53-54.
[114]Memiş, s.12.

kişisel verilerin korunması için alınacak güvenlik tedbirleri, kişisel verilerin aktarımında kullanılacak teknolojik yöntemler, kişisel verilerin yedeklenmesinde, silinmesinde veya yok edilmesinde kullanılacak yöntemlerin belirlenmesi görevini veri işleyene bırakabilir. Grup üyesi şirketin de veri sorumlusu olarak veri işleme ve aktarım faaliyeti kapsamındaki görev ve yetkilerini kendisini oluşturan organları ve operasyonel departmanları dışında farklı bir tüzel kişi olan ifa yardımcısı veya hizmet sağlayıcısı olarak faaliyet gösterecek grup üyesi diğer bir şirkete devretmesi mümkündür. Bu yönde bir devir işlemi sonrasında veri sorumlusu olan grup üyesi şirketin veri işleme ve aktarımdan kaynaklı olarak KVKK ve alt mevzuat hükümleri uyarınca doğacak yükümlülükleri ortadan kalkmayacak ve devreden ilgili grup üyesi şirket hala veri sorumlusu olarak faaliyet göstermeye ve veri sorumlusu olmaktan doğan yasal yükümlülüklerin gerektiği gibi yerine getirmekten sorumlu olmaya devam edecektir. Görüldüğü gibi veri sorumlusu grup şirketin bir veri işleme veya veri aktarım faaliyetini bağlı şirketi üzerinden yürütmesi halinde veri sorumlusu sıfatı geçerliliğini koruyacak ve bu veri işleme ve aktarım faaliyetinden kaynaklı olarak doğrudan ya da dolaylı bir şekilde ilgili kişiler ve/veya üçüncü kişiler nezdinde ortaya çıkacak zararların tazmin edilmesinden yine veri sorumlusu grup üyesi şirket sorumlu olacaktır[115].

Veri sorumluların KVKK ve alt mevzuat hükümleri uyarınca işlenen kişisel verilerin sahibi ilgili kişilere karşı taşıdıkları sorumluluğa istinaden gerçekleştirdikleri veri işleme ve aktarım faaliyetlerinin Kurul tarafından takip edilebilirliklerinin sağlanması ve veri sorumluları için KVKK'da öngörülen denetim ve yaptırım mekanizmalarının etkinlik kazanabilmesi amacıyla KVKK m. 16 uyarınca Türkiye'de veri işleme ve aktarım faaliyetinde bulunan veri sorumlularının bu kapsamda kurulmuş veri sorumluları siciline kayıt olma ve veri işleme ve aktarım faaliyetlerini bildirme yükümlülüğü bulunmaktadır. Kurum tarafından Veri Sorumluları Sicil Bilgi Sistemi ("VERBİS") adıyla kurulan bu sicile veri sorumluların atayacakları bir irtibat kişisi ve/veya veri sorumlusu temsilcisi ile

[115] Dülger, s.25.

kaydolması ve kişisel veri işleme ve aktarım faaliyetlerine ilişkin VERBİS üzerinden talep edilen gerekli bilgileri bildirmesi Türkiye'de kurulu olsun ya da olmasın Türkiye'de veri işleme faaliyeti gerçekleştiren her bir veri sorumlusu için bir şarttır[116]. Bu sistemin kuruluş amacı, veri sorumlularının kim olduğunu, hangi tür verileri, hangi amaçlarla ve hangi faaliyetleri süresince işlediklerini, bu verileri hangi ortamlarda ve ne kadar süreyle sakladıklarını, üçüncü kişilere aktarıp aktarmadıklarını ve aktarımda bulunmaları halinde hangi amaçla ve kimlere yönelik aktarımda bulunduklarını ve işlenen ve aktarıma tabi tutulan kişisel verilerin korunması ve gizliliğin sağlanması için almış oldukları tedbirlerin neler olduğunu kamuya açıklamak ve dolayısıyla kişisel verilerin korunması alanında aleni, takip edilebilir ve sürdürülebilir bir sistem yaratmaktır[117]. Şirketler topluluğu dahilinde veri sorumlusu olarak Türkiye'de veri işleme ve aktarım faaliyeti gerçekleştiren her bir grup üyesi şirketin de merkezi Türkiye'de bulunsun ya da bulunmasın VERBİS'e kayıt ve bildirim yükümlülüğü bulunmaktadır. Aksi halde zamanında ve gereğine uygun bir şekilde VERBİS kaydını yerine getirmeyen veri sorumluları için KVKK m.18 uyarınca Kurul tarafından 1.000.000 TL'ye varan idari para cezalarına hükmedilebilmektedir.

Grup üyesi şirketin yabancı bir ülkede kurulmuş olmasının VERBİS yükümlülüğünü ortadan kaldırmayacağının unutulmaması gerekmektedir[118]. Bununla birlikte Kurul 23 Haziran 2019 tarihinde 2019/225 sayılı kararında yurt dışında kurulu olan ancak Türkiye'de açtığı bir şubesi ile faaliyet gösteren şirketlerin TTK m.40 uyarınca Türkiye'de tescil edilen şubeleri için de VERBİS'e kayıt yükümlülüğü getirmektedir. Bu kapsamda grup üyesi şirketlerin Türkiye'de doğrudan bir bağlı şirketi olsun ya da olmasın bir şube aracılığıyla veri işleme faaliyeti gerçekleştirmesi halinde şubesinin VERBİS'e kaydolmasına dair gerekli işlemleri yerine getirmesi gerekmektedir. Görüldüğü gibi Kurul, yürüttüğü veri

[116] Çekin, s.121
[117] Kişisel Verileri Koruma Kurumu, Veri Sorumluları Sicili Nedir? https://www.kvkk.gov.tr/Icerik/2043/Veri-Sorumluları-Sicili-Nedir? Erişim Tarihi: 30.11.2021.
[118] Sevgi Erarslan, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, s.133

işleme faaliyetlerinin mahiyetine binaen yabancı şirketlerin Türkiye'deki şubelerini de TTK uyarınca bir tüzel kişilik arz etmeseler de veri sorumlusu olarak addetmekte ve yabancı şirketin Türkiye'deki faaliyetlerini kontrol altına alma yoluna gitmektedir. Bu bakımdan yabancı şirketlerin şubelerinin de Tüzük ile uyumlu olarak yabancı şirketin Türkiye'deki grup üyesi şirketi olarak ele alındığını söylemek yanlış olmayacaktır. Öyle ki Tüzük AB dışında kurulmuş yabancı bir şirketin AB'de bulunan şubesinin faaliyetleri çerçevesinde veri işleme ve aktarım faaliyetleri gerçekleştirmesi Tüzük hükümlerine tabi olması gerektiğini belirtmekte ve bu noktada AB'de kurulmuş bir işletme ile AB dışında üçüncü bir ülkede kurulmuş veri sorumlusunun veri işleme faaliyetleri arasında açık bir bağ bulunduğunun saptanması durumunda AB dışında kurulmuş olan veri sorumlusunun Tüzük hükümlerine tabi olacağını ifade etmektedir. Öte yandan AB dışında kurulmuş olan şirketlerin, veri sorumlusu (veri kontrolörü) veya veri işleyen olarak Tüzük'e tabi olmasına ilişkin olarak Tüzük m.3/1 uyarınca yer verilen "işletme" kavramı da Tüzük'ün AB dışındaki yabancı veri sorumlusu/veri işleyen bir şirketin, girişimin ya da oluşumun AB sınırları içerisinde kurulmuş olan işletmesi aracılığıyla ve bu işletmenin faaliyetleri çerçevesinde Tüzük hükümlerine tabi olması gerektiğini sonucunu doğurmaktadır. Diğer taraftan Kurul söz konusu kararında yabancı şirketlerin Türkiye'de kurdukları irtibat bürolarının herhangi bir ticari faaliyet yürütmediklerinden hareketle VERBİS'e kayıtla yükümlü olmadıklarını belirtmiştir.

VERBİS'e kayıt esasında kamuya açıklık ilkesine dayandığından ilgili kişilerin bu kayıtlar sayesinde grup üyesi şirket tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin ayrıntılarına dair bilgi etme ve gerekli kontrolleri sağlama imkânı bulunmaktadır. Ayrıca bu kayıtların yabancı bir şirketin Türkiye'de gerçekleştirdiği kişisel veri işleme faaliyetlerinin mahiyetinin anlaşılabilmesi ve olası bir veri ihlali halinde Kurul tarafından sürece daha hızlı bir şekilde müdahale edilebilmesi amaçlanmaktadır[119]. İlgili kişilere sağladığı bu yararın yanı sıra özellikle

[119] Dilşat Yılmaz, Yeni Bir İdari Faaliyet Alanı: "VERBİS" (Veri Sorumluları Sicil Bilgi Sistemi), s.25.

Türkiye'ye veri aktaran ve Türkiye'de veri işleme faaliyeti gerçekleştiren çok uluslu grup şirketler için de topluluk içerisindeki kişisel verilerin işlenmesinde şeffaflığın sağlanması ve bu sayede topluluk içi denetimin kolaylaşması, kişisel verilerin gelişigüzel işlenmesinin önüne geçilerek bu alanda veri sorumlusu olan diğer grup üyesi şirketlerin olası bir veri ihlali ya da hukuka aykırı bir veri işleme faaliyeti sebebiyle yaptırıma tabi tutulma riskinin indirgenmesi, kişisel veri işlemesi faaliyetlerinin topluluk dahilinde disiplin altına alınmasının sağlanması, veri sorumlusu grup üyesi şirketin kişisel verisini işlediği ilgili kişilere hesap verebilirliğinin artırılması, veri sorumlusu grup üyesi şirketin KVKK ve alt mevzuatına uyumunun kolaylaşması gibi grup üyesi şirket ve toplulukta bulunan diğer grup şirketler için de faydaları bulunmaktadır. Ayrıca grup üyesi şirketler arasında gerçekleştirilecek kişisel veri aktarımları için hazırlanacak bağlayıcı şirket kurallarının getirdiği şartların sağlanması adına da VERBİS kaydının tamamlanmış olması grup üyesi şirketlerce Kurul'a yapılacak izin başvurularında kolaylık sağlayabilecektir.

Veri işleyen sıfatıyla şirketin gerçekleştirebileceği faaliyetlere geçmeden önce veri sorumlusu sıfatıyla ilgili olarak belirtmemiz gereken son bir husus da veri sorumlusu ile veri işleyen arasındaki sorumluluk ilişkisi ve görev dağılımıdır. KVKK ve alt mevzuattaki pek çok yükümlülüğün muhatabı belirttiğimiz üzere veri sorumlusu şirket iken, veri işleyenin sorumluluk sahası veri sorumlusu şirkete nazaran daha sınırlıdır[120]. Veri sorumlusu veri işleyen ile akdedeceği bir sözleşme ile veri işleyenin teknik olarak imkanlarının daha gelişmiş olmasına istinaden veri işlemeye ve aktarımına ilişkin belirli hususlarda karar verme yetkisini veri işleyene aktarabilir[121]. Bu durumlarda veri sorumlusunun çalışacağı veri işleyeni büyük bir dikkatle seçmesi ve veri işleme ve aktarım faaliyetlerinin veri işleyen vasıtasıyla gerçekleşeceği durumlarda sürekli olan veri işleyeni denetim ve gözetim altında tutması önem arz etmektedir. Aksi halde veri işleyen tarafından gerçekleştirilen

[120] Gamze Turan Başara, '' Kişisel Veri İşleme Sözleşmesi'', s.21
[121] MEMİŞ, Tekin, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, C. 3, S. 6, Y. 2017, s. 23

hukuka aykırı bir veri işleme ve aktarım faaliyeti ya da bu faaliyetlerin hukuka uygunluğunun sağlanması adına alınacak bir güvenlik tedbirinin eksikliği veri sorumlusu için gerek ilgili kişiler gerekse Kurul nezdinde çeşitli yaptırım risklerine maruz kalmasına sebep olabilecektir.

Türkiye'de faaliyet gösteren veri sorumlusu bir grup üyesi şirketin pazarlama faaliyetlerine ilişkin yapacağı analiz ve anket çalışmaları için bir veri işleyen şirket ile çalışması ve pazarlama faaliyetleri kapsamında işlenecek verilerin ve yapılacak anket araçlarının veri işleyen tarafından kararlaştırmasına onay vermesi halinde kişisel veri işleme ve elde etme yöntemleri hususunda veri işleyene yetki devrinde bulunmuş olacaktır. Diğer taraftan grup üyesi şirketin bulut hizmeti sunan bir şirkete grup şirketin sorumluluğunda olan kişisel verilerin saklanması ve depolanması için yetki vermesi halinde yine veri sorumlusu grup üyesi şirket tarafından veri işleyen şirkete kişisel verilerin hangi yöntemle saklanacağı hususunda bir yetki devri yapılmış olacaktır[122]. Öte yandan grup üyesi şirketin veri güvenliğini sağlamak adına sızma testi gibi belirli teknik tedbirleri almak adına çalıştığı teknoloji şirketini kişisel verilerin korunması için hangi metotların kullanılacağı ve tedbirlerin alınacağı hususunda yetkilendirdiği kabul edilecektir. Tüm bu örneklerde görüldüğü gibi veri sorumlusu şirketin veri işleyen ile söz konusu kişisel veri işleme ve aktarım faaliyeti özelinde bir görev ve yetki dağılımına gitmesi mümkündür[123]. Bu durumlarda veri sorumlusunun kişisel verilerin korunmasına dair sorumluluğunu bir arada çalıştığı veri işleyen ile paylaştığı kabul edilir. Söz konusu görev ve yetki dağılımı ile sorumluluğun paylaşımı genellikle veri sorumlusunun veri işleyen ile aralarında akdedecekleri veri işleme e aktarım sözleşmelerinde detaylı olarak düzenlenebilmektedir. Ancak böyle bir sözleşmesel düzenlemenin bulunmaması halinde veri sorumlusu ve veri işleyen arasında kanunen geçerli olacak bir sorumluluk düzeni ortaya çıkacaktır ve

[122] Memiş, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, C. 3, S. 6, Y. 2017, s. 32.
[123] Gamze Turan Başara, '' Kişisel Veri İşleme Sözleşmesi'', s.25

veri işleyen kendisine atfedilebildiği oranda veri işleme ve aktarım faaliyetine ilişkin ortaya çıkan hukuka aykırılıktan dolayı sorumlu olacaktır[124].

Veri sorumlusu sıfatıyla grup üyesi şirketin veri işleme ve aktarım faaliyetine ilişkin görev ve yetkilerini belirli durumlarda aynı gruptaki diğer bir grup üyesi şirkete devretmesi de mümkündür. Böyle bir durumda aynı grup içerisindeki şirketler arasında veri sorumlusu ve veri işleyen ilişkisi gündeme gelecektir. Uygulamada özellikle hâkim şirketlerin bağlı şirketleri aracılığıyla yürüttükleri ticari faaliyetleri sırasında bağlı şirketlere verdiği talimatlar uyarınca veri işleme faaliyeti gerçekleştirdiği görülmektedir. Ancak hâkim şirketin veri sorumlusu bağlı şirketin ise veri işleyen olacağı yönünde genel bir tanımdan bahsetmek mümkün olmayacaktır. Şirketler topluluğu bünyesindeki hâkim ve bağlı şirketler arasındaki veri sorumlusu ve veri işleyen sıfatları gerçekleşecek veri işleme ve aktarım faaliyetine bağlı olarak belirlenmeli ve çok uluslu grup şirketler arasındaki kişisel veri aktarımının hukuka uygunluğunun sağlanması adına veri sorumlusu ve veri işleyen arasında imzalanacak taahhütname ve varsa bağlayıcı şirket kurallarında da bu ilişkinin açık bir şekilde ortaya konması gerekmektedir.

2.1.2. Veri İşleyen Grup Şirket

KVKK m.3/1 (ğ) uyarınca veri işleyen, veri sorumlusunun devrettiği yetkiye istinaden veri sorumlusunun namına kişisel veri işleme faaliyetinde bulunan gerçek veya tüzel kişidir[125]. Veri işleyen tüzel veya gerçek kişi, ticari ve hukuki bir yapı olarak veri sorumlusundan bağımsız bir kişilik olsa da veri işleme ve aktarım faaliyetleri ve veri sorumlusu ile arasındaki denetim ve talimat ilişkisi itibariyle veri sorumlusundan tamamen bağımsız değildir ve veri sorumlusunun talimatları içerisinde ve veri sorumlusunun verdiği yetkiyle istinaden söz konusu veri işleme ve aktarım faaliyetini gerçekleştirmektedir. Veri işleyen şirket, çoğu zaman veri sorumlusu şirketin menfaatlerini gerçekleştirmek ve veri sorumlusu tarafından

[124] Küzeci, s.45
[125] Memiş, s.7

belirtilen amaçların yerine getirilmesi için veri işleme ve aktarım faaliyetleri göstermektedir, bu sebeple veri işleyenler aksi kararlaştırılmadıkça veri sorumlusundan bağımsız şekilde karar verme yetkisine sahip değildir[126]. Ancak yukarıda da belirttiğimiz üzere veri sorumlusunun menfaatini gerçekleştirmek için veri işleme ve aktarım faaliyetlerinde bulunurken belirli durumlarda veri işleyen şirketler işlenen kişisel verilerin saklanması, imhası ve hatta üçüncü kişilere aktarılması gibi veri işlemenin teknik detaylarına ilişkin söz hakkı sahibi olurlar[127]. Öyle ki veri işleyen, her ne kadar veri sorumlusunun emir ve talimatları doğrultusunda hareket etse de veri sorumlusunun menfaatini gerçekleştirmek için gerekli olan veri akışını ve hareketliliği belirleme konusunda kendi içinde bir özerkliğe sahiptir ve veri işleme amaçlarını aşmaksızın belirli veri işleme ve aktarım faaliyetleri gerçekleştirebilirler.

Örneğin bir insan kaynakları veya muhasebe programı geliştiren ve bu programı müşterilerine satan şirket, müşterilerine sunduğu hizmet kapsamında bu program üzerinden işledikleri ve sakladıkları müşteri verileri için müşterilerinin veri işleyeni sıfatıyla hareket ederler. Ancak söz konusu hizmet veren şirketin müşterilerinin hizmetten beklediği azami faydayı sağlamaları adına alt veri işleyen sıfatıyla hareket eden üçüncü kişi hizmet sağlayıcı şirketler ile çalışması da mümkündür. Bu durumda veri işleyen olarak hizmet veren şirketin programın teknik ihtiyaçlarının giderilmesi, düzenli olarak bakım ve onarımlarının yapılması, güncelleme, yedekleme, bulut hizmeti, barındırma gibi hizmetlerin alınması konularda üçüncü kişilerle kendi takdiri üzerine ticari bir ilişkiye girmesi gündeme gelebilir. Böyle bir durumda hizmet veren yazılım şirketinin yazılımın daha iyi çalışması ve müşterilerine yönelik taahhüt ettiği kesintisiz hizmeti sunabilmesi adına doğrudan ya da dolaylı olarak üçüncü kişi hizmet sağlayıcı şirketlere müşterisinin bu yönde açık ve yazılı bir talimatı olmasa da kişisel veri aktarımında bulunması gündeme gelebilecektir. Görüldüğü üzere her ne kadar veri işleyen, veri sorumlusunun talimatlarıyla hareket etse de ve bunun ötesinde bir veri işleme faaliyeti

[126] Aşıkoğlu, s.73.
[127] Küzeci, s.32

gerçekleştirmemekle yükümlü olsa da burada asıl hareket noktasının veri işleyenin veri sorumlusunun menfaatine aykırı olacak ve işleme amacını aşan bir veri işleme ve aktarım faaliyeti gerçekleştirmemesidir[128].

Yukarıda da belirttiğimiz üzere şirketler topluluğu bünyesinde belirli grup üyesi şirketlerin veri sorumlusu olan diğer grup üyesi şirketlerinin veri işleyeni olarak faaliyet göstermesi mümkündür. Öyle ki bir holding şirketin pay sahibi olduğu bağlı şirketinin yönetim kurulunda kararlar alınırken bağlı şirketin ticari faaliyetlerine ilişkin verilen kararların holding şirket lehine oy çokluğuyla alınmasını sağlaması ve bağlı şirketlerin bu kararlar doğrultusunda holding şirket adına ve lehine yürüttüğü faaliyetlerde veri işleyen sıfatıyla hareket etmesi gündeme gelebilir. Örneğin hakim şirketin müşterisiyle imzalayacağı hizmet sözleşmesine kendisinin taraf olmasına rağmen bu sözleşme uyarınca verilecek hizmeti bağlı şirketi üzerinden müşterilerine sunması halinde de bağlı şirket hakim şirketin verdiği yetki ile ve söz konusu hizmet sözleşmesi tahtında hakim şirketin üstlendiği yükümlülüklerin yerine getirilmesi için bağlı şirkete verdiği talimatlar uyarınca veri işleme ve aktarım faaliyetleri gerçekleştirecek ise bu durumda da bağlı şirket veri işleyen ve hakim şirket ise veri sorumlusu olarak hareket etmiş olacaktır. Grup üyesi şirketlerden bazılarının faal bir şekilde çalışmaması ve olarak ticari faaliyet göstermemesi ancak diğer grup üyesi şirketler için işe alım faaliyetleri yürütmesi halinde de insan kaynakları işlerini yürüterek diğer grup üyesi şirketler için istihdam olanağı sağlayan grup üyesi şirketin işveren sıfatıyla hareket eden veri sorumlusu şirketlerin veri işleyeni olarak faaliyet gösterdiği belirtilebilecektir. Diğer taraftan söz konusu grup üyesi şirketin herhangi bir ticari faaliyet yürütmeksizin yalnızca şirketler topluluğuna ait yazılım ve donanımların sunucularının bulunduğu ve diğer grup üyesi şirketler için bir barındırma şirketi olarak kullanılması halinde de bu şirketin diğer grup üyesi şirketlerin saklama faaliyetlerinin yürütülmesinde yetkili veri işleyen şirket olarak kabul edilmesi mümkündür. Bu durumlardan ilkinde topluluğun insan kaynakları hizmetlerini

[128] Gamze Turan Başara, '' Kişisel Veri İşleme Sözleşmesi'', s.27

yürüterek işe alım işlemleri ile ilgili veri işleyen ve bulduğu personel adayların diğer grup üyesi şirketler nezdinde istihdam edilmesini sağlayan grup üyesi şirketin işveren olarak hareket eden grup üyesi şirketler karşısında bu şirketlerin veri işleyeni olarak kişisel veri işleme ve aktarım faaliyetleri yürüttüğünü ifade etmek ve ikinci örnekte ise yazılım ve donanımların sunucularının barındırıldığı ve yalnızca topluluğa ait kayıtların saklanması ve arşiv hizmetlerinin verilmesi ile sınırlı faaliyet yürüten grup üyesi şirketin de yine bu faaliyetleri özelinde diğer grup üyesi şirketlere karşı veri işleyen olarak hareket ettiği belirtmek yanlış olmayacaktır.

Şirket topluluğunda yer alan grup şirketlerin belirli konularda birbirilerinden hizmet alması halinde bazı grup şirketlerin veri sorumlusu grup üyesi şirketlere karşı veri işleyen olarak veri işleme ve aktarım faaliyetlerinde bulunacağını belirttik. Bununla birlikte grup içi hizmet tedarikinin yanı sıra grup üyesi şirketlerin grup üyesi olmayan topluluk dışından bir hizmet sağlayıcı ile anlaşarak hizmet alımı gerçekleştirmesi uygulamada daha çok karşılaşılan hizmet ilişkileridir. Grup üyesi şirkete hizmet veren şirketlerin grup dışından bağımsız bir şirket olması halinde hizmet sağlayan şirketin hizmet ilişkisi kapsamında veri sorumlusu grup üyesi şirketin veri işleyeni olarak değerlendirilmesi mümkün olacaktır. Örneğin grup üyesi şirketlerin istihdam ettiği çalışanlarına yönelik özel sağlık sigortası yapan sigorta şirketi sigortacılık faaliyetleri için işlemiş olduğu grup üyesi şirket çalışanlarının kişisel verileri karşısında veri işleyen sıfatını haizdir. Diğer taraftan grup üyesi şirketin çalışanların ücretlerinin hesaplanması ve grup şirkete ilişkin diğer muhasebesel işlemlerin yürütülmesi için grup üyesi şirkete hizmet veren mali müşavirlik şirketi veya bağımsız denetim şirketi ya da bordrolama şirketi de ilgili grup üyesi şirketin hizmet sağlayıcıları olarak veri işleyen olarak hareket etmektedir. Öte yandan grup şirketin diğer grup şirketler ile arasındaki uyuşmazlıkların çözümü ve sözleşmelerinin incelenmesi için gerek hukuki gerekse teknik konularda hizmet aldığı avukatları ve danışmanlar da yine grup üyesi şirketin belirlediği amaçlar doğrultusunda ve grup üyesi şirketin menfaatleri ve talimatları doğrultusunda veri işleme ve aktarım faaliyetleri gerçekleştireceğinden grup üyesi

şirketin veri işleyeni olarak kabul edilebilecektir. Bununla birlikte bir veri sorumlusunun aynı ya da farklı konuda birden fazla veri işleyen ile çalışması ya da bir veri işleyenin de aynı veya farklı bir konuda birden fazla veri sorumlusu adına veri işleme faaliyeti gerçekleştirmesi mümkündür[129]. Örneğin X A.Ş.'nin çalışanlarına ilişkin özel sağlık sigortası işlemlerini yürüten sigorta şirketinin aynı şekilde Y A.Ş.'nin de çalışanları için de sigortacılık hizmeti vermesi halinde, sigorta şirketi veri sorumlusu sıfatını haiz hem X A.Ş. hem de Y A.Ş. için veri işleyen sıfatıyla hareket etmiş olacaktır.

Yukarıda da belirttiğimiz gibi veri sorumlusu şirketin kişisel verilerin toplanacağı, aktarılacağı ve saklanacağı yöntemler ile kişisel verilerin korunması için alınması gereken güvenlik tedbirlerinin belirlenmesi, kanuni sınırlar içinde kişisel verilerin hangi süreyle saklanacağı, kişisel verilerin silinmesi, anonim hale getirilmesi, yok edilmesi teknik işlemlerin yürütülmesi gibi konularda veri işleyen şirkete veri sorumlusu olmasından doğan belirli yetkilerini devredebilmektedir[130]. Ancak veri sorumlusunun veri işleyene yönelik bu yönde yapacağı bir yetki devri işlemi yasal olarak veri sorumlusunun veri işleyene devrettiği konulardaki sorumluluğunun ortadan kaldırmamakla birlikte söz konusu yetki devri, veri sorumlusunun yasal sorumluluklarının da devri anlamına gelmemektedir. Veri sorumlusu daha iyi hizmet kalitesine sahip ve teknolojik olarak belirli faaliyetleri gerçekleştirmeye yetkin olan bir veri işleyen şirkete veri sorumlusu olduğu kişisel verilerin saklanması gibi belirli konularda yetki devrinde bulunsa da veri işleyen tarafından KVKK ve alt mevzuat hükümleri uyarınca bu verilerin korunması için gerekli olan

[129]Memiş, s.15.

[130] İlke Gürsel, İşçinin Kişisel Verilerinin Korunması Hakkı, Ankara: Adalet Yayınevi, 2016, s. 135. Kurum tarafından hazırlanan rehberde veri sorumlusunun veri işleyene devredebileceği yetkiler örnek niteliğinde sayılmıştır. Buna göre, "kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı, kişisel verilerin hangi yöntemle saklanacağı, kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları, kişisel verilerin aktarımının hangi yöntemle yapılacağı, kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot ve kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri" devredilebilecek yetkilerdendir (Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi, s. 57, https://www.kvkk. gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF, Erişim: 20.09.2020).

yeterli güvenlik tedbirinin alınmaması sebebiyle ortaya çıkabilecek zararlardan dolayı veri sorumlusunun hukuki sorumluluğu devam edecektir. Ancak böyle bir durumda veri işleyenin gereken teknik tedbirleri almaması vb. gibi kendisine atfedilebilecek bir sebeple zararın ortaya çıkmasına neden olmuşsa veri sorumlusu ile birlikte sorumluluğu gündeme gelecektir. Öyle ki bu atfedilebilirlik veri işleyenin veri sorumlusunun verdiği yetkiye dayanarak gerçekleştirdiği veri işleme faaliyetiyle bu faaliyet sonucu ortaya çıkan zarar arasında bir illiyet bağının bulunmasına bağlıdır[131]. KVKK m. 12/2'de de "Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur." hükmüne yer verilerek kişisel verilerinin bir veri işleyen aracılığıyla işlenmesi halinde veri işleyenin aktif ya da pasif bir hareketinden dolayı alınması gereken bir veri güvenliğinin eksikliğinden ya da uygunsuzluğundan kaynaklı olarak herhangi bir zararın ortaya çıkması halinde hakları ihlal edilen ilgili kişilerin tazmin edilmesi hususunda hem veri sorumlusu hem de veri işleyen yasal olarak birlikte sorumlu tutulacaktır. Bununla birlikte veri işleyen ile veri sorumlusunun kendi aralarında sorumluluk ilişkini ile sorumluluğun sınırlarını ve görev ve yetkilerini belirleyen bir veri işleme ve aktarım sözleşmesi ya da protokolü imzalamaları da mümkündür[132]. Ancak böyle bir sözleşmesel düzenlemeye dayanarak veri işleyen tarafından yeterli güvenlik tedbirinin alınmaması sebebiyle zarara uğrayan kişisel veri sahibi ilgili kişilerin veri sorumlusuna başvurması halinde veri sorumlusunun bu başvuruyu reddetmesi ve ilgili kişileri veri işleyene yönlendirmesi hukuken geçerli olmayacak ve söz konusu sözleşmesel düzenleme yalnızca veri sorumlusu ile veri işleyen arasındaki rücu ilişkisinde uygulama alanı bulacaktır.

Bununla birlikte veri işleyenin davranışı ile meydana gelen zarar arasında illiyet bağının kesilmesine yol açan sebepler kişisel veri işleme faaliyetinden doğan

[131] İlliyet bağı hakkında ayrıntılı bilgi için bkz. Fikret EREN, Sorumluluk Hukuku Açısından Uygun İlliyet Bağı Teorisi, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1975, s. 51 vd.
[132] Aşıkoğlu, s.73.

aykırılık sebebiyle gündeme gelecek sorumluluk bakımından da geçerli olacaktır. Buna göre veri işleyenin öngörülemediği ya da öngörse de önleyemediği mücbir sebeplerden birinin vuku bulması ya da söz konusu veri işleme faaliyetinden zarar görenin bizzat ağır kusurunun bulunması ya da veri işleyen ve ilgili kişiden farklı olarak üçüncü bir kişinin ağır kusurunun bulunması halinde illiyet bağını kesen olaylar olarak kabul edilecektir[133]. Örneğin kişisel veri işleme ve aktarım sözleşmesi uyarınca kişisel verileri yedeklemeyi üstlenen bulut şirketinin sunucularının bir siber saldırı sebebiyle bloke olması ve bu sebeple veri sorumlusu şirketin kişisel verilerinin yer aldığı bulut havuzuna erişimin mümkün olmaması halinde bir üçüncü kişinin ağır kusuru bulunduğundan somut olayın şartlarına göre hayatın olağan şartlarına uygun olarak bu durumun veri işleyenin almadığı bir veri güvenliği tedbirinden dolayı ileri gelmesini söylemek zor ise bu sebeple ortaya çıkan zarardan veri işleyenin sorumlu olmaması gündeme gelebilecektir.

Son olarak grup üyesi şirketler arasındaki kişisel veri aktarımlarının hukuka uygun bir zeminde gerçekleşmesi için hazırlanan taahhütnameler ve bağlayıcı şirket kurallarının daha basit bir görünümü olan veri sorumlusu ve veri işleyen arasındaki veri işleme ve aktarım sözleşmelerinin hukuki niteliğinden bahsetmek de faydalı olacaktır. Kişisel veri işleme ve aktarım sözleşmesi veri sorumlusu ve veri işleyen arasında imzalanabileceği gibi iki veri sorumlusu arasında da imzalanabilecektir. Bununla birlikte bu sözleşmelerin ikiden daha fazla tarafın katılacağı sözleşmeler olarak akdedilmesi önünde de herhangi bir engel bulunmamaktadır. Kişisel veri işleme ve aktarımı sözleşmesi TBK kapsamında akdedilen bir sözleşme gibi tarafların karşılıklı ve birbirine uygun irade beyanlarıyla kurulan ve taraflar bakımından gerek borçlandırıcı gerekse tasarruf etkisi doğuran özel bir sözleşmedir. KVKK'da kişisel veri işleme ve aktarım sözleşmesinin tanımına yer verilmemiştir, ayrıca TBK ya da başka bir kanunda da veri işleme ve aktarım sözleşmeleri tüm unsurlarıyla düzenlenmediği için bu sözleşmelere isimsiz (atipik)

[133] İlliyet bağı hakkında ayrıntılı bilgi için bkz. Fikret EREN, Sorumluluk Hukuku Açısından Uygun İlliyet Bağı Teorisi, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1975, s. 51 vd.

bir sözleşme olarak denilebilecektir[134]. Kişisel veri işleme ve aktarım sözleşmesinin esaslı unsurlarından biri, veri işleyenin veri sorumlusunun menfaatlerini gözetecek şekilde ve veri sorumlusunun verdiği talimatlara uygun olarak kişisel verilerin işlenmesi borcunu üstlenmesidir. Bu noktada kişisel veri işleme ve aktarım sözleşmesinin esasında bir vekalet sözleşmesine ilişkin temel unsurları içerdiğini belirtmek yanlış olmayacaktır. Tıpkı vekalet sözleşmesinde olduğu gibi veri işleme ve aktarım sözleşmesinde de veri işleyen olarak taraflardan biri veri sorumlusu olan diğer tarafın menfaatine ve talimatlarına uygun olarak bir iş görme borcunu üstlenmekte ve taraflar arasında bir güven ilişkisi tesis edilmektedir. Öte yandan doktrinde bir görüş ise veri işleyenin veri sorumlusuna esasında doğrudan ve salt veri işleme ve aktarım fiilini değil, işleme ve aktarım sonucunda meydana gelen çıktıyı taahhüt ettiğini taraflar arasında bu yönüyle eser sözleşmesine benzer ilişki olduğunu savunmaktadır[135]. Bu haliyle farklı sözleşme türlerine ilişkin unsurlar ihtiva ettiğinden dolayı veri işleme ve aktarım sözleşmesinin isimsiz ve karma nitelikte bir sözleşme olduğu kabul edilebilecektir. TBK m. 502/2 uyarınca vekalete ilişkin hükümlerin somut olayın şartlarına uygun düştüğü ölçüde TBK'da düzenleme altına alınmayan diğer iş görme sözleşmeleri için de uygulama alanı bulacağı hüküm altına alınmıştır. Bu düzenleme ışığında isimsiz ve karma bir sözleşme olarak kabul edilebilecek kişisel veri işleme ve aktarım sözleşmesine KVKK ve alt mevzuat hükümlerinin yanı sıra TBK'daki vekalet sözleşmesine ilişkin hükümler de uygulanabilecektir[136].

Gerçekten de veri işleyenin veri sorumlusunun verdiği yetkiye dayanarak gerçekleştireceği veri işleme faaliyetlerinde yerine getirmesi gereken özen yükümlülüğü[137], veri sorumlusunun talimatlarına uyma ve kusuruyla sebep olduğu

[134] Aynı yönde bkz. Taştan, Kişisel Verilerin Korunması, s. 121.
[135] Taştan, Kişisel Verilerin Korunması, s. 121.
[136] Sonuç borcuna ilişkin edime ise niteliğine uygun düştüğü ölçüde eser sözleşmesine ilişkin hükümler uygulanacaktır.
[137] Vekilin özen borcunun belirlenmesinde mesleki bilgi ve tecrübesinin de dikkate alınması gerektiği kabul edilmektedir (Bkz. EREN, Özel Hükümler, s. 742; Özen Başpınar, s. 163; Tandoğan, C. II, s. 410-411; AYDOĞDU ve KAHVECİ, Özel Borç İlişkileri, s. 799; Gümüş, C. II, s. 153; Weber, BSK OR, Art. 398, N. 28; Fellmann, BK OR, Art. 398, N. 358).

zararları tazmin etme yükümlülüğü [138], sadakat ve gözetim yükümlülüğü[139], hesap verme yükümlülüğü[140], kayıt tutma[141] ve veri işleme ve aktarım faaliyeti sonrasında talep halinde çıktıları veri sorumlusuna iade etme[142] yükümlülükleri göz önünde bulundurulduğunda taraflar arasında vekalet ilişkisine benzer bir yapının ortaya çıktığı söylenebilecektir. Bu kapsamda söz konusu yükümlülüklerin her birinin esasında grup şirketler arasında gerçekleşecek kişisel veri aktarımlarında veri sorumlusu ve veri işleyen olarak hareket edecek her bir grup üyesi şirket tarafından taahhüt edilmesi ve bu aktarımın hukuka uygunluğunu sağlamak adına hazırlayarak Kurul'un onayına sunacakları bağlayıcı şirket kurallarının unsurlarıyla doğrudan bağlantılı olduğu görülmektedir.

2.2. Grup Şirketler Arasındaki Kişisel Veri Aktarımları

Yukarıda aynı şirketler topluluğu dahilindeki birden fazla grup şirket arasında gerçekleşen kişisel veri aktarımlarının KVKK ve alt mevzuat hükümleri uyarınca üçüncü kişiye veri aktarımı olarak kabul edileceğini ve bu aktarımın alıcı sıfatını haiz grup üyesi şirketin Türkiye'de ya da Türkiye dışında kurulu olması halinde KVKK m.8'de düzenlenen yurt içine aktarım ya da KVKK m.9'da düzenlenen yurt dışına aktarım şartlarına tabi olacağını belirtmiştik. KVKK m.9 uyarınca gerçekleşen kişisel veri aktarımlarının tarafı olan çok uluslu grup şirketler, gerek hukuki gerekse iktisadi olarak birbirleriyle bağımlı bir ilişki içerisinde hareket eden

[138] Taştan, Kişisel Verilerin Korunması, s. 139.
[139] Vekilin sadakat yükümlülüğü hakkında bkz. Yavuz, Acar ve Özen, Özel Hükümler, s. 1204 vd.; Kılıçoğlu, Özel Hükümler, s. 544; Tandoğan, C. II, s. 407 vd.; Eren, Özel Hükümler, s. 744; Fellmann, BK OR, Art. 398, N. 23; Weber, BSK OR, Art. 398, N. 8 vd.
[140] Vekalet sözleşmesinde hesap verme yükümlülüğü hakkında ayrıntılı bilgi için bkz. Eren, Özel Hükümler, s. 746 vd.; Yavuz, Acar ve Özen, Özel Hükümler, s. 1207 vd.; Tandoğan, C. II, s. 479 vd.; Aydoğdu ve Kahveci, Özel Borç İlişkileri, s. 801; Gümüş,
C. II, s. 169; Aral ve Ayrancı, Özel Borç İlişkileri, s. 455; Zevkliler ve Gökyayla, Özel Borç İlişkileri, s. 623; Weber, BSK OR, Art. 400, N. 3 vd.; Fellmann, BK OR, Art. 400, N. 7 vd.
[141] TAŞTAN, Kişisel Verilerin Korunması, s. 144.
[142] TAŞTAN, Kişisel Verilerin Korunması, s. 139.

oluşumlardır. Bu bağımlı nitelikleri gereği her biri arasında yönetsel, mali, ticari, hukuki ve vergisel pek çok konuda sürekli bir bilgi alışverişi gerçekleşir[143].

TTK uyarınca hakim ve bağlı şirkete yüklenen bildirim[144], tescil ve ilan yükümlülüklerinin yerine getirilmesi, hakim şirket ve bağlı şirket tarafından yıllık olarak faaliyet, bağlılık ve denetim raporlarının düzenlenmesi[145], hakim şirketin bağlı şirket aracılığıyla kredi alma, teminat gösterme, kefil olma vb. gibi hukuki işlemler gerçekleştirmesi, bu işlemlerin bağlı şirketin menfaatlerine halel getirmemesi için hakim şirket tarafından gerekli önlemlerin alınması, bu işlemlerden dolayı hakim şirketin hakimiyet ilişkisini kötüye kullandığının ortaya çıkması halinde bağlı şirketin uğradığı zarara karşılık hakim şirket tarafından bir denkleştirme yoluna gidilmesi, hakim şirketin ve bağlı şirketin yönetim kurulu üyeleri ile pay sahiplerinin hakim şirket ve bağlı şirket ya da bağlı şirketler arasında yapılan işlemler hakkında bilgi talep etmesi ve bu taleplerin yerine getirilmesi gibi hukuki gereklilikler uyarınca grup üyesi şirketler arasında gerek yurt içinde gerekse yurt dışına kişisel veri aktarımları yapılabilmektedir. Bununla birlikte grup üyesi şirketin diğer bir grup üyesi şirket ile ya da diğer grup üyesi şirketi de etkileyecek şekilde topluluk dışından bir üçüncü kişi ile arasında hissedarlar sözleşmesi, pay devri sözleşmesi, hakimiyet sözleşmesi, distribütörlük sözleşmesi, acentelik sözleşmesi, franchise sözleşmesi, hizmet sözleşmesi, tedarik sözleşmesi, satın alma sözleşmesi, kredi sözleşmesi gibi belirli sözleşmelerin imzalanması ile ticari ilişki içine girilmesi ve bu sözleşmelerden doğan yükümlülüklerini yerine getirilmesi için taraflar gerçekleştirilecek kişisel veri aktarımları da çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına örnek teşkil etmektedir.

Diğer taraftan grup şirketlerin aynı veya farklı ülkelerde gerçekleştirdikleri yatırım, üretim, araştırma ve geliştirme (Ar-Ge), satış, pazarlama, iş geliştirme, insan kaynakları, ihracat, ithalat vb. gibi faaliyetleri süresince de grup üyesi şirketler

[143] Ahmet Kamacı ve Mehmet İnanç Turan, Küreselleşme Sürecinde Çok Uluslu Şirketlerin Ekonomik Açıdan Değerlendirilmesi. Yönetim, Ekonomi, Edebiyat, İslami ve Politik Bilimler Dergisi, s. 81-92.
[144] Detaylı bilgi için bkz. Okutan Nisson s. 189
[145] Detaylı bilgi için bkz. Okutan Nisson s. 32

arasında yürüttükleri faaliyetler ve işlemler ile bağlantılı olarak aralarında kişisel veri aktarımları gündeme gelebilmektedir[146]. Ayrıca topluluk üyeleri arasında ilgili grup şirket(ler)e ilişkin olarak hazırlanan vekaletname, imza sirküleri, yetki belgesi, yönetim/müdürler kurulu kararı, genel/ortaklar kurul toplantı tutanağı, yönetimin atama ve istifasına ilişkin olarak düzenlenen imza beyannamesi, görev kabul beyannamesi, ibra ve istifa mektupları, şirket esas sözleşmesi, yönetim kurulu beyanları, pay senetleri, çek, poliçe, bono, kefaletname, teminat mektubu, mali müşavir raporları, bilanço, gelir-gider ve kar-zarar tablosu ile diğer sicil belgeleri gibi topluluğun ve grup şirketlerin kurumsal belgelerinin hazırlanması, yetkili kişilerce imzalanması ve grup üyesi şirketler arasında paylaşılması halinde de bu belgelerde yer alan pay sahiplerine, yönetim/müdürler kurulu üyelerine, yöneticilere, imza yetkililerine, temsilcilere, vekillere ve ilgili diğer üçüncü kişilere ait kişisel veriler aktarıma tabi tutulmaktadır.

Bununla birlikte grup üyesi şirketlerin çalışanlarına dair özlük dosyalarında tuttukları kimlik, evlilik cüzdanı, ikametgah belgesi, diploma, sertifikalar, askerlik belgesi, sağlık raporları, adli sicil kaydı, iş sağlığı ve güvenliği ile iş kazalarına ilişkin belgeler, fazla çalışma ve görevlendirme belgesi gibi kayıtların toplanması ve bunların çeşitli sebeplerle grup üyesi şirketler arasında paylaşılması durumunda da grup üyesi şirketlerin çalışanlarına dair kişisel veriler gerek yurt içinde gerekse yurt dışına aktarılabilmektedir. Diğer taraftan mülakat ve toplantı notları, çalışanlara dair görev dağılım şemaları, kurumsal politikalar ve planlar, müşteri listeleri, faturalar, irsaliyeler, makbuzlar, protokoller, çizelgeler, mahkeme kararları, dilekçeler, tutanaklar ve e-posta yazışmaları ile kişisel veri içeren diğer her türlü belge, bilgi ve kaydın düzenlenmesi ve grup üyesi şirketler arasında paylaşımı halinde de grup üyesi şirketin çalışanlarına, taşeronlarına, danışmanlarına, müşterilere, tedarikçilere, iş ortaklarına ve ilgili diğer üçüncü kişilere ait kimlik, iletişim, lokasyon, sağlık, cezai mahkumiyet, finans, hukuki işlem, mesleki deneyim vb. pek çok kişisel veri aktarılmaktadır.

[146] Hasan Tağraf, Küreselleşme Süreci ve Çokuluslu İşletmelerin Küreselleşme Sürecine Etkisi, C.Ü. İktisadi ve İdari Bilimler Dergisi, s. 33-47.

Çok uluslu grup şirketler arasındaki kişisel veri aktarımları KVKK uyarınca kişisel verilerin yurt dışına aktarımı olarak kabul edildiğinden bu aktarımların hukuka uygunluklarının sağlanması için KVKK'da düzenlenen işleme ve aktarım şartlarının yerine getirilmesi gerekmektedir[147]. Bu kapsamda Türkiye'de kurulu grup üyesi bir şirketin veri sorumlusu ya da veri işleyen sıfatıyla yurt dışındaki bir grup üyesi şirkete kişisel veri aktarımında bulunması halinde aktarımı yapan Türkiye'deki grup üyesi şirketin KVKK m.9 uyarınca aktarıma tabi tutulacak kişisel verinin ilgili kişilerinden açık rızalarını temin etmesi bu aktarım için bir hukuka uygunluk sebebi teşkil edecektir. Ancak açık rızanın ilgili kişi tarafından zaman geri alınabilir olmasından ve açık rızanın geri alınması halindeyse Türkiye'de kurulu olan ve yurt dışındaki grup üyesi şirkete kişisel veri aktarımında bulunan şirketin açık rıza şartına dayanarak gerçekleştirdiği kişisel veri aktarımına derhal son vermesi gerekmektedir, aksi halde hukuka uygunluk sebebinden yoksun bir aktarım işlemi gündeme geleceğinden bu şekilde yapılan aktarım faaliyeti hukuka aykırı olarak kabul edilecektir. Dolayısıyla yurt dışına yapılacak kişisel veri aktarımlarında açık rıza dışındaki diğer yolların değerlendirilmesi gerekebilir. KVKK m.5/2 veya m.6/3 uyarınca öngörülen hukuka uygunluk şartlarından en az birinin bulunması halinde ilgili kişinin açık rızası olmaksızın Türkiye'deki grup üyesi şirket tarafından aktarımın alıcısı olan yurt dışındaki grup üyesi şirket ile birlikte hazırlayacakları ve imzalayacakları bir veri aktarım taahhütnamesi ile ya da aktarımın tarafı olan tüm grup üyesi şirketlerin bir araya gelerek düzenleyecekleri ve imzalayacakları bağlayıcı şirket kuralları ile Kurul'a yurt dışına veri aktarımı izni başvurusunda bulunmaları alternatif bir yol olarak görülebilir. Ancak Kurul tarafından kendisine sunulan taahhütname başvuruları için şimdiye kadar izin verdiği bilinen oldukça az sayıda şirketin bulunmasından ve hatta bağlayıcı şirket kurallarına ilişkin ise henüz herhangi bir izin kararı yayımlamamış olmasından hareketle bu mekanizmaların kısa vadede Türkiye'den yurt dışına yapılacak kişisel veri aktarımları için bir hukuka uygunluk şartı olarak uygulanabilir olmadığı sonucuna varılabilecektir. Bu sebeple Kurul tarafından 16 Mayıs 2018 ve 10 Nisan

[147] Dülger, GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları, s.4

2020 tarihlerinde yapılan duyurular ile asgari unsurları açılanan taahhütnamelerin ve bağlayıcı şirket kurallarının aktarıma tabi grup üyesi şirketlerce hazırlanarak Kurul'a izin başvurusunda bulunulması sonrasında Kurul'un bu başvuruları onaylayacağı tarihe kadar grup şirketlerin ilgili kişilerden uygun bir şekilde temin etmiş oldukları ve hala geçerli olan açık rıza beyanlarına istinaden yurt dışına kişisel veri aktarımında bulunmaları şimdilik yegâne yol olarak görünmektedir. Bu aktarımlar esnasında Kurul tarafından yapılan başvurulara izin verilmesi için aranan şartlardan biri de aktarımın ilgili kişinin açık rızası dışında KVKK m. 5/2'de ve 6/3'te yer alan veri işleme şartlarını taşıyıp taşımadığı ve aktarımın taraflarınca aktarıma tabi tutulan kişisel verilerin güvenliğinin sağlanması adına hangi idari ve teknik tedbirlerin alındığıdır. Görüldüğü üzere aktarım faaliyetlerinin dayandığı hukuka uygunluk sebepleri ve veri güvenliğinin sağlanması için alınması gereken idari ve teknik tedbirler meseleleri de çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının hukuka uygunluklarının sağlanması için büyük önem arz etmektedir.

Çok uluslu grup şirketler yürütmüş oldukları ticari faaliyetler ile birlikte başta ekonomik amaçlar başta olmak üzere yönetsel, vergisel, hukuki ve sair amaçlarla grup arasında kişisel veri aktarımları gerçekleştirmektedir. Bununla birlikte grup üyesi şirketler arasında yapılan kişisel veri aktarımlarının gelişi güzel bir şekilde gerçekleşerek ilgili kişilerin haklarının zarara uğratılmaması ve hukuka uygun zeminde bir veri aktarım faaliyeti gerçekleştirilmesi adına bu aktarımlara ilişkin grup için belirli kurallar öngörülmesi gerekmektedir[148]. Öyle ki ticaret hayatındaki karlılık amacı ve grup şirket üyelerinin farklı ülkelerde kurulmuş olmalarından kaynaklı olarak ortaya çıkan mevzuat değişiklikleri bu aktarımları veri güvenliğinin sağlanması konusunda oldukça riskli kılmaktadır. Global düzeyde bakıldığında çok uluslu grup şirketlerin pek çoğunun ticari merkezlerinin ABD ve AB'de bulunduğu görülmektedir. Durum böyle olunca ABD ve AB üye ülkeleri arasında merkezleri her iki coğrafya bulunan grup şirketleri arasında pek çok kişisel veri aktarımı

[148] Dülger, GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları, s.4

gerçekleşmektedir. Ancak bu aktarımların ABD ve AB'nin kişisel verilerin korunmasına ilişkin farklı mevzuat düzenlemelerine ve uygulama kurallarına sahip olması sebebiyle hukuka uygunluklarının ayrıca değerlendirilmesi gerekmektedir. Özellikle AB'nin Schrems I ve II kararları sonrasında ABD'ye yapacağı kişisel veri aktarımlarını, yeterli güvenceye sahip bulmaması söz konusu aktarım faaliyetlerinin hangi amaçla gerçekleştiğinin ve bu amacın hukuka uygunluğu ile tabi olacağı kuralların incelenmesini önemli hale getirmiştir[149]. Çok uluslu grup şirketler esasında ticari ve ekonomik amaçlarla verileri topluluk içindeki üye şirketlere aktarsa bile, üye şirketlerin farklı ülkelerde kurulu olması, kişisel veri işleme ve aktarım faaliyetlerinin amaçlarının hukuka uygunluğunun sağlanması ile aktarıma tabi kişisel verilerin aktarıldığı ülkede de yeterli ve eşit seviyede korunması için önem arz etmektedir. Söz konusu korumayı taahhüt eden metinler arasında önemli bir yere sahip olan bağlayıcı şirket kuraları da grup üyesi şirketler arasındaki kişisel veri aktarımlarının amaçlarının ayrıntılı bir şekilde belirtildiği ve hukuka uygunluk şartlarına tabi kılınarak topluluk bünyesinde aktarıma tabi bütün grup üyesi şirketler tarafından kabul edilmekte ve hukuken bağlayıcı olacak şekilde topluluk içerisinde uygulama alanı bulmaktadır. Bağlayıcı şirket kurallarını kabul eden grup üyesi şirketin, veri işleme faaliyetlerini ve bu faaliyetlerin altında yatan amaçları göz önünde bulundurarak kişisel verilerin korunması için gereken ihtiyaçları dikkate alması ve bu ihtiyaçları karşılamak için aldığı idari ve teknik tedbirleri yetkili veri otoritesine sunarak uygunluğunu alması gerekmektedir. AEA içinde Tüzük'e uygun ve Tüzük ile eşit seviyede kişisel veri koruma düzeni vaat eden bu kurallar, grup şirket içinde serbestçe veri dolaşımını temin etmektedirler[150]. Çok uluslu grup şirketler arasında aktarıma tabi tutulan kişisel verilerin güvenliğinin sağlanması ve koruma altına alınmasını taahhüt eden bu kurallar, AB

[149] Gülçin Gümüş, Dülger ''Schrems II Kararı ve Sonuçları'', s.6

[150]Daniela Masoch, "Why Should Companies Invest in Binding Corporate Rules?', 2019, https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, Erişim Tarihi: 02.12.2021.

hukuku için olduğu gibi ülkemiz dahil başka hukuk sistemleri için de benzer şekilde aktarımların hukuka uygunluğunu tesis etmekte önemli bir role sahiptir[151].

Öte yandan Çalışmamızın üçüncü bölümünde de belirteceğimiz üzere sınır ötesi kişisel veri aktarımlarında bulunacak grup üyesi şirketlerin alabilecekleri bir güvenlik tedbiri olarak hukuka uygun veri aktarımlarının sağlanması için hazırlayabilecekleri bağlayıcı şirket kurallarında da söz konusu aktarımların hukuka uygunluk sebeplerinin diğer bir deyişle yasal dayanaklarının açık ve anlaşılır bir şekilde düzenlenmesi beklenmektedir. Söz konusu hukuka uygunluk sebepleri ile bu sebeplere bağlı olarak her bir aktarım faaliyeti için grup üyesi şirketlerin tabi olacağı genel veri işleme ilkeleri ve alınacak veri güvenliği tedbirlerinin bağlayıcı şirket kurallarında eksiksiz bir şekilde düzenlenmesi yetkili veri koruma otoritesi tarafından alınan başvurularda bu kurallar için yapılacak değerlendirmeler ve onay süreci için de büyük önem arz etmekte ve bu unsurların bağlayıcı şirket kurallarında belirtilmesi kurallar için bir geçerlilik şartı teşkil etmektedir. Bu sebeple grup üyesi şirketler tarafından yapılacak aktarımların en az bir hukuka uygunluk sebebine dayanarak ve genel veri işleme ilkeleri ile veri güvenliği tedbirlerine tabi olacak şekilde gerçekleşmesi beklenmektedir. Bu noktada söz konusu hukuka uygunluk sebeplerinin, genel veri işleme ilkelerinin ve alınabilecek veri güvenliği tedbirlerinin bu kurallar dahilinde belirtilmesi ve eksiksiz bir şekilde uygulamaya konulması için grup şirketler arasındaki kişisel veri aktarım faaliyetinin hukuka uygun sebeplerinin ve alınabilecek veri güvenliği ilkeleri ile grup şirketlerin veri aktarım süreçlerinde tabi olmaları gereken genel veri işleme ilkelerinin de incelenmesi ve iyi anlaşılması faydalı olacaktır.

KVKK m.3/ı'da veri sorumlusunun kişisel verilerin işleme amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan tüzel veya gerçek kişiyi ifade ettiği belirtilmiştir. Bu bağlamda, bu tanım uyarınca

[151]Claire Sullivan, EU GDPR Or APEC CBPR? A Comparative Analysis of The Approach of The EU And APEC To Cross Border Data Transfers And Protectionof Personal Data İn The Iot Era, Computer Law and Security Review, C. 35, 2019, s.382.

veri sorumlusu olarak hareket eden grup üyesi şirketlerin kişisel veri aktarımlarını gerçekleştirmeden önce bu aktarım amaçlarını belirlemeleri gerekmektedir[152]. Grup şirketler arasındaki kişisel verileri aktarım ve işleme amaçları belirlenirken topluluğun çıkarları ve kurumsal politikaları önemli bir rol oynamaktadır. Buna karşılık uygulamada ticari amaçlarla müşterinin hedeflenmesi, kişi özelinde alışveriş ve tüketim alışkanlıklarının belirlenmesi amacıyla profilleme, ticari ileti gönderimi ve reklam faaliyetleri gibi belirli amaçlarla kişisel veriler grup şirketler arasında ve dolaylı olarak yurt dışına aktarılırken mevzuat hükümlerine uygun hareket edilmediği görülmektedir. Oysa ki Türkiye'de merkezi bulunan grup üyesi şirketler tarafından diğer grup üyelerine yapılacak kişisel veri aktarımlarının KVKK ve alt mevzuatında yer alan düzenlemelere ve şartlara eksiksiz bir şekilde uygun olması ve kişisel verilerin aktarımı esnasında kişisel veri işlemenin genel ilkelerinden olan kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gibi kurallara da itibar edilmesi gerekmektedir.

Diğer taraftan çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının KVKK m. 5 ve 6'da öngörülen hukuka uygunluk sebeplerinden en az birini taşıması gerekmektedir. Bu sebepler KVKK m.5'te düzenlenen ilgili kişinin açık rızası veya ilgili kişinin açık rızası olmasa da söz konusu kişisel veri işleme ve/veya aktarım faaliyetinin kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel veri işlemenin ve/veya aktarımının zorunlu olması, ilgili kişinin kendisi tarafından söz konusu kişisel verinin alenileştirilmiş olması, bir hakkın tesisi,

[152]Dülger, s.263.

kullanılması veya korunması için kişisel veri işlemenin zorunlu olması ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şeklindedir. Bunun yanı sıra aktarıma tabi kişisel verinin özel nitelikli olması halinde bu verilerden sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ilgili kişinin açık rızası ile ya da kanunlarda öngörülen hâllerde ilgili kişinin açık rızası olmasa da işlenebilmektedir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilmektedir[153]. Çok uluslu grup şirketler arasında gerçekleşecek kişisel veri aktarımlarında da bu veri işleme şartlarından en az birinin bulunması ve kişisel veri aktarımının hukuka uygunluk şartlarından en az birini taşıması gerekmektedir.

Kural olarak kişisel verilerin işlenmesinde ilgili kişinin açık rızasının bulunmaması halinde yukarıda belirttiğimiz ve KVKK m.5/2'de[154] düzenlenen diğer hukuka uygunluk şartlarından birinin varlığı aranacaktır. Bu şartların yanı sıra kişisel verilerin işlenirken ve aktarılırken KVKK m.4 uyarınca öngörülen hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine de uyulması gerektiği unutulmamalıdır. Kişisel verilerin işlenmesi ve aktarımı için ilgili kişinin açık rızasının bulunması, diğer

[153] Erarslan, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, s.45

[154] KVKK m.5"(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması".

hukuka uygunluk sebeplerine nazaran KVKK m.8/1 ve 9/1 uyarınca gerek yurt içi ve gerek yurt dışı aktarımlarda en önemli şartı oluşturmakta ve dolayısıyla hukuka uygunluk sebebidir. Bu kapsamda ilgili kişinin açık rızasının bulunması, çok uluslu grup şirketlerin kendi aralarındaki kişisel veri aktarımlarının amaçlarını hukuka uygun hale getirecektir. Ancak, ilgili kişinin açık rızasının bulunmadığı hallerde, yurt içindeki grup üyesi şirkete kişisel veri aktarımı ile yurt dışında kurulu olan grup üyesi şirkete kişisel veri aktarımlarının hukuka uygunluklarının sağlanması adına KVKK ve alt mevzuat hükümleri uyarınca farklı kriterler öngörülmüştür. Kişisel verilerin yurt içine aktarımı halinde ilgili kişinin açık rızası yoksa, KVKK m.5/2'deki şartların bulunması veya yeterli önlemler alınarak m.6/3'deki[155] sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hâller veya KVKK m.8/2'de anılan diğer hallerde aktarımı mümkün olabilecektir. Buna karşılık kişisel verilerin yurt dışına aktarımı halinde ilgili kişinin açık rızası yoksa, KVKK m.5/2 veya 6/3'deki koşullardan birinin bulunması ve yabancı ülkede yeterli korumanın bulunması ya da yeterli korumanın bulunmaması durumunda ise KVKK m.9/2 uyarınca Türkiye'deki ve ilgili yabancı ülkedeki grup üyesi şirketlerin veri sorumlusu-veri sorumlusu veya veri sorumlusu-veri işleyen olarak aktarıma tabi kişisel veriler için yeterli bir korumanın sağlanacağını yazılı olarak taahhüt etmeleri ve ilgili taahhütleri için Kurul'un izninin alınması şartları aranmaktadır[156]. Bu koşulların bulunmaması halinde, grup üyesi şirketler arasında yapılacak aktarımların amacı ne olursa olsun hukuka uygunluk sebepleri gerçekleşmemiş ve hukuka uygun bir aktarım yapılmamış olacaktır.

Bu sebeple uygulamada çok uluslu grup şirketler arasındaki kişisel veri aktarımına sebep olan faaliyetlerin incelenmesi ve hukuka uygunluklarının değerlendirilmesi büyük önem arz etmektedir. Bu kapsamda yapılacak bir inceleme ve değerlendirme

[155]KVKK m.6 "(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir".

[156] Çekin, 2020, s.73 vd.

özellikle çok uluslu grup şirketler tarafından yurt dışına veri aktarımının da bulunduğu veri sorumlusu-veri sorumlusu veya veri sorumlusu-veri işleyen taahhütnameleri veya bağlayıcı şirket kurallarının hazırlanması ve bu metinlerin Kurul tarafından uygun bulunup onaylanması aşamasında da etkili rol oynayacaktır. Örneğin ilgili kişinin açık rızasının bulunmaması halinde grup şirketler açısından KVKK m.5/2'de yer alan ve açık rızanın aranmadığı hallerin varlığına bakılması gerekecek, KVKK m.5/2 (a) uyarınca kanunlarda veri işlenmesi için açıkça öngörülen hallerde açık rızanın varlığı aranmayacak ve yurt içindeki grup şirketler arasında yapılacak kişisel veri aktarımları için KVKK m.8/2 ve yurt dışında bulunan grup üyesi şirketlere yapılacak kişisel veri aktarımlarında ise KVKK m.9/2'deki koşulların sağlanıp sağlanmadığı incelenecektir. TTK m.195/5 ve 401 uyarınca grup şirketler tarafından faaliyet raporu ve bağlılık raporu hazırlanması ya da topluluk içindeki grup üyesi şirketlere ait finansal tabloların konsolide edilmesi hallerinde işlenecek ve aktarıma tabi tutulacak kişisel verilerin kanunlarda açıkça öngörülme şartı uyarınca işlendiğinin ve aktarıldığının kabulü gerekecek ve bu aktarım faaliyeti Türk hukukunda hukuka uygun olarak değerlendirilebilecektir[157].

2.3. Grup Şirketler Arasındaki Kişisel Veri Aktarımlarının Amaçları

2.3.1. Ekonomik ve Ticari Amaçlar

Çok uluslu grup şirketlerin dünyanın pek çok yerine yayılmış büyük ve kapsamlı ticari faaliyetleri, bugün dünya ekonomisinde büyük önem arz eden ve ülkelerin de ekonomik politikaları üzerinde belirleyici etkileri bulunan bir gerçeklik haline gelmiştir. Bu yapıların kimi çevreler tarafından 20. yüzyılda ortaya çıktığı ileri sürülse de, farklı formlarda varlıklarının bu tarihten daha öncesine dayandığı söylenebilir[158]. Çok uluslu şirketler; hâkim şirketin ticari faaliyetlerini kendi ülkesi dışına da taşıması ve uluslararası düzeyde ticaret faaliyetleri yürütmesi amacıyla kurulmakta ve dünyanın pek çok yerinde gelişerek örgütlenmektedir. Bu büyüme

[157] Dündar, s.85-86; Çakır Çelebi, s.20
[158]Danailov, s.10.

sırasında grup şirketler ticari faaliyetleri nedeniyle kuruldukları ülkenin ve ekonomik alanlarının sınırları içinde kalmamış ve farklı ülkelerde de yaptıkları yatırımlarla topluluk halini almışlardır. Bununla birlikte çok uluslu grup şirketler hem kendilerine hem de faaliyette bulundukları ülkelere katkı sağlamak adına çevre konuları, sürdürülebilir kalkınma, insan hakları ve hatta siyaset sahalarında da belirli etkiler oluşturmuş ve zaman zaman çözümlere ve bazen de uluslararası sorunlara yol açmışlardır.

Çok uluslu şirketlerin grup üyesi şirketleri, bulundukları ülkenin iç hukukuna uygun olarak kurulan ve faaliyet göstermekle yükümlü olan şirketlerdir ve şirketler topluluğunda hâkim şirket konumunda olan şirketin farklı ülkelerdeki yatırımlarının hukuki kişilik bulmuş hallerini teşkil ederler. Bu sayede hâkim şirketler diğer ülkelerdeki grup şirketleri aracılığıyla ilgili ülkeler arasında bir ticaret ağı oluşturarak geniş çaplı bir ekonomik ve hukuki yapılanma oluştururlar[159]. Ekonomik hayatta tüm şirket ve ticari işletmelerde olduğu gibi, çok uluslu grup şirketlerin de amacı kâr etmek ve kendi ekonomik çıkarlarını korumaktır[160]. Çok uluslu grup şirketler, bir ülkede ticari faaliyet yürütmek, bu ülkedeki pazarı tanımak ve mümkünse pazarda aktif bir rol oynamak, yatırım faaliyetleri ile ticari hacmini genişletmek, faaliyet alanlarına girdiği müddetçe ürün ve hizmetlerini o ülkedeki piyasaya sunmak gibi temel ekonomik amaçlar gütmektedir. Bu ekonomik amaçlarını gerçekleştirmek için kuruldukları ülkedeki ticari güçlerini ve karlarını artırabilmeye çalışırlar ve bu sebeple faaliyet alanlarına göre yürüttükleri üretim faaliyetlerinin hacmini genişletmek, ürün ve hizmet çeşitliliğini ve kalitesini artırmak, daha fazla tüketiciye hitap etmek, bayilik ağını genişletmek, satışlarını artırmak gibi amaçlarla hareket ederler. Bu süre zarfında hedef kitlelerini ve çoğu zaman tüketici eğilimlerini belirlemek, sözleşme müzakereleri ve süreçlerini yürütmek, pazarlama faaliyetleri ile tanıtım ve reklamlar yapmak adına kişisel veri işlemek zorunda kalırlar. Kişisel verilerin işlenmeye başlaması halinde de çok

[159] Fulya Kıvılcım, Küreselleşme Olgusu ve Çokuluslu Şirketlerin Küreselleşme Süreci Üzerindeki Rolü, Ekonomi Bilimleri Dergisi, s. 12
[160] Efe Dündar, Uluslararası Ticaret Hukukunda Doğrudan Yabancı Yatırımlar ve Çok Uluslu Şirketler İncelemesi, Marmara Üniversitesi Öneri Dergisi, s. 273 vd.

uluslu grup şirketlerin her biri kurulduğu ve faaliyet gösterdiği ülkenin kişisel verilerine ilişkin mevzuat hükümlerine uygun şekilde hareket etmeli ve mevzuatın belirlediği çerçevede kişisel veri işleme ve aktarım faaliyetlerinde bulunmalıdır.

Grup şirketler içindeki kişisel veri aktarımlarını mevzuata uyum açısından bir düzene oturtan bağlayıcı şirket kuralları, grup şirketler topluluğunun kendi arasındaki kişisel veri aktarımlarındaki ihtiyaçların ve amaçların tespiti edilmesi üzerine hazırlanmakta ve bu aktarımların ihtiyaç duyduğu hukuka uygunluk şartını temin etmeyi amaçlamaktadır[161]. Bağlayıcı şirket kurallarının hazırlanarak Kurul'un onayından geçebilmesi için çok uluslu grup şirketler arasındaki ticari ve ekonomik amaçlarla gerçekleştirilen kişisel veri aktarımlarının KVKK m. 5 ve 6'da öngörülen hukuka uygunluk sebeplerinden en az birini karşılaması gerekmektedir. Bu kapsamda yurt dışında bulunan hakim şirket ile bu hakim şirketin Türkiye'de kurulu olan bağlı şirketi ile ürünlerinin Türkiye'deki dağıtımını yapması adına distribütörlük ilişkisi içine girmesi ya da yurt dışındaki hakim şirketin Türkiye'ye de hizmet sunmak istemesi halinde Türkiye'de kurulu bağlı şirketinin yapmış olduğu piyasa araştırması sonrası kendisine yönlendirdiği Türkiye'de faaliyet gösteren ve hizmet talep eden müşteriler ile tanıştırması ve bağlı şirketin hakim şirkete aracılık faaliyetinde bulunması gibi ticari faaliyetler esnasında grup üyesi şirketlerin yetkili kişilerine, irtibat kişilerine ve müşterilere ve müşterilerin yetkili kişileri ile irtibat kişilerine ait kişisel veriler işlenirken bu verilerin taraflar arasında ya da taraflardan biriyle üçüncü kişi arasında bir sözleşmenin kurulması ve/veya ifası için gerekli olduğu değerlendirilebilecektir.

Diğer taraftan şirketler topluluğu bünyesindeki bir grup üyesi şirketin Türkiye'deki grup şirketlerine hizmet sağlaması ve grup şirketler arasında bir hizmet tedariki ilişkisinin bulunması halinde de tedarikçi sıfatıyla faaliyet gösteren grup üyesi şirket ile hizmet alan grup üyesi şirketin irtibat kişilerine ve yetkili kişilerine ait kişisel verilerin de taraflar arasındaki tedarik sözleşmesinin ifası için gerekli olduğu

[161] Dülger, GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları, s.3

sonucuna varılabilecektir. Bununla birlikte grup şirketler arasında gerçekleşecek olası bir pay devri halinde pay devrine bağlı olarak alınacak yetkili organ kararlarının[162] ve pay devrine bağlı olarak tutulacak kayıtların, pay devir sözleşmesinin devre taraf grup şirketler arasında paylaşılması da TTK kapsamında öngörülen şartların yerine getirilmesi adına gerekli olduğundan kişisel verilerin kanunlarda açıkça öngörülen sebeplerle işlenmesine örnek olarak gösterilebilecektir. Öte yandan grup şirketlerin herhangi bir pay devri ya da birleşme veya devralma işlemleri öncesinde gerekli görmeleri halinde gerçekleştirdikleri incelemeler (*due diligence*) ile ve bu incelemeler ışığında hazırlanan raporlar ve düzenlenen belgeler aracılığıyla birbirlerine aktarmış oldukları şirket yöneticilerine ve yönetim yetkilerine, sermaye yapısına ve ortaklarına, taraf oldukları sözleşmesel ve protokollerine, izin ve ruhsatlarına, mülkiyetlerinde bulunan ya da kiraladıkları veya farklı bir hak uyarınca ellerinde bulundurdukları menkul ve gayrimenkullerine, fikri ve sınai haklarına, sigortalarına ve gerekli görülen diğer konulara ilişkin bilgilerin de bir sözleşmenin müzakeresi ve ifası ya da veri sorumlusu grup üyesi şirketin yükümlülüklerini yerine getirmesi için gerekli olması veyahut veri sorumlusu şirketin meşru menfaati uyarınca aktarıldığını belirtmek yanlış olmayacaktır. Bu işlemler sonrasında grup üyesi şirketlerin taraf oldukları ortaklık sözleşmelerindeki ön şartların veya beyan ve tekeffüllerin yerine getirileceğine dair kayıtların taraflar arasındaki teatisi de yine aynı kapsamda değerlendirilebilecektir.

Grup şirketler arasındaki kişisel verilerin aktarımlarının başka bir sebebi de bir grup şirketin taraf olduğu sözleşmeye eklediği devir maddesi ile söz konusu sözleşmeden doğan hak ve yükümlülüklerinin yerine getirilmesini bir başka grup üyesi şirkete aktarabilmesidir. Bu durum ödemelerin daha çok sözleşmeye taraf olan şirket yerine bu borcu devrettiği diğer grup üyesi şirket tarafından gerçekleştirilmesi halinde ortaya çıkar. Grup üyesi şirketler arasında gerçekleşen ödeme

[162] Detaylı bilgi için bkz. E. Dündar, Yeni Türk Ticaret Kanunu Çerçevesinde Çok Uluslu Şirketler, Yayımlanmamış Doktora Tezi, İstanbul Kültür Üniversitesi, İstanbul 2013, s.85 vd.; Fatma Betül Çakır Çelebi, "Şirketler Topluluğunda Hâkim Teşebbüs", Ticaret ve Fikri Mülkiyet Hukuku Dergisi C.4, S.1,2018, s.123

yükümlülüğünün devri işlemine bağlı olarak taraflar arasında aktarıma tabi olacak kişisel verilerin ise yine KVKK m.5 uyarınca öngörülen sözleşmenin ifası kapsamında gerçekleştiği belirtilebilecektir. Öte yandan bir grup üyesi şirketin diğer grup üyesi şirkete taraf olduğu bir sözleşmedeki ödeme yükümlülüğünü yerine getirmesi için teminat göstermesi veya kefil olması da ödemenin gerçekleştirilebilmesi amacıyla bu kapsamda taraflar arasında gerçekleşecek veri aktarım faaliyetlerinin sözleşmenin ifası için gerekli olmasına örnek teşkil edebilecektir. Aynı şekilde holding şirket tarafından gerçekleştirilen mülakat süreçleri sonucunda istihdam edilmesine karar verilen personel adayının bağlı şirketlerden birinde iş başı yapması ya da halihazırda Türkiye'deki bir grup üyesi şirkette çalışan personelin yurt dışındaki grup üyesi şirkete transfer olması halinde holding şirket ile bağlı şirket arasında aktarılacak personele ait özlük bilgilerinin de ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusu olan bağlı şirketin meşru menfaatleri uyarınca işlendiğinin ve aktarıldığının belirtilmesi somut olayın şartlarına göre mümkün olabilecektir. Görüldüğü üzere çok uluslu grup şirketlerin yürüttükleri ticari faaliyetleri süresince gerçekleştirdikleri kişisel veri aktarımları da değişkenlik gösterebilmekte ve aktarımın şeklinde göre KVKK kapsamında en az bir veri işleme şartına dayanması hukuka uygunluklarının sağlanmasında büyük rol oynamaktadır.

2.3.2. Hukuki ve Vergisel Amaçlar

Uygulamada çok uluslu grup şirketler arasında gerçekleşen kişisel veri aktarımlarının ekonomik ve ticari faaliyetlerin yerine getirilmesinin yanı sıra hukuki ve vergisel sebeplere bağlı olarak da gerçekleşebildiği görülmektedir. Hukuki ve vergisel konulara ilişkin gerçekleşen kişisel veri aktarımlarının da esasında doğrudan ekonomik ve ticari amaçlarla yapılan kişisel veri aktarım faaliyetlerinden bağımsız olmadığını ve bu faaliyetlerin bir sonucu ya da gerekliliği olarak gündeme geldiğini söylemek mümkündür. Öyle ki TBK kapsamında alacağın devri ve kefalet gibi işlemlere bağlı olarak yapılacak sözleşmelerin şekil şartına bağlı olması sebebiyle grup üyesi şirketler arasında bu işlemlere taraf

olmaktan ileri gelen kişisel veri aktarım halleri kanunlarda açıkça öngörülen hallerden kaynaklı olarak kişisel verilerin işlenmesine ve aktarımına örnek teşkil edeceğinden bu aktarım aynı zamanda hukuki bir boyut da taşıyacaktır. Bununla birlikte topluluk içerisindeki grup üyesi şirketler arasında gerçekleşen söz konusu kefalet işleminin ya da herhangi bir borç devri veya teminat gösterme işleminin de TTK m. 199 ve diğer ilgili maddeleri uyarınca grup şirketler tarafından hazırlanması gereken bağlılık raporunda ve faaliyet raporlarında belirtilmesi[163] ve bu raporların hazırlanması için grup üyesi şirketler arasında gerçekleştirilecek kişisel veri aktarımlarının da yine hukuki sebeplerle gündeme geldiğini ve tarafların veri sorumlusu olarak hukuki yükümlülüklerinin yerine getirilmesi ve/veya açıkça kanunlarda öngörülen hallerden kaynaklı olarak gerçekleştiğini belirtmek mümkündür.

Bununla birlikte TTK uyarınca Türkiye'de anonim şirket olarak kurulan grup üyesi şirkete hakim şirket olan yurt dışındaki diğer bir grup üyesi şirketin yönetim kurulu üyesi olarak atanması ve TTK uyarınca bu üyenin gerçek kişi temsilcisinin atanması için sicil nezdinde yapılacak işlemler ve bu işlemlere bağlı düzenlenecek kayıtların grup üyesi şirketler arasında aktarılması halinde de aktarıma tabi kişisel verilerin tarafların veri sorumlusu olarak hukuki yükümlülüklerinin yerine getirilmesi ve/veya açıkça kanunlarda öngörülen hallerden kaynaklı olarak gerçekleştiğini belirtmek mümkündür. Diğer taraftan bu şirketin TTK m.409 ve devamı maddeler uyarınca yıllık olarak gerçekleştireceği olağan genel kurul için çağrı ve toplantı yapılması durumlarında da çağrı için alınan yönetim kurulu kararı, toplantı yapılacağı bilgisinin ilgili pay sahiplerine ulaştırılması için düzenlenen davet yazıları, genel kurul toplantısı[164] esnasında alınan kararların geçirildiği toplantı tutanağı ve hazır bulunanlar listesi gibi belgelerin hazırlanması için pay sahibi olan grup şirketler arasındaki kişisel veri aktarımları da bu kapsamda değerlendirilebilecektir. Öte yandan Türkiye'de yeni kurulan bu şirkete diğer grup

[163] Detaylı bilgi için bkz. Pulaşlı s. 171
[164] Detaylı bilgi için bkz. Arcan Tuzcu, "Halka açık şirketlerde kurumsal yönetim anlayışı: İMKB-100 Örneği", s. 45.

üyesi şirketlerde yetkili olan yöneticilerden birinin imza yetkilisi olarak atanması halinde bu şirketin kuruluş sonrası ticari faaliyetlerine başlayabilmesi için iş yeri açma ve çalışma ruhsatının düzenlenmesi adına belediyeye ve vergi açılışının yapılması adına ilgili vergi dairesine başvurması gibi Türkiye'deki ilgili kurum ve kuruluşlar nezdinde yapacağı işlemler için gerekli olan bilgilerin aktarımı halinde de kişisel verilerin ilgili grup şirketlerin veri sorumlusu olarak hukuki yükümlülüklerinin yerine getirilmesi için ve/veya açıkça kanunlarda öngörülen hallerden kaynaklı olarak aktarıldığı savunulabilecektir.

Diğer taraftan TTK'da şirketler topluluğu düzenlemelerinin yer aldığı m.195 ila 209 maddeleri uyarınca şirketler topluluğunun teşekkülü, konusu ve topluluk içi ilişkilerin yürütülmesi, finansal raporlama faaliyetlerinin yerine getirilmesi ve bilgi alma yollarının işletilmesi, pay sahiplerinin haklarının gözetilmesi, alacaklıların korunması ve hakim şirketin güvenden doğan sorumluluğu konularında gerekli tedbirlerin alınması hallerinde de gerçekleştirilen kişisel veri aktarımları açıkça kanunlarda öngörülen hallere örnek gösterilebilecektir. Bununla birlikte yine TTK. m. 401[165] uyarınca grup şirketlerin tablolarını, konsolidasyona tabi finansal tablo ve raporlarını hazırlaması ve bağımsız denetim faaliyetlerine tabi olması halinde söz konusu tabloların oluşturulması ve raporların hazırlanması için grup şirketler arasında veya üçüncü kişilere yönelik yapılan kişisel veri aktarımları da şirketlerin veri sorumlusu olarak kanunlarda ve alt mevzuat hükümlerinde yer alan yükümlülüklerini yerine getirmeleri amacıyla gerçekleştirilmektedir. Son olarak grup şirketlerin çalışanlarına, müşterilerine, tedarikçilerine, iş ortaklarına ve ilgili olan diğer ilgili kişilere dair kayıtları topluluk içinde aktarmaları ve bu kişiler ile

[165] TTK. m. 401: *"(1) Şirketin yönetim kurulu, finansal tabloları ve yönetim kurulunun yıllık faaliyet raporunu düzenlettirip onaylayarak, gecikmeksizin, denetçiye verir. Yönetim kurulu, şirketin defterlerinin, yazışmalarının, belgelerinin, varlıklarının, borçlarının, kasasının, kıymetli evrakının, envanterinin incelenerek denetlenebilmesi için denetçiye gerekli imkânları sağlar. (3) Konsolide finansal tabloları çıkarttırmakla yükümlü olan şirketin yönetim kurulu, konsolide finansal tabloları denetleyecek denetçiye; topluluğun finansal tablolarını, topluluk yıllık faaliyet raporunu, münferit şirketin finansal tablolarını, şirketlerin yönetim kurullarının yıllık faaliyet raporlarını, bir denetim yapılmış ise ana şirketin ve yavru şirketlerin denetim raporlarını vermek zorundadır. Denetçi, birinci fıkranın birinci ve ikinci cümlelerinde öngörülen yetkileri ana ve yavru şirketler yönünden de kullanabilir."*

aralarında başta tazminat talebi olmak üzere muhtelif konularda doğabilecek ilerideki uyuşmazlıklarda kullanabilmek için saklamaları da TBK m. 72 uyarınca gerek hukuki yükümlülüklerinin yerine getirilmesi gerekse uyuşmazlık esnasında şirket lehine bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin işlenmesinin zorunlu olmasına örnek gösterilecektir.

Çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının gerek ticari ve ekonomik gerekse hukuki ve vergisel amaçlar güdülerek çok boyutlu bir şekilde gündeme gelmesi de mümkündür. Grup şirketler arasında mali durumu kötü olan, borca batık olan ya da kredi karşılığı sunacak teminatı bulunmayan grup üyesi bir şirkete diğer bir grup üyesi şirketin kredi sağladığı ve bu şekilde grup şirketlerin kendi aralarında borçlanma işlemlerine başvurulabildikleri görülmektedir. Bu durumda gerçekleşen kredi kullandırımı işlemi her ne kadar ticari ve ekonomik amaçlar güdülerek yürütülse de esasında bu kredinin grup şirketleri arasında transfer fiyatlandırması yoluyla örtülü kazanç teşkil etmesi ve vergisel ve hukuki belirli sorunları da beraberinde getirmesi mümkündür. Öyle ki transfer fiyatlandırması yoluyla örtülü kazanç, dağıtımı 5520 sayılı Kurumlar Vergisi Kanunu m.13.1 uyarınca "Kurumlar, ilişkili kişilerle emsallere uygunluk ilkesine aykırı olarak tespit ettikleri bedel veya fiyat üzerinden mal veya hizmet alım ya da satımında bulunursa, kazanç tamamen veya kısmen transfer fiyatlandırması yoluyla örtülü olarak dağıtılmış sayılır[166]. Alım, satım, imalat ve inşaat işlemleri, kiralama ve kiraya verme işlemleri, ödünç para alınması ve verilmesi, ikramiye, ücret ve benzeri ödemeleri gerektiren işlemler her hal ve şartta mal veya hizmet alım ya da satımı olarak değerlendirilir." şeklinde tanımlanmıştır.

Bu kapsamda bir grup üyesi şirketin kendisi ile ilişkili kişi olarak değerlendirilebilecek diğer grup üyesi şirketten ödünç para alması işlemi örtülü kazanç olarak kabul edilebilecektir. Grup şirketler arasında söz konusu hüküm uyarınca kanuna aykırı bir şekilde transfer fiyatlandırması yoluyla örtülü kazanç

[166] Neslihan Karataş Durmuş, Ticaret Kanunu Kapsamındaki Şirket Toplulukları Ve Bunların Vergi Hukuku Karşısındaki Durumları, s.4

elde edilmesinin önüne geçilmesi için gerekli tedbirlerin alınması ve topluluk içerisinde dahi olsa ilgili işlemin emsallere uygun bir şekilde gerçekleştirilmesi gerekmektedir. Grup şirketler arasında bu şartların sağlanmaması halinde yapılacak işlemlerden doğabilecek yaptırımlar ile karşı karşıya kalmamak adına ilgili grup üyesi şirketler nezdinde yürütülecek muhasebeleştirme işlemlerinin mevzuat hükümlerine ve Kamu Gözetim Kurumu tarafından kabul edilen standartlara uygun hale getirilmesi ve başta banka ve sigorta vergileri ile yapılan işlemin niteliğine uygun düştükçe hesaplanacak katma değer vergisi gibi amme borçların da zamanında ve eksiksiz ödenmesi amacıyla yapılan grup içi kişisel veri aktarımları da hukuki ve vergisel işlemlerin yerine getirilmesi amacıyla gerekli addedilebilecektir. Diğer taraftan söz konusu hukuki gerekçeler ile gerçekleştirilen kişisel veri aktarımlarının dayandığı yasal düzenlemelerin grup üyesi şirketin kurulduğu ve faaliyet gösterdiği ülkenin mevzuatına göre değişiklik gösterebileceği de unutulmamalı ve böyle bir kişisel veri aktarımında hukuka uygunluğun tam olarak anlaşılabilmesi için her iki ülkenin de mevzuat hükümlerinin karşılaştırmalı bir şekilde incelenmesi gerekmektedir.

Öte yandan, TTK uyarınca tüzel kişi olarak kabul edilmese de Kurul tarafından 23/07/2019 tarihinde yapılan 2019/225 sayılı açıklama ile VERBİS'e kayıt yükümlülüğü getirilen ve veri sorumlusu olarak ele alınan yurt dışında kurulu şirketlerin Türkiye'deki şubeleri tarafından yurt dışındaki şirkete yapılacak kişisel veri aktarımlarına değinmek de faydalı olacaktır. Söz konusu yabancı şirketin Türkiye'de bulunan şubesinin yürütmüş olduğu ticari faaliyetler göz önünde bulundurulduğunda bu şubenin bir veri sorumlusu olarak kabul edilmesi esasında şube tarafından yurt dışındaki merkez şirkete yapılan kişisel veri aktarımlarında grup şirketler arasındaki kişisel veri aktarımına benzer bir yapı gündeme gelmektedir[167]. Öyle ki Kurul, şube tarafından yürütülen kişisel veri işleme ve aktarım faaliyetlerini KVKK ve alt mevzuat kapsamına alabilmek ve şube

[167] KVKK, Yurtdışında yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Karar Özeti, https://kvkk.gov.tr/Icerik/5545/2019-225

tarafından yurt dışına aktarılan ve yurt dışında da merkez şirket tarafından işlenen kişisel verilerin güvenliğinin sağlanmasından doğacak sorumluluğu bir mercide toplayabilmek amacıyla yabancı şirketlerin Türkiye'deki şubelerini veri sorumlusu sıfatıyla VERBİS'e kayıtla yükümlü kılmış ve takibe almıştır. Türkiye'de kurulu şubenin Kurum tarafından veri sorumlusu olarak kabul edilmesi ve şube tarafından istihdam edilen çalışan bilgilerinin veya taraf olunan sözleşmelere dair bilgilerin yurt dışındaki veri sorumlusu merkez şirkete aktarımı halinde de KVKK uyarınca veri sorumlusu – veri sorumlusu arasında bir kişisel veri aktarımı gündeme geldiği ileri sürülebilecektir. Bu yönde bir aktarımın grup şirketler arasındaki kişisel veri aktarımı olduğunu belirtmek isabetli olmayacaksa da iki yapı arasındaki kişisel veri hukuku uyarınca kurulan ilişkinin grup içi aktarımlarla benzer olduğu söylenebilecektir. TTK m.40/4'e göre, merkezleri Türkiye sınırları haricinde bulunan ticari teşebbüslerin Türkiye'deki şubeleri, yerli ticari teşebbüsler gibi tescil olurlar[168]. Ayrıca bu şubeler için ikamet yeri Türkiye'de olan tam yetkili bir ticari temsilci atanması yükümlülüğü öngörülmektedir. Bu ilişkinin ise gerek şubenin kuruluşu ile kuruluşuna ve faaliyetlerini yürütmesine bağlı olarak gerekli olan hukuki ve vergisel yükümlülüklerinin yerine getirilmesi gerekse ekonomik bir yapı olarak Türkiye'de çeşitli ticari faaliyetler yürütmesi itibariyle sözleşmenin ifası, kanunlarda açıkça öngörülmesi, veri sorumlusunun hukuki yükümlülüklerinin yerine getirilmesi veya meşru menfaatinin sağlanması gibi hukuka uygunluk sebeplerine dayandığı ifade edilebilecektir. Benzer bir bakış açısı yabancı bir şirketin Türkiye'de ticari faaliyetler yürütmek dışında haberleşme, temsil, ağırlama vb. amaçlarla kurduğu irtibat büroları[169] tarafından Türkiye'de elde edilen kişisel verilerin yurt dışındaki merkez şirkete aktarılması halinde de gündeme gelebilecektir.

[168] Şube kavramı ve özellikleri ile ilgili olarak bkz. Karayalçın, s. 185-188; Karahan, s. 23 vd.; Pekdinçer, T: Ticaret Sicili Açısından Merkez – Şube – Satış Mağazası Kavramları, Prof. Dr. Fahiman Tekil'in Anısına Armağan, İstanbul 2003, s. 471 vd.

[169] İrtibat bürosu kavramı ve özellikleri ile ilgili olarak bkz. Hacı Kara, Türk Hukukunda İrtibat Bürosu ve Özellikleri

2.3.3. Diğer Amaçlar

Çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının doğrudan ticari ve ekonomik ya da hukuki veya vergisel bir amaçla gerçekleşmediği ve grup şirketlere ilişkin kurumsal politikaların ve topluluk işlerinin yürütülmesi gibi farklı amaçlara dayandığı durumlar da bulunmaktadır. Bu amaçlar da grup şirketler arasındaki kişisel veri aktarımlarının bir sözleşmenin kurulması veya ifası ya da veri sorumlusu sıfatıyla grup şirketlerin hukuki yükümlülüklerinin yerine getirilmesinin sağlanması amaçları dışında daha çok topluluk bünyesinde bulunan grup üyesi şirketlerin ve topluluğun meşru menfaatlerinin sağlanması gibi farklı hukuka uygunluk sebeplerine dayandığını söylemek mümkündür. Çok uluslu grup şirketler arasında insan kaynakları politikaları gereği her ay düzenli olarak dergi çıkarılması, belirli aralıklarla eğitimlerin ve toplantıların düzenlenmesi, sosyalleşme etkinliklerinin ve organizasyonların yapılması bu tür faaliyetlere örnek gösterilebilir. Topluluğun her bir üye grup şirketinin katılımıyla yürütülebilecek bu faaliyetler ile grup şirketler arasında belirli kişisel veri aktarımları da gerçekleşebilmektedir. Söz konusu amaçlarla yapılan veri aktarımları belirli durumlarda veri sorumlusu olarak her bir grup şirketin meşru menfaatlerinin sağlanması sebebine dayansa da belirli durumlarda ise ancak aktarıma tabi kişisel verilerin sahibi olan kişilerin açık rızalarının bulunması ile hukuka uygunluk kazanabilmektedir[170]. Örneğin çok uluslu bir grup şirketin her ay çıkarılan dergisinde Türkiye'de kurulu olan grup üyesi şirketin ARGE ekibinden bir çalışanın ayın en iyi elamanı olarak seçilmesi ve adı, soyadı, özgeçmişi ve fotoğrafı gibi kişisel verilerinin grup üyesi şirketler arasında sirküle edilecek bir topluluk dergisinde yayımlanması halinde ilgili çalışanın açık rızasının alınması gerekebilecektir. Diğer taraftan farklı ülkelerde merkezleri bulunan grup üyesi şirketlerden çalışanların bir zirvede bir araya gelerek çekildikleri fotoğrafın topluluğa ait bir sosyal medya hesabında paylaşılması halinde de somut olayın şartlarına göre fotoğrafı paylaşılacak çalışandan açık rıza alınması gerektiği ya da

[170] Meşru Menfaat kavramı için bkz: Dülger, Kişisel Verileri Koruma Kurulunun 16 Nisan 2019 Tarihinde Yayınlamış Olduğu Kararı Bağlamında "Veri Sorumlusunun Meşru Menfaati" Kavramı

bu paylaşımın topluluğu piyasada canlı ve farkındalığı yüksek bir şirket olarak gösterecek olması gerekçesiyle ilgili çalışanın açık rızası olmasa dahi veri sorumlusu şirketin meşru menfaati uyarınca paylaşıldığı söylenebilecektir.

Çok uluslu grup şirketler arasındaki olağan işlerin yürütülmesi amacıyla her bir grup üyesi çalışan arasındaki e-posta yazışmaları ve gerek bu yazışmalar gerekse farklı yollarla gerçekleşebilecek topluluğun kurumsal politikaları uyarınca belirli aralıklarla hazırlanan raporların, pazarlama, satın alma, üretim, tedarik gibi çeşitli konularda hazırlanan strateji planlarının, müşteri listelerinin, çalışanların görev dağılımlarının, ücret politikalarının ve diğer çıktıların aktarımı faaliyetleri, grup üyesi şirketlerin pazarlama hedefleri uyarınca gerçekleştirdikleri reklam, kampanya ve tanıtım çalışmaları ve tüm faaliyetler süresince grup içi bilgi paylaşımları da çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına birer örnek teşkil etmektedir. Grup şirketlerin tabi oldukları ülkelerin mevzuat hükümlerine, taraf oldukları işlemlere, faaliyet alanlarına ve topluluğa ilişkin insan kaynakları, pazarlama, üretim, ARGE gibi farklı konulardaki kurumsal politikalarına bağlı olarak gerçekleştirilebilecek kişisel veri aktarımları da çeşitlilik göstermektedir. Bu faaliyetler ve kişisel veri aktarımları çeşitlilik gösterse de grup şirketlerin gerçekleştirdikleri kişisel veri işleme ve aktarım faaliyetlerine ilişkin tabi oldukları mevzuat düzenlemelerine itibar etmesi ve hukuka uygunluk şartını karşılamaları gerekmektedir. Öyle ki çok uluslu şirketler kişisel veri aktarımlarında hukuka uygunluk sebeplerini sağlamakla birlikte aynı zamanda bu aktarımın yapıldığı grup üyesi şirketin bulunduğu ülkede de kişisel verilerin belirli bir veri koruma düzeyine tabi olacağını taahhüt etmelidir. Bu kapsamda hangi amaçla olursa olsun grup üyesi şirketler arasında gerçekleşen kişisel veri aktarımları için ilgili grup üyesi şirketin hesap verebilirliği sağlaması ve aktarımların hukuka uygun bir şekilde gerçekleşmesi açısında şirket içinde farkındalığı artırması ve bu amaçla gerekli güvenlik tedbirlerini alması gerekmektedir.

2.4. Grup Şirketler Arasındaki Kişisel Veri Güvenliği

2.4.1. Genel Olarak

Veri güvenliği kavramı, kişisel veri koruma hukukunda pek çok alana temas eden bir kavramdır[171]. Bu kavram esasında kişisel verilerin işlenmesi ve aktarımı hallerinde veri işlemenin genel ilkelerinin tesis edilmesine işaret etmektedir ve veri güvenliği tedbirlerinin her birinin veri işlemenin genel ilkelerinin birer özel görünümü olduğunu söylemek yanlış olmayacaktır[172]. Kişisel verilerin işlenmesinde genel ilkelere uyulmaması durumunda, veri işleme faaliyeti hukuka uygun şekilde yapılmış olmayacak ve bu durum karşısında KVKK'da öngörülen yaptırımlar uygulama alanı bulacaktır[173]. Veri güvenliği ile kişisel verilerin işlenmesi faaliyetleri sırasında kişisel verileri işlenen ilgili kişilerin temel hak ve özgürlüklerinin korunması ve menfaatlerinin gözetilmesi amaçlanmaktadır. Bu çerçevede, veri güvenliğinin sağlanması amacıyla kişisel verilerin işlenmesinde büyük bir önem taşıyan genel ilkelerin ulusal ve uluslararası kişisel veri mevzuatlarında da düzenlendiği görülmektedir[174].

Tüzük m.5'de kişisel verilerin işlenirken ve aktarılırken uyulması gereken temel prensipler düzenlenmiştir. Bu prensipler; kişisel verilerin hukuka uygun, dürüstlük ve şeffaflık ilkesi çerçevesinde işlenmesi (Tüzük m.5/1-a), belirli, açık ve meşru amaçlarla işlenmesi (m.5/1-b, 13,14), kişisel verilerin elde edilme amacıyla ilgili ve bu amacı aşmayacak biçimde işlenmesi (m.5/1-c), işlenen kişisel verilerin doğru ve güncel olması (m.5/1-d), kişisel verinin saklanma amacı için gereken süre ile sınırlı olarak tutulmasıdır (m.5/1-e). "Veri kalitesi prensipleri" şeklinde adlandırılan bu ilkeler, OECD Rehber İlkeleri ile mülga Direktif m.6'da yer alan bu ilkeler ile de benzerlik göstermektedir ve KVKK m.4/2'de de yine bu prensipler esas alınarak

[171] Ebru Yeniman Yıldırım, Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması, s.5
[172] Hakan Çetin, Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi, s.2

[174] Aksoy, s.101.

veri işlemenin genel ilkelerine yer verilmiştir. KVKK m.4'te yer alan ve *"kişisel verilerin işlenmesinde genel ilkeler"* başlığı altında düzenlenen ilkeler kişisel veri koruma hukukunun temel yapı taşlarını teşkil etmekte ve KVKK ve alt mevzuat hükümlerinin uygulamasında ve yorumlanmasında da her zaman göz önünde tutulması gereken esas kurallardır[175]. Bu maddeye göre kişisel verilerin işlenmesi sırasında uyulması gereken temel ilkeler; *"hukuka ve dürüstlük kurallarına uygun olma", "doğru ve gerektiğinde güncel olma", "belirli, açık ve meşru amaçlar için kullanma", "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"*dir[176]. Söz konusu ilkelerin herhangi bir veri işleme faaliyeti ayrı tutulmaksızın grup şirketler tarafından ve bu şirketler bünyesindeki bütün departman ve birimlerde gerçekleşen veri işleme faaliyetleri için uygulanması gerekmektedir. Diğer bir deyişle kişisel verilerin işlenmesine ilişkin ilkeler tüm kişisel veri işleme faaliyetlerin özünde bulunmalı ve söz konusu faaliyetler bu ilkelere uygun olarak gerçekleşmelidir.

Temel ilkelerin yanı sıra çok uluslu grup şirketler arasındaki kişisel veri aktarımlarında veri güvenliğinin sağlanması için alınması gereken diğer bir yükümlülük ise aktarıma tabi tutulacak kişisel verilerin ilgili kişilerinin söz konusu aktarım faaliyetine ilişkin olarak kapsamlı ve KVKK m.10 uyarınca belirtilen şartlar altında bilgilendirilmesi ve aktarımı gerçekleştiren şirketin aydınlatma yükümlülüğünü yerine getirmesidir. Aydınlatma yükümlülüğünün uygun bir şekilde yerine getirilmesi ile aktarıma tabi tutulan kişisel verilerine ilişkin KVKK ve alt mevzuat hükümlerinde tanınan haklar hakkında bilgi sahibi olan ilgili kişiye bu hakları etkili bir şekilde kullanabilmesi için gerekli çalışmaların yürütülmesi gerekmektedir[177]. Bu kapsamda aktarımın tarafı olan grup üyesi şirketlerin ilgili kişi taleplerine yönelik olarak başvuru ve şikâyet mekanizmalarını belirlemesi ve uygulamaya koyması veri güvenliğinin sağlanması noktasında büyük önem arz

[175] Akdağ, s.71.
[176] Özkan, s.103.
[177] Şehriban İpek Aşıkoğlu Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda, s.5

etmektedir. Diğer taraftan çok uluslu grup şirketler arasında aktarılacak kişisel verilerin güvenliğinin sağlanması, ilgili grup üyesi şirketçe kişisel verilerin işlendiği ve aktarıldığı gerek fiziki gerekse elektronik ortamlarda mevcut risk ve tehditlerin belirlenerek gerekli idari ve teknik tedbirlerin alınması ve topluluk çalışanlarının kişisel verilerin korunması alanındaki farkındalığını artıracak eğitimlere tabi tutulması da büyük oranda ilgilidir. Çalışmamızın bu bölümde çok uluslu grup şirketler bakımından kişisel veri aktarım faaliyetleri yürütülürken veri güvenliğinin sağlanması adına uyulması gereken temel veri işleme ilkeleri ve bu kapsamda yerine getirilmesi gereken yükümlülükler ile alınabilecek idari ve teknik tedbirleri inceleyeceğiz.

2.4.2. Hukuka ve Dürüstlük Kuralına Uygun Olma İlkesi

Hukuka ve dürüstlük kuralına uygun şekilde veri işlenme ilkesi, diğer ilkelerin de temeli niteliğinde olan ve ilk sırada gelen bir ilkedir. Tüzük m.5/1-a'da da kişisel verilerin hukuka ve dürüstlük kuralına uygun şekilde işlenmesi gerektiği ifade edilmiştir. *"Hukuka uygun olma ilkesi",* kişisel veri işleme faaliyetlerinin kanunlara ve diğer mevzuat hükümlerine uygun bir şekilde gerçekleşmesi gerektiğini de içene alan bir ilkedir ancak bu faaliyetlerin yalnızca mevzuata uygun olması değil, aynı zamanda hukukun temel ilkelerine de uygunluğunu amaçlamaktadır. Hukuka ve dürüstlük kurallarına uygun hareket etme yükümlülüğü grup şirketler için kişisel verilerin herhangi bir mevzuat ile sınırlı kalınmaksızın her türlü kanun hükmüyle ve hukuk düzenlemeleriyle uyumlu olunması anlamına gelmektedir[178]. Dürüstlük kuralları uyarınca çok uluslu grup şirketlerin kişisel veri işleme ve aktarım faaliyetleri süresince ilgili kişinin haklı menfaatlerine ve çıkarlarına aykırı hareket etmemesi ve bu yönde bir sonucun ortaya çıkmasına doğrudan ya da dolaylı olarak sebep olmaması gerekmektedir. Diğer bir deyişle dürüstlük kuralları uyarınca veri sorumlusu sıfatıyla grup üyesi şirketlerden her birinin verileri işlenen ve grup içinde aktarıma tabi tutulan ilgili kişinin makul beklentilerini karşılaması

[178] Özdemir, s. 137; Küzeci, s. 201.

önerilmektedir[179]. Bununla birlikte aktarımın tarafı olan grup üyesi şirketlerin kişisel veri aktarım faaliyetleri sonucu ilgili kişinin bu aktarımdan beklemediği ve beklemesinin de gerekmediği sonuçların ortaya çıkmasını önleyici tedbirler alması gerekmektedir.

Dürüstlük kuralına uygun bir şekilde veri aktarım faaliyeti gerçekleştirilmesi verileri aktarılan ilgili kişinin gerçekleşecek veri aktarım faaliyetine ilişkin bilgilendirilmesini de içine alır. Bu kural veri sorumlusu sıfatıyla grup üyesi şirket tarafından ilgili kişinin gerçekleşen veri aktarım faaliyetiyle ilgili aydınlatılmasının temel dayanağı niteliğindedir. İlgili kişinin veri aktarım faaliyetinin amacı ve diğer ayrıntıları ile bu aktarım karşısındaki haklarına ilişkin olarak bilgilendirilmesi ve aktarımın doğuracağı sonuçlarıyla ilgili gerekli hususlarda uyarılması gerekmektedir[180]. Bu bakımdan grup üyesi her bir şirketin kişisel veri aktarım faaliyetleri boyunca şeffaf olması[181], ilgili kişiyi aktarıma ilişkin bilgilendirmesi ve hesap verilebilir bir şekilde aktarım faaliyetlerini yürütmesi beklenmektedir. Görüldüğü üzere hukuka ve dürüstlük kuralına uygun olarak hareket etme yükümlülüğü genel nitelikli bir kural olup kişisel verilerin korunması mevzuatında öngörülen her türlü düzenlemeyi kapsamaktadır. Bu düzenlemelerin yanı sıra genel hukuk kuralları ile evrensel ilkelere de uygun hareket edilmesi anlamına gelmektedir.

Özellikle dürüstlük kuralı ile veri işleme faaliyetleri süresince ilgililerin verilerinin ihlal edilmemesi amaçlanmaktadır. Bu da veri sorumlusu sıfatıyla her bir grup üyesi şirketin veri aktarımında hakkını kötüye kullanmaması ve güven kurallarına riayet etmesi ile mümkündür. Diğer bir deyişle veri sorumlusu sıfatıyla grup üyesi şirketlerin kişisel veri aktarım hakkını amacına uygun bir şekilde kullanması beklenmektedir. Ayrıca dürüstlük kuralının içeriği her somut veri aktarım

[179]Küzeci, s.201.
[180]Afra Ece Kaya, Kişilik Hakkı Olarak Kişisel Veriler ve Yeni Kişisel Verilerin Korunması Kanunu, Terazi Hukuk Dergisi, Cilt:12, Sayı:125, Ocak 2017, s.67-80.
[181]Güray Dağ, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Yayımlanmamış Doktora Tezi, Marmara Üniversitesi, İstanbul, 2011, s.118.

faaliyetinde ayrıca değerlendirilmeli ve bu değerlendirme süresince objektif ilkelere dayanılmalıdır. Aksi halde ilgili kişilerin sübjektif durumları göz önünde bulundurularak gerçekleşen bir veri aktarım faaliyeti ilgili kişiler arasında da eşitliği olumsuz yönde etkileyebilecektir. "Dürüstlük kuralına uygun olma ilkesi" ile esasında TMK m.2'deki dürüstlük kuralının[182] kişisel verilerin korunması mevzuatında da korunmaya çalıştığı unutulmamalıdır[183].

2.4.3. Doğru ve Güncel Olma İlkesi

Çok uluslu grup şirketler arasında gerçekleşen kişisel veri aktarım faaliyetleri süresince gerçekleştirdiği aktarıma konu olan kişisel verilerin doğru ve güncel olması gerekmektedir. Bu kural yalnızca kişisel verilerin korunmasına değil, aynı zamanda işlem güvenliğinin sağlanması ile aktarımın diğer hukuk kurallarına da uyumlu bir şekilde gerçekleşmesi için büyük önem arz etmektedir. Grup şirketler arasında doğru olmayan veya güncellenmesi gereken kişisel veriler üzerinden gerçekleşen veri aktarım faaliyetleri aktarım amacının tam olarak gerçekleşmemesine de yol açabilecektir. Bununla birlikte bu durum aktarımın tarafı olan grup üyesi şirketlerin hukuki ve ticari olarak da zarar görmesine yol açacaktır. KVKK m.11'de ve ilgili kişilere tanınmış kişisel verilerin düzeltilmesini talep etme [184] hakkı da esasında kişisel verilerin güncel ve doğru olması ilkesinin yerine getirilmesi yükümlülüğüne dayanmaktadır. Bu hakkın ilgili kişiye sunulabilmesi ve etkin bir şekilde yerine getirilebilmesi[185] için ilgili kişinin gerçekleşen veri aktarım faaliyetlerine konu kişisel verilerinin güncel ve doğru olması gerekmektedir. Ayrıca kişisel veri aktarımı gerçekleştiren grup şirketin söz konusu aktarıma ilişkin olarak ilgili kişiyi aydınlatması da büyük bir önem taşımaktadır. Öyle ki bu aydınlatma faaliyeti ilgili kişilere haklarının tam bir şekilde bildirilmesini

[182] Dürüstlük kuralı, hak ve borçlarını yerine getirirken orta zekalı, makul ve dürüst bir kişiden aynı durum ve koşullarda yapmaları beklenecek şekilde davranma yükümlülüğüdür, bkz. Gökhan Antalya, Murat Topuz, Medeni Hukuk C. I, Genişletilmiş 3. Baskı, Ankara 2019, s. 494.
[183] Özdemir, s.138.
[184]Oğuz Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınları, İstanbul 2010, s.90.
[185] Özdemir, s.138.

sağlamaktadır ve ilgilinin hakları konusunda yeterli bir şekilde bilgilenmesi sayesinde grup üyesi şirket tarafından bu ilkeye uyum sağlanması da kolaylaşmaktadır. Çünkü aktarılan kişisel verilerin güncel veya doğru olmaması halinde bunun ilgili kişi tarafından tespit edilmesi üzerine ilgili kişi tarafından düzeltme talebinde bulunulması halinde ilgili grup üyesi şirket tarafından kişisel verilerin güncel ve doğru olması sağlanabilecektir.

Veri sorumlusu her bir grup üyesi şirketin işlediği ve diğer bir grup üyesi şirkete aktardığı kişisel verilerin doğru ve güncel olmasını sağlamak konusunda aktif bir özen yükümlülüğü bulunmaktadır[186]. Bu sebeple her bir grup üyesi şirketin bu amaçla belirli dönemlerde tuttuğu belge ve kayıtlarını güncellemesi ve kendilerine gelen düzeltme talepleri[187] uygun bir şekilde yerine getirmesi gerekmektedir. Aksi halde grup şirketler arasında ilgili kişiye ait eski ya da yanlış bir banka hesap numarası kullanılarak çalışana yönelik yapılmak istenen ödemenin farklı kişilere gönderilmesi ya da grup üyesi şirketin müşterisine ait yanlış veya güncel olmayan bir adrese tebligat göndermesi veyahut teslimatta bulunması gibi büyük zararlar ortaya çıkabilecektir. Ayrıca yanlış veya eksik tutulan kişisel verilerin işlenmesi ve aktarımı halinde ilgili kişinin temel hak ve hürriyetlerine, ekonomik çıkarlarına veya manevi bütünlüğüne de zarar gelmesi muhtemeldir[188]. Bu yönüyle kişisel verilerin güncel ve doğru olması ilkesi hem ilgili kişi hem de aktarıma taraf olan ilgili grup üyesi şirketler için büyük önem arz etmektedir[189].

Çok uluslu grup şirketler tarafından aktarılacak kişisel verilerin doğruluğunun sağlanması bu verilerin toplandığı kanalların ve kaynakların da güvenilirliğinin belirlenmesini gerekli kılmaktadır. Bu bakımdan verilerin toplanma şekli büyük bir önem arz etmektedir. Grup üyesi şirketler kişisel verilerin toplandığı kaynakların geçerliliğini ve güvenirliliğini kontrol etmeli ve bu kontrol sonucu veri kaynağının

[186] Özkan, s.107.
[187] Akgül, s.157-158; Özdemir, s.138.
[188] Develioğlu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2017, s.48.
[189] Develioğlu, s.48; Göçmen Uyarer, s.122.

güvenilir olduğu kanısına varması halinde kişisel veri aktarımında bulunmalıdır. Bu kapsamda her bir grup üyesi şirketin aktarıma tabi kişiler verilerin doğru ve güncel şekilde tutulması amacıyla gereken idari ve teknik tedbirleri almakla sorumlu olduğunu belirtmek gerekir[190].

2.4.4. Belirli, Açık ve Meşru Amaçlarla İşlenme İlkesi

Kişisel verilerin her bir grup üyesi şirket tarafından belirli, açık ve meşru amaçlar uyarınca işlenmesi ve aktarıma tabi tutulması gerekmektedir. Bu ilke uyarınca bir kişisel verinin işleme amacının anılan üç şartı da sağlaması bir zorunluluktur. Belirli ve açık, fakat meşru olmayan bir amaçla ya da meşru ancak açık olmayan bir amaçla gerçekleşen veri işleme faaliyeti hukuka aykırı olarak kabul edilecektir. Kişisel verilerin açık bir amaç için işlenmesi ilgili kişinin kişisel veri işleme faaliyetini açık bir şekilde anlamasını ifade etmektedir. Öyle ki aktarımı gerçekleştirecek olan grup üyesi şirket tarafından ilgili kişi, kişisel veri işleme ve dolayısıyla aktarım faaliyetinin amacı ve sonuçlarına ilişkin açık bir şekilde bilgilendirilmelidir.

Kişisel verilerin meşru bir amaç uyarınca işlenmesi ve aktarımı ise bu faaliyetin ancak KVKK'da öngörülen hukuka uygunluk sebeplerinden en az birine dayanması ile mümkündür. Buna göre veri sorumlusu sıfatıyla her bir grup üyesi şirketin kişisel veri aktarımları esnasında yukarıda belirttiğimiz veri işleme şartlarından en az birine dayanması gerekmektedir ve aksi halde yapılacak kişisel veri aktarım faaliyeti hukuka aykırı olarak değerlendirilecektir[191]. Kişisel verilerin meşru bir amaçla işlenmesi ve aktarımı veri işleme ve aktarım faaliyetlerinin her zaman veri sorumlusunun meşru menfaatine uygun olarak gerçekleştiği anlamına gelmez. Meşru amaç veri sorumlusunun meşru menfaatinden çok daha geniş bir kavramdır. Bu bakımdan meşru amaç veri sorumlusu sıfatıyla grup üyesi şirket tarafından veri

[190]Ayözger Öngün, s.145.
[191]Kurul Kararı, 01.10.2019 T., 2019/294 K. https://www.kvkk.gov.tr/Icerik/6556/2019-294 Erişim Tarihi: 05.12.2021.

işleme ve aktarım faaliyetinin sözleşmenin ifası, hukuki yükümlülüğünün yerine getirilmesi ya da bir hak tesis etmesi şeklinde KVKK m.5 uyarınca öngörülen işleme şartlarından birine dayandırılması mümkündür. Örneğin grup üyesi bir şirketin bir sözleşmenin ifası amacıyla gerçek kişi müşterisine ait kimlik ve banka bilgilerini diğer bir grup üyesi şirkete aktarması meşru bir amaçla kişisel verilerin aktarıldığı anlamına gelmektedir.

Kişisel verilerin belirli bir amaç uyarınca işlenmesi ise veri işleme faaliyetinin yöneldiği amacın önceden belirlenmiş olması ve bunun halihazırda ilgiliye bildirilmiş olmasını ifade etmektedir. Bunun için toplanan kişisel verilerin hangi amaçla işleneceklerinin ilgili grup üyesi şirket tarafından işin gereği, şirket veya topluluğun kurumsal politikası vb. uyarınca kesin bir şekilde önceden belirlenmesi ve akabinde bu amaca ilişkin olarak ilgili kişinin gereğine uygun bir şekilde bilgilendirilmesi gerekmektedir. Bu sebeple her bir grup üyesi şirketin kişisel verilerin belirli bir amaç için işlenebilmesini ve aktarımını sağlamak adına ilgili kişiye yönelik yapacağı aydınlatma yükümlülüğünü tam bir şekilde yerine getirmesi büyük önem arz etmektedir. Aksi halde grup üyesi şirketlerin kişisel verileri ilgili kişiye bildirdiği amaç dışında aktarıma tabi tutması bu ilkeye aykırı hareket etmesi sonucunu doğuracaktır.

Kişisel verilerin işlenme amacının yalnızca ilgili grup üyesi şirket veya şirketler topluluğu üyesi olan diğer grup şirketler tarafından bilinmesi ve tahmin edilebilir olması da kişisel verilerin işlenme amaçlarının açık ve belirli olması ilkesine aykırılık teşkil etmektedir. Yukarıda belirtildiği üzere ilgili grup üyesi tarafından söz konusu amaçların ilgisi kişiye de bildirilmesi gerekmektedir. Bu bilgilendirme ise kişisel verinin işlenme ve aktarım amaçlarının açıklandığı ayrıntılı aydınlatma ve açık rıza metinlerinin hazırlanması ve ilgili kişiye uygun bir şekilde sunulması ile yerine getirilebilecektir. Aynı zamanda ilgili kişi tarafından aktarıma taraf olan grup üyesi şirkete yapılan başvurulara yönelik verilecek cevaplarla da işleme ve aktarım amacına ilişkin detayların ilgili kişiye sunulması mümkündür. Bu süre zarfında grup üyesi şirketin ilgili kişiye karşı anlaşılabilir olma kaygısı gütmesi ve

olabildiğince teknik terminoloji kullanmaktan kaçınması faydalı olacaktır[192]. Bununla birlikte topluluk bünyesinde Türkiye'de yürüttüğü veri işleme faaliyetleri ile veri sorumlusu olarak faaliyet gösteren grup üyesi şirketler tarafından VERBİS'e yapılacak bildirim yükümlülüğü esnasında da kişisel verilerin işlenme ve aktarım amaçlarının açık ve anlaşılır bir şekilde belirtilmesi gerekmekte, söz konusu grup üyesi şirketler tarafından yürütülen her türlü veri işleme ve aktarım faaliyetlerinin işleme amaçlarının da veri sorumlusu olarak ilgili grup üyesi şirket tarafından hazırlanan kişisel veri envanterlerinde açıkça yazılması gerektiği unutulmamaktadır.

2.4.5. Amaçla Bağlantılı, Sınırlı ve Ölçülü İşlenme İlkesi

Çok uluslu grup şirketler tarafından kişisel veri işleme ve aktarım faaliyetlerinin kişisel verinin işlenme ve aktarım amaçlarıyla bağlantılı, sınırlı ve ölçülü olarak gerçekleşmesi gerekmektedir. Kişisel verilerin işlenme ve aktarım amacıyla bağlantılı ve sınırlı olarak işlenmesi aktarımda bulunan grup üyesi şirket tarafından kişisel verinin aktarım için belirlenen amacın ötesinde işlenmemesi anlamına gelmektedir [193]. Dolayısıyla ilgili grup üyesi şirketi yalnızca açık, belirli ve meşru bir şekilde belirlediği amaç için gerekli ve elverişli olan kişisel verileri işleme ve aktarım faaliyetine tabi tutmalıdır[194]. Bu kapsamda grup üyesi şirketin işleme amacının gerçekleştirilmesi dışında kalan ve esasında ihtiyaç duyulmayan kişisel verileri işlemeye ve aktarım faaliyetlerine tabi tutmaya son vermesi ve bu verileri derhal imha etmesi uygun olacaktır.

Bu ilke uyarınca grup üyesi şirketlerin sonradan ortaya çıkma ihtimali bulunan ihtiyaçların göz önünde bulundurarak da veri işleme ve aktarım faaliyetlerini

[192]Ayözger Öngün, s.136; Özkan, s.108.
[193] Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, On İki Levha Yayıncılık, İstanbul, 1. Baskı, 2015, s.30; Develioğlu, s.46.
[194]Sevgi Eraslan Türkmen, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller,1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019, s.121.

sürdürmemesi gerekir[195][196]. Öyle ki ilgili kişinin bir kişisel verinin ilgili grup şirketi tarafından kendisinden elde edilmesi halinde ilgili kişi nezdinde bu kişisel verinin haklı olarak yalnızca kendisine bildirilen ve gerekli görülen amaç için işleneceği ve aktarılacağı düşüncesi bulunmaktadır. Bu haklı beklentinin karşılanmaması ve ilgili grup üyesi şirket tarafından verinin ilgili kişiye bildirilen amaç dışında ve ileride ortaya çıkabilecek başka bir ihtiyaç uyarınca aktarılması halinde ise yeni bir veri işleme faaliyeti gerçekleştiği kabul edilecektir. Bu durumda ilgili grup üyesi şirket tarafından gerçekleştirilen bu yeni veri işleme faaliyeti için KVKK'da öngörülen veri işleme şartlarından en az birinin tekrar sağlanması gerekecektir [197].

Bununla birlikte ölçülülük ilkesi uyarınca aktarımda bulunacak grup üyesi şirketten veri aktarım faaliyeti ile hedeflediği amaç arasında makul bir dengenin bulunması beklenir[198]. Bu ilke ancak aktarım ile hedeflenen amacın gerektirdiği ölçüde verinin aktarıma tabi tutulması anlamına gelmektedir. Örneğin yurt dışında kurulu olan hâkim şirket tarafından düzenlenen bir eğitime Türkiye'deki bağlı şirketten bir çalışanın katılım sağlayacak olması halinde bağlı şirket tarafından eğitime katılacak çalışan ile ilgili din verisinin hâkim şirkete aktarımı ölçülü bir veri işleme ve aktarım faaliyeti olarak değerlendirilemeyecektir. Hâkim şirket tarafından eğitime katılım için gerekli görülen kişisel veriler dışında bir aktarım faaliyeti gerçekleştirilmesi ölçülülük ilkesine aykırı olarak kabul edilecektir. Bu sebeple aktarımda bulunacak ilgili grup üyesi şirketin her bir veri işleme ve aktarım faaliyeti özelinde veri minimizasyonunu sağlaması uygun olacaktır.

2.4.6. Gereken Süre Boyunca Muhafaza Edilme İlkesi

Kişisel verilerin muhafaza edilmesi de tıpkı kişisel verilerin aktarımı gibi bir kişisel veri işleme faaliyeti olarak kabul edilmekte ve bu sebeple saklama faaliyetleri esnasında grup üyesi şirketler bakımından kişisel verilerin işlenmesine ilişkin

[195] Özdemir, s.142; Korkmaz, s.116.
[196] Akdağ, s.75.
[197] Ayözger Öngün, s.138.
[198] Özkan, s.112.

mevzuat hükümlerinin yerine getirilmesi gerekmektedir. KVKK m.12 uyarınca veri sorumlusu sıfatıyla her bir grup üyesi şirketin kişisel verilerin saklanmasına ilişkin gerekli güvenlik ve gizlilik önlemlerini alması, bu kapsamda kişisel verilerin saklandığı ortamların güvenliklerini sağlanması ve kişisel verilerin aktarım öncesi veya sonrası ilgili grup üyesi şirket tarafından belirlenen saklama sürelerinin de işleme amacının gerektirdiğinden daha uzun bir süre olmaması gerekmektedir. Amaçla sınırlılık ilkesi uyarınca kişisel veriler yalnızca işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Bu süre belirli durumlarda mevzuattan kaynaklanmakta bazense işin niteliğinden ortaya çıkmaktadır. Örneğin grup üyesi şirketin iş sağlığı ve güvenliğine ilişkin kayıtları ilgili mevzuat uyarınca çalışanının işten ayrılışından itibaren 15 yıl kadar daha saklayabileceği düzenlenmişken ilgili grup üyesi şirkete yapılan iş başvurularına ilişkin kayıtların ise ne kadar süreyle saklanması gerektiği herhangi bir mevzuat hükmüyle düzenlenmemiştir. Grup şirketler tarafından kişisel verinin saklanmasına ilişkin süre belirlenirken saklanacak kişisel verinin işlenme amacına bağlı olarak ilk etapta ilgili mevzuat hükümlerinin incelenmesi büyük önem arz etmektedir. Bu kapsamda ilgili mevzuat uyarınca öngörülen zamanaşımı ve hak düşürücü sürelere itibar edilerek yürütülen muhafaza faaliyetleri hukuka uygun kabul edilebilecektir. Ancak söz konusu kişisel verinin işlenme ve aktarım amacına ilişkin mevzuatta herhangi bir yasal süre sınırlaması öngörülmemesi halindeyse ilgili grup üyesi şirketin bu süreyi işin niteliğini değerlendirerek makul bir şekilde belirlemesi gerekmektedir. Bu kapsamda belirlenecek makul süre ise söz konusu kişisel verinin işleme ve aktarım amacıyla uygun olmalıdır.

Grup şirketler tarafından belirlenen saklama süresine şirketin saklama ve imha politikasından açık bir şekilde yer verilmesi gerekmektedir. Bununla birlikte Türkiye'de veri işleme faaliyetleri gösteren ilgili grup üyesi şirket için hazırlanan kişisel veri envanterlerinde ve yapılacak VERBİS kaydı bildiriminde de bu şirket tarafından kişisel verilerin hangi sürelerle saklandığının belirtilmesi beklenmektedir. Bu sayede ilgili grup şirketin işlediği kişisel verilerin ne kadar süreyle saklandığı da aleniyet kazanmaktadır. Bu sürenin sona ermesinin ardından

kişisel verilerin ilgili grup üyesi şirket tarafından derhal imha edilmesi gerekmektedir[199]. Söz konusu imha işlemi kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesi ile gerçekleştirilebilecektir. Aksi halde saklama süresi dolan kişisel verinin muhafaza edilmeye devam etmesi ilgili grup üyesi şirket tarafından hukuka aykırı bir şekilde kişisel verilerin işlenmesi sonucuna yol açabilecektir. Ayrıca ilgili grup üyesi şirket tarafından ileride veri işleme veya aktarım faaliyetine tabi tutulacağı gerekçesiyle belirli verilerin saklanmasına devam edilmemesi de faydalı olacaktır. Bu halde işleme amacı ve kişisel veri arasındaki nedensellik bağı sona ermekte ve kişisel verinin işlenme ve saklanması faaliyeti işlevsiz duruma gelmektedir[200].

2.4.7. Aydınlatma Yükümlülüğünün Yerine Getirilmesi

Aydınlatma yükümlülüğü KVKK m.10'da düzenlenmiş olup esasında kişisel veri işleme faaliyetine ilişkin olarak ilgili kişiye bilgi verilmesi amacını taşımaktadır. Aydınlatma yükümlülüğü gerek doğrudan veri sorumlusunun kendisi ya da varsa ve bu hususta yetkilendirilmişse veri işleyen tarafında da yerine getirilebilmektedir. KVKK m.10 uyarınca aydınlatma yükümlülüğü ile işleme ve aktarım faaliyetine yerine getiren veri sorumlusunun ve varsa temsilcisinin kim olduğunun, ilgili kişiye kişisel verilerinin hangi amaçlarla ve hukuki sebeplere dayanılarak işlendiğinin, işlenen bu kişisel verilerinin hangi yollarla toplanmış ve elde edilmiş olduğunun, bu verilerin üçüncü bir kişiye aktarılacak ise aktarılacak alıcı grubunda hangi kişilerin bulunduğunun ve hangi amaçlarla aktarımın gerçekleşeceğinin ve ilgili kişinin KVKK m.11 uyarınca sahip olduğu kişisel veri haklarının neler olduğunun bildirilmesi gerekmektedir[201]. Veri güvenliğinin sağlanması adına ilgili kişinin veri işleme ve aktarım faaliyetlerine ilişkin bilgilendirilmesi büyük önem taşımaktadır. Çünkü kişisel verilerinin işlendiğini ve/veya aktarıldığını bilmeyen ya da bilse de bu işleme ve aktarım faaliyetlerinin detayları hakkında tam olarak bilgi sahibi

[199] Göçmen Uyarer, s.125.
[200] Küzeci, s.215.
[201] Taştan, s.158; Cihan Avcı Braun, Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, Haziran 2018, s.19.

olmayan ilgili kişi, KVKK m.11 uyarınca kendisine tanınan kişisel veri aktarım haklarından tam olarak yararlanamayacaktır.

Bu açıdan ilgili kişinin aydınlatılması, gerek ilgili kişinin grup üyesi şirket tarafından yürütülen işleme ve aktarım faaliyetlerine karşı kanunen sahip olduğu haklarından haberdar olması ve gerekli gördüğü durumlarda bu haklarını kullanabilmesi gerekse bu hakların kullanılmasına imkan vererek varsa grup üyesi şirketin ilgili kişinin haklarına halel getirecek veya eksik ya da yanlış bir biçimde gerçekleştirdiği kişisel veri işleme ve aktarım faaliyetine ilişkin gerekli çalışmayı gerçekleştirerek bu faaliyetin hukuka uygun hale getirilmesine yardımcı olmaktadır. Görüldüğü üzere aydınlatma yükümlülüğünün yerine getirilmesi ile bu yükümlülüğe bağlı olarak kişinin KVKK m.11 uyarınca öngörülen ilgili haklarına ilişkin bilgilendirilmesi ve bu hakların etkin bir şekilde ilgili grup üyesi şirket tarafından geliştirilecek şikâyet mekanizmaları ile uygulamaya geçirilmesi veri işleme ve aktarım faaliyetinin hukuka uygunluğu açısından da büyük önem taşımaktadır.

Diğer taraftan aydınlatma yükümlülüğü ile kişisel veri işleme ve aktarım faaliyetine şeffaflık kazandırılmak[202] ve bu yükümlülüğün ifası ile aydınlatma yükümlülüğünü yerine getiren grup şirketler ilgili kişiye ve hatta Kurum'a karşı bir taahhüt altına girmektedir. Şu kadar ki bu taahhüt ilgili grup üyesi şirket tarafından gerçekleştirilecek kişisel veri işleme ve aktarım faaliyetinin ilgili kişiye bildirilen şekilde ve sınırlarda gerçekleşecek olmasıdır. KVKK m.10 uyarınca getirilen bu yükümlülük ile veri sorumlusu ve veri işleyen grup şirketler aktarıma tabi tutulacak kişisel verileri keyfiyete yer verecek şekilde ve gelişigüzel olarak işleyemeyecek ve aydınlatma yükümlülüğü uyarınca ilgili kişiye bilgi verdiği şartlarla sınırlı kalacaktır. Görüldüğü üzere aydınlatma yükümlülüğünün yerine getirilmesi veri sorumlusu ve veri işleyen grup şirketlerin ilgili veri sahibi kişi tarafından sürekli bir denetimi ve gözetimi altında olmasını da teşvik etmektedir. Şeffaflık ilkesi ile bağlı

[202] Dülger, s.297.

olarak ilgili grup üyesi şirket tarafından yerine getirilecek aydınlatma yükümlülüğü kapsamında verilen bilgilerin veri sorumluları tarafından bildirimde bulunulan VERBİS kaydında yer alan bilgiler ile uyuşması da Tebliğ kapsamında düzenleme altına alınan yükümlülüklerden biridir[203].

KVKK m.10'da genel hatlarıyla düzenleme altına alınan aydınlatma yükümlülüğüne ilişkin Kurum tarafından çıkarılan ve 10 Mart 2018 tarihinde Resmî Gazete'de yayımlanan *"Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"* ("Tebliğ") de bu konuya ilişkin olarak ayrıntılı düzenlemeler içermektedir. Tebliğ m.5/1 uyarınca aydınlatma yükümlülüğü sözlü veya yazılı yapılabilmektedir. Buna göre grup üyesi şirket gerçekleştireceği veri işleme ve aktarım faaliyetlerine ilişkin aydınlatma yükümlülüğünü somut olayın niteliğine uygun düştüğü sürece internet sitesinde yayınlayarak ya da iş yerindeki ilan panosuna asarak veya ilgili kişilere bu hususta ses kaydı göndererek ya da onlara çağrı merkezi yoluyla ulaşarak fiziki ya da elektronik ortamlar aracılığıyla yerine getirilebilecektir[204]. Tebliğ m.5/1 (e) uyarınca aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna bırakıldığından ilgili grup üyesi şirket tarafından bu yükümlülüğün ilerleyen dönemlerde ortaya çıkabilecek herhangi bir uyuşmazlığı önlemek ya da bu uyuşmazlıkta ileri sürebilmek adına yazılı yollarla yapılması faydalı olacaktır. Bununla birlikte aydınlatma yükümlülüğünün ne zaman yerine getirilmesi gerektiği de incelenmesi gereken bir husustur. Kural uyarınca ilgili kişi en geç veri işleme ve aktarım faaliyetine başlanılmadan önce aydınlatılmalıdır. Diğer taraftan Tebliğ m. 6/1 uyarınca kişisel verilerin doğrudan ilgili kişiden elde edilmemesi halinde kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde yerine getirilmesi gerektiği belirtilmektedir[205]. Öte yandan aydınlatma yükümlüğünün yerine getirilmesi ilgili kişinin talebine bağlı olmayıp ilgili grup üyesi şirket tarafından yapılacak veri işleme ve aktarım faaliyetiyle ilgili olarak ilgili kişiden herhangi bir

[203] Dülger, s.301.
[204] Dülger, s.298.
[205] Dülger, s.303.

talep gelmese de kanuni olarak bu yükümlülüğün KVKK ve Tebliğ kapsamında öngörülen şartlara eksiksiz bir şekilde uyulmak suretiyle yerine getirilmesi gerekmektedir.

İlgili grup üyesi şirket tarafından yapılacak her bir veri işleme ve aktarım faaliyeti ve bu faaliyetin detayları ilgili kişiye yapılacak aydınlatma metninde yer almalı ve ilgiliye bildirilmelidir. Aydınlatma metninde yer alan hususlardan herhangi birinin değişmesi halinde ise bu değişikliğin derhal ilgili kişiye bildirilmesi önem arz etmektedir. Öyle ki grup üyesi şirketler arasında yapılan kişisel veri aktarım faaliyetinin amacının değişiklik göstermesi halinde ilgili kişinin kişisel verilerinin aktarılmasına ilişkin yeni sebep hakkında bilgilendirilmesi gerekmektedir. Bununla birlikte Tebliğ m. 5/1 (a) uyarınca çok uluslu grup şirketler arasında yapılan aktarım faaliyetinin dayandığı veri işleme şartlarından hangisine dayanılırsa dayanılsın aydınlatma yükümlülüğünün yerine getirilmesi zorunludur. Bu kapsamda kişisel verilerin yurt dışındaki grup üyesi bir şirkete aktarımı halinde ilgili kişinin açık rızasının bulunması aktarımı gerçekleştirecek ilgili grup üyesi şirketin ilgili kişiyi aydınlatma yükümlülüğünü bertaraf etmeyecektir[206]. Bu noktada açık rızanın bilgilendirmeye dayalı olarak ilgili kişinin açıkladığı özgür irade beyanı olarak kabul edilmesi de yine açık rızanın geçerli olabilmesi için aydınlatma yükümlülüğünün gereğine uygun olarak yerine getirilmesinin önemini ortaya koymaktadır. Ancak aydınlatma yükümlülüğünün yerine getirilmesi ile ilgili kişinin açık rızası alınmış sayılmamakta, ilgili kişiye söz konusu veri işleme ve aktarım faaliyetine ilişkin açık rızasının olup olmadığı ayrıca yöneltilerek sorulmalıdır.

Son olarak aydınlatma yükümlülüğünün gereğine uygun bir şekilde yerine getirilebilmesi için grup üyesi şirketin ilgili kişi onun anlayacağı şekilde basit ve anlaşılır bir dil kullanarak bilgilendirmesi gerektiği unutulmamalıdır. Özellikle çok uluslu grup şirketler tarafından yerine getirilerek aydınlatma yükümlülüklerinin

[206] Dülger, s.300.

mümkünse ilgili kişinin bulunduğu ülkenin diline veya somut olayın şartları el veriyorsa İngilizce veya faaliyet alanlarının yoğunlaştığı ülkelerden birinin dilinde yerine getirilmesi de etkili bir şekilde bu yükümlülüğün yerine getirilmesi açısından önem taşımaktadır.

2.4.8. Başvuru ve Şikâyet Mekanizmalarının Oluşturulması

Şikâyet mekanizması, aydınlatma yükümlülüğü ile birlikte KVKK m.11 uyarınca ilgili kişiye tanınan kanuni hakların ilgili kişiye tebliğ edilmesi sonrası gerekli görmesi halinde ilgili kişinin bu hakları ilgili grup üyesi şirkete yönelik kullanabilmesi açısından büyük önem arz etmektedir. KVKK m. 11 uyarınca ilgili kişiye getirilen bu hak aynı zamanda Tüzük m.21'de de düzenleme altına alınmıştır. Tüzük uyarınca tanınan bu hakların başında ilgili kişinin veri işleme ve/veya aktarım faaliyetine ilişkin itiraz hakkıdır. Bu itiraz hakkı başı başına yürütülen veri işleme ve/veya aktarım faaliyetinin durdurulmasına veya sona erdirilmesine ilişkin olabileceği gibi aynı zamanda bu faaliyetin belirli noktalardan değiştirilmesine yönelik de olabilir. Fakat şu kadar ki ilgilisi kişinin itiraz hakkını kullanması halinde veri sorumlusu tarafından ilgili kişinin söz konusu veri işleme ve/veya aktarım faaliyetinde hak ve hürriyetlerine üstün gelen bir nedenin bulunması veya veri sorumlusunun bu faaliyetin bir hakkın tesisi, kullanılması veya savunulması için gerekli olduğunu ikna edici biçimde ortaya koyması halinde söz konusu veri işleme ve/veya aktarım faaliyetine devam edilebilecektir. Ayrıca Tüzük m.21/6 uyarınca veri işleme ve/veya aktarım faaliyetinin kamu yararına gerçekleştiği hallerde de itiraz hakkının somut olayın koşullarına göre reddedilebileceği düzenlenmektedir[207].

KVKK m.11 uyarınca kişisel verileri işlenen ve aktarılan herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; a) kişisel veri işlenip işlenmediğini öğrenme, b) kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) kişisel

[207] Yörük, s.83.

verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) KVKK m.7'de öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) talep üzerine veri sorumlusu tarafından düzeltme veya imha kapsamında yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) işlenen kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve ğ) kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğranması hâlinde bu zararın giderilmesini talep etme hakları bulunmaktadır. Söz konusu hakların tamamının ilgili grup şirket tarafından yapılacak aydınlatma kapsamında ilgili kişiye açık ve anlaşılır bir biçimde bildirilmesi gerekmektedir[208]. Bununla birlikte bu hakların bildirilmesinin yanı sıra bu taleplerin ilgili kişilerce hangi yollarla grup şirkete iletileceğinin de aydınlatma kapsamında belirtilmesi gerekmektedir[209]. Bu noktada veri sorumlusuna başvuru hususunu düzenleyen KVKK m.13 uyarınca ilgili kişi tarafından veri sorumlusuna yapılacak başvuruların yazılı olması gerektiğinden ilgili grup şirket tarafından yürütülen kişisel verilerin işlenmesine dair her türlü ilgili kişi taleplerinin kabul edildiği "kvkk" uzantılı bir e-posta adresinin belirlenmesi ve bu adrese gerek varsa grup şirketin internet sitesinde ve/veya ilgili kişilere yönelik sunacakları aydınlatma metinlerinde yer verilmesi faydalı olacaktır. İlgili grup şirket tarafından bu yönde oluşturulmuş özel bir e-posta adresi bulunmuyorsa şirketin kayıtlı elektronik posta (KEP) adresi ya da kurumsal e-posta adresi ya da varsa şirketin VERBİS kaydı esnasında bildirdiği irtibat kişisinin veya mevzuata uyuma görevlisinin e-posta adresi de kullanılabilecektir. Bununla birlikte e-posta adresi yerine başvuruların fiziki yollarla veri sorumlusunun ilgili kişiye bildireceği açık adresine iletilmesinin kararlaştırılması da mümkündür. Bu kapsamda esas olan başvuruların yazılı bir şekilde ve hangi kanaldan

[208] KVKK, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s.4
[209] Aşıkoğlu, s.48

yürütüleceğinin gerek ilgili grup üyesi şirket gerekse ilgili kişi tarafından belirli olmasıdır.

Veri sorumlusu tarafından ilgili kişi taleplerinin kabul alınacağı bu kanalların belirli aralıklarla kontrol edilmesi hak kayıplarının yaşanmaması ve veri sorumlusu tarafından olası bir hukuka aykırı veri işleme ve/veya aktarım faaliyetlerine devam edilmemesi açısından büyük önem taşımaktadır[210]. KVKK m. 13/2 uyarınca veri sorumlusu olarak ilgili grup üyesi şirketin kendisine yöneltilen talebi, talebin niteliğine göre en kısa sürede ve en geç otuz gün içerisinde sonuçlandırması gerekmektedir. Bu hükümde veri sorumlusu şirketin ilgili kişinin taleplerini yerine getirirken ilgili kişiden kural olarak herhangi bir ücret talep etmemesi gerektiği ve ancak bu talebin ek bir maliyet gerektirmesi halinde ilgiliden ücret talep edilebileceği düzenlenmiştir. Hükmün devamında ise bu kapsamda ilgili kişiden talep edilecek ücretin Kurul'ca belirlenen tarife üzerinden kararlaştırılacağı ve ilgili kişinin başvurusunun veri sorumlusunun hatasından ileri gelmesi halinde bu ücretin ilgili kişiye iade edilmesi gerektiği düzenlenmiştir. KVKK m. 13/3'te ise veri sorumlusunun bu talebi reddetmesi halinde bu ret beyanını gerekçesi ile birlikte ilgili kişiye yazılı olarak bildirmesi gerektiği belirtilmektedir. Ayrıca veri sorumlusu tarafından 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[211] ("Başvuru Tebliği")'de düzenlenen hüküm ve şartlara da uyulması gerekmektedir. Başvuru Tebliği m. 4 ve 5 hükümleri uyarınca ilgili grup üyesi şirkete yönelik yapılacak başvuruların, ilgili kişi tarafından ad, soyadı, T.C. kimlik numarası gibi gerekli bilgilerin başvuru esnasında belirtilmesi, veri sorumlusuna yazılı olarak başvuruda bulunulması, başvuruların Türkçe dilinde yapılması gibi belirli şartların yerine getirilerek yapılması gerektiği düzenleme altına alınmıştır. Ancak ilgili kişi tarafından bu şartların eksik bir şekilde yerine getirilmesi suretiyle başvuruda bulunulması halinde, ilgili grup üyesi şirketin veri sorumlusu olarak mümkünse

[210] Samet Saygı, 6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları, s.8
[211] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ (R.G. tarihi 10.04.2018), https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm

ilgili kişiyi başvurusunun hangi şartları sağlaması halinde dikkate alınabileceği konusunda bilgilendirmesi, gerek hak kayıplarının önüne geçilmesi gerekse bu başvuru sayesinde veri sorumlusu tarafından yapılan veri işleme faaliyetlerinin hukuka uygunlukları açısından tekrar değerlendirilme altına alınabilmesi adına önem arz etmektedir. İlgili kişi tarafından yapılacak başvuruların reddedilmesi ya da veri sorumlusunun otuz günden daha geç bir sürede başvuruya cevap vermesi veyahut başvurunun kabul edilmesine rağmen ilgili kişinin yapılan işlemin yeterliliğinden memnuniyet duymaması halinde ilgili kişinin KVKK m.14/1 uyarınca veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kurul'a şikâyet hakkı bulunmaktadır[212].

Bununla birlikte Kurul'a başvuruda bulunmanın ön şartı ilgili kişinin veri sorumlusuna başvuru yolu tüketmesi olup aksi halde Kurul tarafından bu başvuru usulden reddedilebilecektir[213]. Öte yandan KVKK m.14/3 uyarınca ilgili kişinin kişilik haklarını ihlal eden veri işleme ve aktarım faaliyetleri karşısında Kurul'a başvurunun yanı sıra hukuk ve/veya ceza mahkemelerine de başvurma ve tazminat talebinde bulunma ve/veya ilgili grup üyesi şirketin gerçek kişi yöneticilerinin cezai sorumluluklarına gitme hakkı da saklı tutulmuştur.

Çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına ilişkin olarak ilgili kişinin Türkiye'de kurulu grup üyesi şirkete başvuruda bulunmasına rağmen bu başvurusunun reddedilmesi ya da verilen cevabı yetersiz bulması ya da grup üyesi şirketin ilgili kişiye geç cevap vermesi halinde ilgili kişi şikâyet hakkını kullanarak Kurul'a başvuruda bulunabilecektir. KVKK m. 15 uyarınca Kurul'a yapılacak başvuruların 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun m.6'da öngörülen şartları taşıması gerekmektedir. Ancak bu şartları taşıyan şikâyet başvuruları üzerine inceleme yapacak Kurul, şikâyet tarihinden itibaren altmış gün içinde ilgili kişiye cevap vermezse bu durum ilgili kişinin talebinin reddedildiği

[212] KVKK, Başvuru Hakkı
[213] Saygı, 6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları, s.5

anlamına gelmektedir. Buna karşılık Kurul'un talebi inceleyerek ilgili kişiye cevap vermesi halinde bu cevabında ilgili kişinin talebini olumlu değerlendirirse Kurul, ilgili kişinin başvurusu üzerine incelediği kişisel veri işleme ve/veya aktarım faaliyetine ilişkin hukuka aykırılıkları tespit ederek bunların giderilmesi için ilgili veri sorumlusu grup üyesi şirkete bildirimde bulunacaktır. Bu durumda grup üyesi şirketin Kurul tarafından kendisine tebliğ edilen hukuka aykırılığı giderme talimatını gecikmeksizin ve her halde otuz gün içerisinde yerine getirmesi gerekmektedir. Kurul'un bu yönde verebileceği talimatlandırma kararlarının yanı sıra KVKK m. 15/7 uyarınca telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin Türkiye'de kurulu grup üyesi şirketten yurt dışındaki grup üyesi şirkete aktarılmasının durdurulmasına da karar verebilir. Kurul tarafından ilgili kişinin başvurusu üzerine verilen talimat kararının ilgili grup üyesi şirket tarafından zamanında ya da gereğine uygun bir şekilde yerine getirilmemesi ya da hiçbir şekilde yerine getirilmemesi halinde ilgili grup üyesi şirket KVKK m.17 uyarınca yaptırıma tabi tutulacaktır.

Tüzük m.55 gereğince de üye ülkelerde ilgili kişilerin talep ve şikayetlerini incelemekle görevli olacak bir veri denetim kurumu kurulacağı ve bu veri denetim kurumlarının kurulduğu ülkenin sınırları dahilinde Tüzük'ten doğan görev ve yetkileri kullanabileceği düzenlenmiştir. Buna karşılık KVKK düzenlemeleri ile uygun olarak üye devletlerde inceleme ve denetim göreviyle faaliyet gösterecek söz konusu veri denetim kurumlarının mahkemelerin yargı yetkisi dahiline giren alanlarda inceleme ve karar verme yetkisi bulunmadığı düzenlenmiştir[214]. Diğer taraftan çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının hukuka uygun bir şekilde gerçekleşmesi amacıyla hazırlanan ve Kurul'un onayına sunulan bağlayıcı şirket kurallarında da topluluk içi başvuru ve şikâyet mekanizmalarının öngörülmesi ve etkili bir şekilde yürütülmesi gerektiğine ilişkin düzenlemelere yer verilmesi gerekmektedir. Söz konusu düzenlemeler ile ilgili kişinin grup içi kişisel veri işleme ve aktarım faaliyetlerine ilişkin talep ve şikayetlerini hızlı ve kolay bir

[214] Yörük, s.114.

şekilde ilgili grup üyesi şirkete iletebilmesi ve bu başvuruların gecikmeksizin hukuka uygunluklarının değerlendirilerek bağlayıcı şirket kurallarında belirtilen topluluk içi mekanizmalarla etkili bir şekilde çözüme kavuşturulması amaçlanmaktadır. Çalışmamızın üçüncü bölümünde bağlayıcı şirket kurallarını incelenirken bu mekanizmalara gerektikçe tekrar değinilecektir.

2.4.9. Mevcut Risk ve Tehditlerin Belirlenmesi

Çok uluslu grup şirketler arasındaki kişisel veri işleme ve aktarım faaliyetlerinde KVKK ve alt mevzuat hükümlerine uygun hareket edilebilmesi için her bir grup şirketin kişisel verileri işleme ve aktarıma tabi tuttuğu fiziki ve elektronik ortamlardaki mevcut risk ve tehditleri belirlemesi gerekmektedir. [215] Öyle ki topluluk içi kişisel veri aktarımlarının hukuka uygunluklarının sağlanması ve veri güvenliğinin gerektirdiği idari ve teknik tedbirlerin alınabilmesi için topluluk bünyesinde kişisel verilerin korunmasına engel teşkil eden risk ve tehditlerin saptanması büyük önem taşımaktadır. Bu kapsamda her bir grup üyesi şirketin yürüttüğü kişisel veri işleme ve aktarım faaliyetlerinin alanında uzman danışmanlar tarafından gerek hukuki gerekse teknik açılardan incelenmesi ve bu incelemeler sonucu saptanan bulgular ile şirket özelinde bir risk analizi gerçekleştirilmelidir. Yapılacak risk analizleri bu risklerin ortaya çıkaracağı muhtemel kayıpların saptanması ve böylece gerek topluluğun gerekse ilgili kişilerin menfaatlerini korunması ve olası kayıpların önüne geçilmesi adına gerekli aksiyonlar alınabilecektir. Diğer taraftan her bir grup şirketin kişisel veri işleme ve aktarım faaliyetlerini sürdürdüğü elektronik ortamlara ilişkin risk analizleri yürütmesi de faydalı olacaktır. Bu kapsamda gerek yurt içindeki gerekse yurt dışındaki grup üyesi şirketlere kişisel veri aktarılan ortamların GAP analizi ve sızma testi gibi testlere tabi tutularak aktarımın yapılacağı sistemlerin alt yapılarında bulunan

[215] Kişisel Verileri Koruma Kurumu, Veri Güvenliği Rehberi, ISBN : 978-975-19-6834-O, KVKK Yayınları, Ankara, 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, Erişim Tarihi: 10.12.2021.

güvenlik açıkları tespit edilebilecek ve bu açıkların kapatılması adına gerekli yazılım ve donanımların temin edilmesi yoluna gidilebilecektir.

2.4.10. Çalışan Eğitimleri ve Farkındalık Çalışmaları

Çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının KVKK ve alt mevzuat hükümlerine uygun bir şekilde yürütülebilmesi adına her bir grup üyesi şirket tarafından kişisel verilerin korunması alanında çalışanlarına yönelik eğitimler verilmesi ve farkındalık çalışmaları düzenlenmesi büyük önem taşımaktadır. Her bir grup şirketin ticari faaliyetleri ile birlikte yaşayan bir canlı organizma olduğu göz önünde bulundurulduğunda bu organizmanın hareketi sağlayan temel taşlarını da çalışanları oluşturmaktadır. Öyle ki grup şirketin esasında her türlü faaliyeti çalışanları tarafından gerçekleştirildiğinden, aktarımların hukuki sınırlar dahilinde tutulabilmesinin sağlanması ancak şirketi temsil eden çalışanların kişisel verilerin korunması mevzuatına ilişkin farkındalıklarının artırılması ile mümkün olacaktır. Bu kapsamda her bir grup şirketin de çalışanlarının bu alandaki bilinç ve dikkat düzeylerini artırmak ve kişisel verilerin korunması alanındaki temel ilkeleri şirket kültürü haline getirmek yönünde aktif yükümlülüğü bulunmaktadır. Çalışanların grup içi kişisel veri aktarımlarındaki hukuka aykırılıkları veya eksiklikleri tespit edebilecek bilgi düzeyinde olması halinde bunun sonuçları hızlıca telafi edilebilmektedir[216]. Çalışanların gerekli güvenlik önlemlerinin alınmadığı internet sitelerini ziyaret etmesi, e-posta ortamındaki sahte hesaplardan gelen mesajlara yanıt vermesi ve bu hesaplara fark etmeden kişisel veri aktarımında bulunması, veri sorumlusu grup şirket için ciddi veri ihlallerine yol açabilecektir. Bununla birlikte çalışanın kullandığı yazılım programlarından birinin şifresini güçlü bir şekilde oluşturamaması ya da bu şifreyi üçüncü bir kişiyle paylaşması da grup şirket için önemli veri kayıplarına sebep olabilecektir. Bu sebeple çok uluslu grup şirketler arasında aktarıma tabi tutulan kişisel verilerin güvenliğinin sağlanması adına

[216] Kişisel Verileri Koruma Kurumu, Veri Güvenliği Rehberi, ISBN: 978-975-19-6834-O, KVKK Yayınları, Ankara, 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, Erişim Tarihi: 10.12.2021.

çalışanlara yönelik verilecek eğitimler ve farkındalık çalışmaları hayati bir rol oynamaktadır.

2.4.11. Diğer İdari ve Teknik Tedbirlerin Alınması

Çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının hukuka uygunluklarının temin edilmesi ancak bu aktarımlara konu olan kişisel verilerin güvenliğinin ve gizliliğinin sağlanması ile mümkündür. Söz konusu verilerin güvenlik ve gizliliklerinin sağlanması adına aktarımın taraflarını oluşturan grup üyesi şirketlerin gerekli idari ve teknik tedbirleri alması gerekmektedir. Bu tedbirler gerek kişisel verilerin aktarımı öncesi ve sonrasında işlendiği ve saklandığı elektronik ve fiziki ortamlar gerekse aktarımın yürütüldüğü kanallar için alınmalıdır[217]. Bu tedbirlerin alınması ile birlikte aktarıma konu kişisel verilerin olası bir veri ihlaline maruz kalmasının önüne geçilebileceği gibi ilgili grup üyesi şirketin kişisel verilerin korunması mevzuatından kaynaklanan idari ve cezai yaptırımlara maruz kalma riski de en aza inecektir. Topluluk bünyesinde kişisel verilerin işlendiği ve aktarıldığı ortamlara ve faaliyetlere örnek olarak şirket bilgisayarları tutulan belgeler, listeler, raporlar ve diğer kayıtlar, e-posta ortamında yapılan yazışmalar, arşivlenen faturalar, çizelgeler, görev dağılımları, sözleşmeler, irsaliyeler, özlük dosyaları ve diğer fiziki kayıtlar, insan kaynakları ve muhasebe işlemlerinin yürütüldüğü yazılım programları, şirket internet sitesinin ve portallarının kullanımı, kamera kayıtlarının alınması ve yüz tanıma ve/veya parmak okuma sistemleri verilebilir. Kişisel verilerin işlendiği ve aktarıldığı tüm bu ortamlarda veri sorumlusu ve veri işleyen sıfatıyla grup üyesi şirketlerin KVKK m.12 uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin güvenli bir şekilde muhafazasını sağlamak alması gereken tedbirleri almakla yükümlü olduğu belirtilmektedir. Bu tedbirlerden çok uluslu grup şirketler için önem arz eden başlıcalarını aşağıda şekilde sıralayabiliriz:

[217] Nafiye Yücedağ, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, s.7

2.4.11.1.Siber Güvenlik

Topluluk içindeki kişisel verilerin işlendiği, aktarıldığı ve saklandığı bilgi teknoloji sistemlerinin güvenliğini sağlamak adına her bir grup üyesi şirket tarafından bu sistemlerde siber güvenliğe ilişkin gerekli teknik tedbirlerin alınması gerekmektedir. Bu kapsamda her bir grup üyesi şirket çalışanı tarafından ağ bağlantıları ve internet kullanımı boyunca bağlanılan internet ağlarından ve ziyaret edilen internet sitelerinden gelebilecek izinsiz erişim tehditlerine karşı gerekli tedbirlerin alınmış olması önem arz etmektedir. Bu amaçla her bir grup üyesi şirket tarafından güvenlik duvarlarının kurulması ve ağ geçitlerinin oluşturulması hukuka aykırı bir şekilde üçüncü kişilerden gelen erişim taleplerinin engellenmesi adına faydalı olacaktır. Bununla birlikte belirli grup üyesi şirketler tarafından kullanılan eski sürümlü veya orijinal olmayan yazılım ve servisler de ilgili grup üyesi şirket tarafından işlenen ve aktarılan kişisel veriler için güvenlik açıklarına yol açabilecektir. Bu sebeple topluluk bünyesindeki tüm grup üyesi şirketin bu yazılımların en güncel ve orijinal sürümlerini temin etmesi büyük önem arz etmektedir. Mevcut yazılımlar üzerinde gerçekleştirilebilecek yama yöntemi de bu anlamda önemli rol oynayabilecektir. Diğer taraftan grup şirketler tarafından siber saldırılara karşı mücadele edebilmek adına şirkete ait bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden sistemler kullanması ve bu sayede kötü amaçlı yazılımların engellenmesi için gerekli yazılım ve donanımların temin edilmesi gerekmektedir. Özellikle tam korumalı anti virüs ve anti spam ürünlerinin kullanımı ve bunların belirli aralıklarla güncellenmesi grup şirket tarafından işlenen ve aktarıma tabi tutulan kişisel verilerin karşılaşabileceği kötü amaçlı yazılımlardan gelebilecek ihlallere karşı önemli rol oynamaktadır. Ayrıca her bir grup üyesi şirketin şirket bilgisayarlarından internet sitelerini kullanırken bu sitelerin SSL veya diğer güvenli yollar ile korunduğundan emin olması ve yalnızca bu yönde bir güvenlik anahtarının bulunduğu internet sitelerini kullanması siber güvenliğin sağlanması adına alınabilecek önlemler arasında yer almaktadır[218].

[218] KVKK, Kişisel Veri Güvenliği Rehberi, s.4
https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

Grup şirketlerin kişisel verileri işlediği ve aktardığı elektronik ortamlara sınırlı erişimin sağlanması siber güvenlik sisteminin güçlendirilmesi adına büyük önem taşımaktadır. Bu amaçla her bir grup üyesi şirket söz konusu elektronik alanların kullanımına ilişkin çalışanları nezdinde bir yetki ve sorumluluk şeması belirlemeli ve ilgili alanlara yönelik yetkisiz erişimlerin engellenmesini sağlamalıdır. Yetki sınırlarının belirlenmesinin yanı sıra şifreleme de anılabilecek diğer bir önlemdir. Bu kapsamda topluluk bünyesinde bir şifre politikası belirlenmeli ve bu politika uyarınca girilecek şifrelerin büyük ve küçük harflerden ve tahmin edilemeyen kelime, sayı ve noktalama işaretlerinden oluşmasına dikkat edilmelidir. Ayrıca şifre girişi deneme sayısının da sınırlandırılması ve belirli aralıklarla bu şifrelerin değiştirilmesi ve güncellenmesi de faydalı olacaktır. Diğer taraftan grup şirket bünyesinde işten ayrılan çalışana ait kullanıcı hesaplarının silinmesi ve bu hesaplara girişlerin de kapatılması bilgi güvenliğinin sağlanması adına faydalı olacaktır.

2.4.11.2. Veri Güvenliğinin Takibi ve Kontrolü

Çok uluslu grup şirketler arasında kişisel veri aktarımlarının sağlandığı yazılımların, portalların ve diğer ortamların güvenliğinin sağlanması adına alınabilecek önemlerden biri de kişisel veri güvenliğinin aktarımın tarafı olan her bir grup üyesi şirket tarafından takibinin sağlanması ve kontrolünün yapılmasıdır. Bu kontrol ve takibin grup üyesi şirketin yetkilileri tarafından belirli aralıklarla gerçekleştirilmesi, aktarıma tabi tutulacak kişisel verilerin olası bir siber saldırıya maruz kalmaması, söz konusu saldırıların bir an önce tespit edilmesi ve bunlarla mücadele için geç kalınmaması adına büyük bir kolaylık sağlamaktadır. Bu takip grup üyesi şirketlerin bilgi teknolojileri sistemlerindeki açıkların tespit edilmesi, bu amaçla gerekli sızma testlerinin yaptırılması, tüm kullanıcıların log kayıtlarının tutulması ile işlem hareketlerinin düzenli olarak kaydedilmesi ve güvenlik yazılım mesajlarının veya diğer erişim kontrolü kayıtlarının kullanımı ile gerçekleştirilebilecektir. Ayrıca yapılan testler ve incelemeler sonucu ortaya çıkan güvenlik açıklarının ve zafiyet sorunlarının düzenli bir şekilde raporlanması halinde

bu raporlamalar sonucu tespit edilen olası veri ihlali risklerine göre gerekli tedbirler hızlı bir şekilde alınabilecektir[219].

2.4.11.3. Ortam Güvenliği

Grup şirketler tarafından kişisel verilerin güvenliğinin sağlanması, bu verilerin işlendiği, aktarıldığı ve saklandığı ortamların da güvenliğinin sağlanmasıyla mümkündür. Bu sebeple aktarıma tabi her bir grup üyesi şirket tarafından kişisel veri içeren cihazların kaybolması veya çalınması durumlarda karşılaşılabilecek veri ihlali ve tehditlerine karşı gerekli fiziksel ve elektronik güvenlik önleminin alınması ve bu cihazlara veya bu bulundukları yerlere yönelik yapılan müdahalelerin sürekli olarak denetim altında tutulması gerekmektedir. Bu kapsamda örneğin yangın, sel ve deprem gibi dış risklere karşı kişisel veri içeren cihazların ve alanların alarm sistemleriyle korunması ve başta iş sağlığı ve güvenliği mevzuatı olmak üzere ilgili mevzuat hükümleri uyarınca olası kazalara karşı iş yerinde gerekli yükümlülüklerin eksiksiz bir şekilde yerine getirilmesi gerekmektedir[220]. Kişisel verilerin saklandığı arşivlerin veya bu belgelerin bulunduğu depoların da iş yerleri gibi benzer tedbirlerle koruma altına alınması gerektiği unutulmamalıdır.

Bununla birlikte her bir grup üyesi şirketin çalışanlarının iş faaliyetleri ile ilgili olan her türlü bilgileri ve belgeleri şirket tarafından temin edilmesi halinde yalnızca kurumsal bilgisayar ve cihazları dahilinde tutması ve şahsi cihazları ile şahsi e-posta hesapları üzerinden yapılabilecek olası veri aktarımlarının önüne geçmesi gerekmektedir. Aksi halde şirket cihazları ile aynı güvenlik tedbirlerini taşımayan şahsi cihazlar üzerinden yapılan veri işleme ve aktarım faaliyetleri gerek aktarıma tabi kişisel verinin sahibi ilgili kişi gerekse topluluk ve ilgili grup şirket için ciddi zararlara yol açabilecektir. Diğer taraftan grup üyesi şirketin çalışanına ait şahsi cihazlar üzerinden şirketin bilgi sistem ağına erişim sağlaması da grup şirket

[219] KVKK, Kişisel Veri Güvenliği Rehberi, s.18
https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf
[220] P. Mell, "What's Special about Cloud Security?", IT Professional, s.14

nezdindeki güvenlik ihlali risklerini artmaktadır. Bu sebeple aktarımın tarafı olan grup üyesi şirketlerin şahsi cihazlardan gelen erişim taleplerine kapsam veya konu olarak sınırlama getirmesi aktarıma tabi kişisel verilerin güvenliğinin sürdürülebilir olması açısından büyük önem taşımaktadır.

Öte yandan grup şirketler arasındaki kişisel verilerin işlenmesi, saklanması ve aktarımı için kullanılmakta olan CD, DVD, USB, yedekleme cihazları ve sağlayıcı gibi cihazların da ek güvenlik önlemlerinin alındığı farklı bir alanda saklanması, bu alanların kullanılmadığı zamanlarda kapalı ve kilitli tutulması ve bu alanlara giriş çıkışların kamera kaydı ile belirli aralıklarla denetlenmesi ortam güvenliğinin sağlanması adına büyük önem taşımaktadır[221]. Bu alanlar ile ilgili grup üyesi şirket nezdinde işlenen ve saklanan kişisel işlenen verilerin bulunduğu arşiv ve depolara yönelik yapılacak yetkisiz erişimlerin önlenmesi, bu ortamlara girişlerin şifrelenmesi ve bu şifrelemede uluslararası standartlara uygun olarak hazırlanmış programların tercih edilmesi de alınabilecek diğer ortam güvenliği tedbirleri arasında yer almaktadır.

2.4.11.4.Bulut Depolama Hizmetleri

Bulut sistemi, sunucular tarafından ağ üzerinde sanal olarak oluşturulan havuzlarda kişisel veri depolama hizmeti veren bir tür bilişim hizmetidir[222]. Bulut depolama özelliği sayesinde kişisel veriler söz konusu sanal havuzlarda kaydedilmekte ve normal şartlarda kaydedildikleri cihazlarda herhangi bir arıza ortaya çıkması halinde bulut havuzlarında tutulan kişisel veriler zarar görmeden ilgili şirketçe kullanılmaya ve saklanmaya devam edilebilecektir. Veri kayıplarının önüne geçilebilmesi için bulut depolama hizmeti önemli bir veri güvenliği önlemi niteliğindedir. Bununla birlikte depolanmak üzere bulut hizmeti sağlayıcı şirkete aktarılan kişisel verilerin güvenliğinin sağlanması adına bu verilerin düzenli olarak

[221] H. Yang, M. Tate, "Where are we at with cloud computing?: A descriptive literature review", Communications of the Association for Information Systems, s. 31(2).
[222] Cengiz Paşaoğlu, Emel Cevheroğlu, Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması s.5

kontrollerinin gerçekleştirilmesi ve gerektiğinde bu verilere erişim sağlanabilmesi adına ilgili grup şirketin bulut sistemi ile uzaktan erişim kurulmasına imkân veren mekanizmaları devreye sokması ve iki nokta arasında senkronize bir sistem oluşturması faydalı olacaktır. Ayrıca bulut sisteminde depolanan verilere erişim için iki kademeli kimlik doğrulama sistemi gibi şifreleme metotlarının kullanılması da ilgili grup üyesi şirketler dışında bu verilere yapılacak yetkisiz erişimlerin önlenmesi hususunda etkili rol oynayacaktır. Öte yandan bulut hizmetinin sona ermesi halinde ilgili grup üyesi şirket tarafından buluttaki veriler ile bu verilere erişim imkânı veren şifreleme anahtarları ve bunların tüm kopyalarının bulut sisteminde yok edildiğinden emin olunmalıdır. Aksi halde bu durum bulut sisteminde tutulan kişisel verilere yetkisiz erişim sağlanmasına ve ciddi veri ihlallerine yol açabilecektir.

2.4.11.5. Sistem Kontrolleri

Çok uluslu grup şirketler tarafından kişisel verilerin aktarıldığı ve işlendiği e-posta, yazılım, program, uygulama vb. gibi elektronik ortamların sürüm ve sistemlerinde belirli aralıklarla kontrollerin yapılması, bu kontroller sonucunda ihtiyaç görülmesi halinde bu sistemlerin geliştirilmesi ve iyileştirilmesi ile güncel ve yeni sürümlerin temin edilmesi veri güvenliğinin sağlanması adına alınabilecek önlemler arasında yer almaktadır[223]. İlgili grup üyesi şirket tarafından yapılacak düzenli kontroller sayesinde söz konusu elektronik ortamlara ilişkin sistemsel sıkıntılar tespit edilip giderilebilecek ve kişisel veri işleme ve aktarım faaliyetlerinin yürütüldüğü ortamlardaki veri sızıntısına ya da kaybına sebep olabilecek olası risklerin önüne geçilebilmektedir. Sistemlerin periyodik kontrollerinin yanı sıra bu sistemlere yüklenen girdilerin de doğruluklarının kontrol edilmesi ve gerekli görülmesi üzerine güncellenmesi büyük önem taşımaktadır[224]. Örneğin ilgili grup şirketi

[223] Kişisel Verileri Koruma Kurumu, Veri Güvenliği Rehberi, ISBN : 978-975-19-6834-O, KVKK Yayınları, Ankara, 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, Erişim Tarihi: 10.12.2021.
[224] Y. İnağ, E. Ceyhan, Ş. Sağıroğlu, "Bulut Bilişimin Kurumsal Zorlukları ve Çözüm Önerileri", Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTÜ, Ankara, Haziran, 2015

tarafından yurt dışındaki diğer bir grup üyesi şirkete aktarılmak üzere kullanılan muhasebe yazılımına yüklenen çalışan verilerinin doğruluğunun ve güncelliğinin belirli aralıklarla kontrol edilmesi böyledir.

İlgili grup şirket tarafından veri işleme ve aktarım faaliyetlerinin yürütüldüğü elektronik cihazların bakım ve onarıma gönderilmesi halinde bu cihazlarda yer alan kişisel verilerin de cihazlarla birlikte üçüncü bir kişiye aktarımı gündeme gelmektedir. Bu durum üçüncü kişilerce kişisel verilerin hukuka aykırı bir şekilde işlenmesine ve aktarımına sebep olabileceğinden ilgili grup üyesi şirket tarafından kişisel verilerin saklandığı cihazların bakım ve onarım için üçüncü bir kişiye teslim edilmesinden önce bu cihazlarda yer alan kişisel verilerin farklı bir şirket cihazına aktarması ya da onarıma gidecek cihazdan silinmesi gerekmektedir. Diğer taraftan onarıma gidecek cihazların yalnızca arızalı bölümlerinin teslim edilmesi de bu kapsamda ortaya çıkabilecek veri güvenliği risklerinin en aza indirilebilmesi adına önemli bir yoldur.

ÜÇÜNCÜ BÖLÜM

ÇOK ULUSLU GRUP ŞİRKETLERDEKİ KİŞİSEL VERİ AKTARIMLARINDA BAĞLAYICI ŞİRKET KURALLARI

3.1. GENEL OLARAK

Başta çok uluslu grup şirketler olmak üzere ortak bir ekonomik amaç çerçevesinde iş birliği içerisinde hareket eden teşebbüsler ticari faaliyetleri süresince çeşitli amaçlarla bulundukları ülkelerin sınırları dışındaki topluluk üyesi şirkete ya da iş birliği içerisinde olduğu farklı bir teşebbüse kişisel veri aktarımı gerçekleştirebilmektedir[225]. Kişisel verilerin bulunduğu ülkede olduğu kadar aktarıldığı ülkede de aynı ya da benzer bir güvenlik düzeyi ile koruma altına alınabilmesi için aktarımın tarafı olan şirket ve/veya teşebbüslerin gerekli tedbirleri alması ve aktarımın taraflarından bu yönde taahhütler alınması gerekmektedir. Bağlayıcı şirket kuralları da bu kapsamda veri güvenliğinin sağlanması ve kişisel verileri sınır ötesi aktarıma tabi tutulan ilgili kişilerin temel hak ve özgürlüklerinin koruma altına alınabilmesi için aktarımın taraflarının gerekli taahhütleri ileri sürdüğü özel bir uygun güvenlik tedbiri olarak karşımıza çıkmaktadır. Gerek ulusal gerekse uluslararası kişisel veri koruma mevzuatlarında farklı şekillerde hüküm altına alınan bağlayıcı şirket kuralları Türk Hukuku'nda da doğrudan kanuni düzeyde olmasa da Kurum tarafından 10 Nisan 2020 tarihinde kendi internet sitesinde yayımladığı bir duyuru ile uygulamaya dahil edilmiştir. Bağlayıcı şirket kuralları her ne kadar Türk hukukunda mevzuat düzeyinde yazılı olarak hüküm altına alınmamış olsa da bu kuralların içerdiği taahhütler ile KVKK m.9/2 (b)'de yurt dışına veri aktarımı halinde hazırlanması ve Kurul'un onayına sunulması öngörülen taahhütnameler ile benzer olduğunu ve bu taahhütnamelerin çok uluslu grup şirketler için düzenlenmiş özel bir görünümü olduğunu söylemek yanlış olmayacaktır. Şu kadar ki kişisel verilerin aktarımı esnasında korunması ve

[225] Dülger, GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları, s.3

gizliliklerinin sağlanması gibi kişinin temel hak ve özgürlüklere dair hüküm ve sınırlamalar getiren bağlayıcı şirket kurallarının Anayasa'nın 123.maddesine uygun olarak kanun düzeyinde bir düzenleme ile hüküm altına alınması yerine Kurul'un bu alanda düzenleme yetkisine sahip görülmesinin ve yayımladığı bir duyuru ile bu alanda düzenleme yapmasının bağlayıcı şirket kurallarının hukuk tekniği açısından anayasaya uygunluğu ve kanuniliği için sorgulanabilecek bir husus olduğunu belirtmek de kanımızca yanlış olmayacaktır.

Kurum tarafından 10 Nisan 2020 tarihinde yayımlanan bağlayıcı şirket kurallarına ilişkin duyurusunda Kurum, söz konusu taahhütnamelerin ve mevcut veri aktarım tedbirlerinin çok uluslu grup şirketlerin kendi aralarındaki kişisel veri aktarımı uygulamasında yeterli faydayı ve etkiyi gösteremediğini ifade etmiş ve Tüzük hükümlerinden ve AB uygulamalarından hareketle bağlayıcı şirket kurallarını Türk Hukukuna dahil etmeye karar vermiştir. Bu kapsamda bağlayıcı şirket kuralları Türk hukukunda çok uluslu grup şirketler arasındaki kişisel veri aktarımlarında kullanılmak üzere bir hukuka uygunluk enstrümanı ve güvenlik tedbiri olarak kullanılmaya başlanmıştır. Diğer taraftan AB hukukundan farklı olarak Türk hukukunda bağlayıcı şirket kurallarının aktif bir şekilde uygulamaya konulamamış olduğunu söylemek yanlış olmayacaktır. Bunun sebebi Kurul tarafından kendisine iletilen bağlayıcı şirket kuralları başvuruları için henüz onaylandıkları yönünde herhangi bir karar vermiş olduğunun bilinmemesi ve Kurul internet sitesinde bu yönde bir kararın yayımlanmamış olmasıdır.

AB hukukundan alınan bağlayıcı şirket kuralları kurumu Tüzük kapsamında hakkında Komisyon'un yeterlilik kararı bulunmadığı AEA dışındaki ülkelere yapılacak kişisel veri aktarımlarında aktarımın tarafı olan grup şirketlerce alınabilecek güvenlik tedbirlerinden biri olarak düzenlenmiştir[226]. Öyle ki Kurum tarafından internet sitesinde yayımlanan duyuruda da bağlayıcı şirket kurallarının tıpkı yeterli korumanın bulunmadığı ülkelere yapılacak kişisel veri aktarımlarında

[226] Cemil Kaya, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İÜHFM, 2011, C. 69, S. 1-2, s. 233.

kullanılan taahhütnameler gibi bağlayıcı şirket kurallarının da bir güvenlik tedbiri olarak rol oynayacağı belirtilmektedir. Bu noktada duyuruca bağlayıcı şirket kurallarının yeterli korumanın bulunmadığı ülkelere yapılacak aktarımlarda kullanılabileceğinin belirtilmesi, bu kuralların tıpkı Tüzük kapsamında Komisyon'un yeterlilik kararının olmadığı hallerde başvurulabilecek bir güvenlik tedbiri olarak ele alınması ile uyumlu olduğunu söylemek mümkündür. Her ne kadar KVKK ve alt mevzuat hükümlerinde açıkça düzenlenmese de Türk hukukuna AB hukukundan iktibas edilen bağlayıcı şirket kuralları sınır ötesi aktarımlar kapsamında Tüzük'te ayrıntılı bir şekilde düzenleme alanı bulmaktadır. AEA sınırları haricinde üçüncü ülkeler ile uluslararası örgütlere yapılacak kişisel veri aktarımları, Tüzüğün 40-50 maddeleri arasında yer almaktadır. Tüzük m. 45 uyarınca Komisyon'un yeterlilik kararı verdiği, diğer bir deyişle yeterli koruma düzeyi sağlayan üçüncü ülkelere kişisel veri aktarımı mümkündür. Bununla birlikte Tüzük m.46 uyarınca Komisyon'un yeterlilik kararının bulunmadığı durumlarda bile belirli şartlar altında kişisel veri aktarımının yapılabileceği düzenlenmiştir[227]. Buna göre çalışmamızın ilk ve ikinci bölümlerinde de belirttiğimiz gibi veri sorumlusu veya veri işleyen tarafından gerekli güvenlik tedbirleri alınarak ve kişisel verilerin aktarımının yapılacağı ülkede aktarıma tabi tutulan kişisel veriyle ilgili veri sahibine haklarını kullanabilmesi ve etkili bir hukuki başvuru yolları oluşturulması için gerekli şartlar yerine getirilerek yeterlilik kararının bulunmadığı ülkelere dahi kişisel veri aktarımı yapılabilecektir. Tüzük m. 47 uyarınca alınabilecek güvenlik tedbirlerden biri de bağlayıcı şirket kurallarıdır. Tüzük kapsamında güvenlik tedbirleri olarak yer verilen standart veri koruma hükümleri, davranış kuralları ve sertifikalar gibi yeterli korumayı sağlayan aktarım mekanizmaları bulunsa da gerek bu mekanizmalardan en geniş şekilde düzenlenenin bağlayıcı şirket kuralları olması gerekse bu kuralların doğrudan Çalışmamızın konusu olan çok uluslu grup şirketlere özgü bir şekilde tasarlanarak topluluk şirketlerinin dinamiklerine uygun olarak kaleme alınmış olmalarından

[227] Joanna Kulezsa ''Transboundary Data Protection and International Business Compliance''', International Data Privacy Law, C. 4, S. 4, s. 298 – 306.

hareketle bu kuralların ayrıntılı bir şekilde incelenmesi çok uluslu grup şirketlerdeki kişisel veri aktarımlarının daha iyi anlaşılması adına faydalı olacaktır.

Bağlayıcı şirket kurallarına şirketler topluluğu tarafından gerçekleştirilen veri aktarımlarının yanı sıra gerçek kişi ya da tüzel kişi formunda distribütörlük, franchise, iş ortaklığı, konsorsiyum, ortak girişim gibi müşterek bir ekonomik aktivite çerçevesinde faaliyetlerini yürüten teşebbüs ve taahhüt birlikleri arasında gerçekleşen kişisel veri aktarımları için de başvurulabilmektedir. Burada esas olan ortak bir amaç için sürekli ve düzenli bir iş birliği içerisinde faaliyet göstermek ve bu kapsamda veri aktarımı gerçekleştirmektir. Şu kadar ki bağlayıcı şirket kurallarına başvuran grup üyesi şirketler ya da ortak bir amaç uğruna faaliyet gösteren teşebbüsler olsa da bağlayıcı şirketlerin ilgili veri koruma otoritesi tarafından onaylanabilmesi için bu kurallar için öngörülen geçerlilik şartların eksiksiz bir şekilde yerine getirilmesi, asgari içeriğe yer verilmesi ve usulüne uygun olarak başvuruda bulunulması gerekmektedir[228]. İlgili veri koruma otoritesi tarafından kendisine iletilen bağlayıcı şirket kuralına onay verilmeden önce, bu kuralların içeriği, gerekli tedbirlerin alınıp alınmadığı, tüm bilgilerin eksiksiz ve doğru bir şekilde açıklandığı ve etkili bir şekilde uygulamaya koyulup koyulmayacağı konusunda yeterli mekanizmaların oluşturulup oluşturulmadığı değerlendirilmektedir. Buna karşılık söz konusu başvuru süreci için gerekli şartların ve izlenecek prosedürlerin genel olarak neler olduğu açıklanmış olsa da AB hukukundan farklı olarak Türk hukukunda bu kuralların Kurul tarafından onaylanması üzerine uygulamaya konulduğuna yönelik henüz herhangi bir karar yayımlanmamıştır. Bu durum halihazırda Kurum tarafından yeterli korumanın bulunduğu ülkeler listesinin açıklanmamış olması ve bu sebeple yurt dışına veri aktarımı için yegâne yol olarak ilgili kişinin her an geri alabileceği açık rızasına dayanılarak kişisel veri aktarımlarının yapılıyor olması göz önünde bulundurulduğunda, pratikte ticaret hayatını neredeyse durma noktasına getirme riski ile karşı karşıya bırakmaktadır. Bu noktada bağlayıcı şirket kurallarının yurt

[228] İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, s. 26.

dışına kişisel veri aktarımının hukuka uygun bir şekilde yürütülmesinde oynadığı rolün ve faydalarının ele alınması gerek kişisel veri hukuku doktrini gerekse Kurul ve uygulamaları açısından bağlayıcı şirket kurallarının hayata geçirilmesinin önemini bir kez daha ortaya koyacaktır[229].

Bağlayıcı şirket kuralları, her ne kadar şirketler topluluğunun yanı sıra tüm ekonomik teşebbüsler için de hazırlanabilecekse de uygulamada çoğunlukla grup şirketlerin kişisel veri aktarımında kendi gereksinimlerini karşılamak üzere düzenleyip yürürlüğe koyduğu kurallar olarak karşımıza çıkmaktadır. Grup şirketler kendi aralarında Çalışmamızın ikinci bölümünde belirttiğimiz üzere ekonomik, ticari, hukuki, vergisel vb. pek çok amaçla kişisel veri aktarımı gerçekleştirebilmektedir. Ancak, grup şirketin merkezi AB sınırları içindeyse veya üyelerinden biri AB sınırları içinde faaliyet gösteriyorsa bu şirketin AB sınırları dışında bulunan bir üye grup şirkete kişisel veri aktarımında bulunması halinde Tüzük'e uyum sağlaması ve gerekiyorsa bağlayıcı şirket kurallarının hazırlanması gibi uygun güvenlik tedbirlerini alması gerekmektedir.

Bu kapsamda üye şirketlerce hazırlanarak uygulamaya konulacak bağlayıcı şirket kuralları, topluluktaki tüm üye şirketler için hukuken bağlayıcı ve yaptırım doğrucu bir nitelik taşımaktadır. Şu kadar ki grup üyesi şirketler arasında yapılacak aktarımın hukuka uygun hale getirilmesi için bağlayıcı şirket kuralları dışında diğer güvenlik önlemlerine başvurulması da mümkündür. Ancak böyle bir durumda grup şirketlerin her seferinde gerçekleştirecekleri her bir veri aktarım faaliyeti için söz konusu güvenlik tedbirini almaları gerekmektedir ki bu durum pratikte veri aktarımının aksamasına ve zorluklar yaşanmasına sebebiyet verebilmektedir. Bu bağlamda veri aktarımı açısından grup şirketler için en pratik yol, bağlayıcı şirket kurallarının oluşturulmasıdır[230]. Diğer taraftan yeterlilik kararının bulunduğu ülkelere yapılacak aktarımlarda grup üyesi şirketlerce bağlayıcı şirket kuralları gibi Tüzük kapsamında düzenlenen güvenlik tedbirlerin alınmasına gerek de

[229] İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, s. 38, 49.
[230] Toparlak, s.45.

bulunmamaktadır. Çalışmamızın bu bölümünde ulusal ve uluslararası mevzuat hükümlerinde ve uygulamalarında çok uluslu grup şirketler arasındaki kişisel veri aktarımlarına özgü olarak düzenlenmiş ve çok uluslu grup şirketlerdeki kişisel veri aktarımlarının hukuka uygunluklarının sağlanması anlamında büyük bir rol oynayan bağlayıcı şirket kurallarından ve bu kuralların ihtiva ettiği düzenlemelerden bahsedilecektir.

3.2. BAĞLAYICI ŞİRKET KURALLARI

3.2.1. Bağlayıcı Şirket Kuralları Kavramı

Bağlayıcı şirket kuralları[231], grup üyesi şirketlerin kendi aralarındaki kişisel veri aktarımlarında yeterli ve eşit düzeyde koruma sağlanması için hazırlanan metinlerdir. Her bir grup üyesi şirket bulunduğu ülkede kendisine aktarılan kişisel verilerin güvenliğinin ve gizliliğinin sağlanması için gerekli tedbiri alacağını ve aksi halde bu tedbirlerin gereğine uygun bir şekilde yerine getirilmemesi halinde bu durumun yarattığı aykırılıklardan sorumlu olacağı yazılı bir şekilde taahhüt etmektedir[232]. Bu kurallar, grup şirket içindeki bütün üyeler açısından hukuken bağlayıcı kabul edilmekte ve grup üyesi şirketler arasında gerçekleşen bütün kişisel veri işleme faaliyetleri için uygulama alanı bulmaktadır. Öyle ki bağlayıcı şirket kurallarının hazırlanması ve onaylanması ile uygulama konulmasından sonra grup üyesi şirketler kendi aralarında gerçekleştirdikleri her türlü veri aktarımı için bu kurallar çerçevesinde taahhüt ettiği tedbirleri yerine getirmelidir. Bağlayıcı şirket kuralları hazırlayarak grup üyesi şirketlerin, yürüttükleri veri işleme faaliyetleri ve bu faaliyetlerin dinamiklerini ve bu faaliyetlerin altında yatan ticari ve operasyonel hareketlerini göz önünde bulundurması gerekmektedir. Diğer bir deyişle ticari faaliyetleri ya da gereği hangi grup üyesi şirkete ve ülkeye daha sık veri aktarımının gerçekleşeceğinin tespiti ile bu ülke hukukuna göre alınması gereken ek tedbirler

[231] Bağlayıcı şirket kuralları, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfersoutside-eu/binding-corporate-rules_en, Erişim Tarihi: 12.12.2021.
[232]Christopher Kuner, European Data ProtectionLaw (Corporate Compliance and Regulation), Second Edition, Oxford University Press, 2007, s.218 vd.

varsa bu tedbirlerin alınması sağlanabilecektir ya da aktarımın daha çok özel nitelikli kişisel veriler üzerinden sağlanacak olması halinde bu veriler için daha sıkı güvenlik tedbirlerinin alınması gerektiği ortaya çıkacaktır. Bununla birlikte aktarımın gerçekleşeceği kanalların belirlenmesi üzerine de bu kanallara (e-posta, internet sitesi, yazılım vb.) bağlı olarak alınabilecek tedbirler de farklılaşabilecektir. Görüldüğü üzere bağlayıcı şirket kurallarının topluluğun ve aktarımın tarafı olan her bir grup üyesi şirketin kişisel veri işleme süreçleri ve ihtiyaçları dikkate alınarak ve kendi dinamiklerine göre hazırlanması büyük önem arz etmektedir.

Kişisel verinin aktarıldığı ülke veya bölge ile uygun ve eşit seviyede veri koruma vaat eden bu kurallar, kişisel verilerin grup şirket içinde serbestçe dolaşımını temin etmektedir[233]. Ancak bu serbestliğin başta grup üyesi şirketlerin bulunduğu ülkede geçerli olan mevzuat hükümleri olmak üzere grup üyesi şirketlerce taraf olunan bağlayıcı şirket kuralları ile çizilen sınırlar içerisinde anlaşılması uygun olacaktır. Diğer taraftan bu kuralların bir kez ilgili veri koruma otoritesinin onayına sunulması ve onay alınması ile birlikte bu kurallar ve ekleriyle başvuruda belirtilen veri işleme amaçları için tekrar bir onay mekanizmasına başvurulmasına gerek bulunmamaktadır. Bu yönüyle bağlayıcı şirket kuralları aynı veri işleme ve aktarım faaliyetleri için tekrar ilgili kişinin açık rızasına dayanılması ya da söz konusu yetkili otoritenin onayının alınması şeklinde uzun prosedürlerin izlenmesi gerekliliğini ortadan kaldırdığını söylemek mümkündür. Kişisel verilerin aktarımının yanı sıra topluluk içerisinde işlenmesinin de bu kurallarla belirli şartlara tabi tutulduğu ve düzenleme altına alındığı görülmektedir. Öyle ki bağlayıcı şirket kuralları, bir şirketler topluluğunun sınır ötesi kişisel veri aktarımları da dâhil olmak üzere kişisel verilerin işlenmesi için topluluktaki tüm grup üyesi şirketler için geçerli olacak ilkeleri ve kuralları belirleyen davranış kuralları olduğunu söylemek yanlış olmayacaktır[234].

[233]Daniela Masoch, "Why Should Companies Invest in Binding Corporate Rules?', 2019, https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, Erişim Tarihi: 12.12.2021.
[234] İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler, 2020, s. 79, Bkz:

Bu kurallar ile ortaya konulan veri işleme ve aktarıma dair ilke ve şartlar, topluluk içindeki veri işleme ve aktarım faaliyetlerine yönelik kendi aralarında ve üçüncü kişilere yönelik bir şeffaflık ve hesap verilebilirlik mekanizması olarak da rol oynamaktadır[235] ve adeta topluluğun kişisel veri işleme faaliyetlerine ilişkin anayasası haline gelmektedir. Kişisel veri aktarım faaliyetlerinde bu kurallara tabi olan grup üyesi şirket, topluluk içinde bulunan tüm şirket ve yapıları ifade etmekte ve bu üyeler haricinde başka şirket ve yapılara yönelik gerçekleşen aktarımlar esasında bağlayıcı şirket kurallarının konusunu oluşturmamaktadır. Bu bağlamda bağlayıcı şirket kuralları, yalnızca topluluk içerisinde serbest veri akışına imkân vermekte[236] ve topluluk dışına yapılacak veri aktarımlarına ilişkin olarak her bir grup şirketin bağlayıcı şirket kurallar dışında kanuni ve sözleşmesel olarak gerekli diğer şartları yerine getirme yükümlülüğü devam etmektedir.

Bağlayıcı şirket kurallarının konu ve kişi bakımından uygulanma kapsamları ve sınırları bulunmaktadır. Türk hukuku uyarınca bağlayıcı şirket kuralları, Türkiye sınırları dışında bulunan ve Kurum tarafından yeterli korumanın bulunduğu ülkeler listesinde yer almayan yabancı ülkelere yapılacak aktarımlarda bir güvenlik tedbiri olarak kullanılmaktadır. Öyle ki yurt dışına veri aktarım aracı olarak hazırlanan bu kurallar Türkiye'de kurulu veri sorumlusu sıfatını haiz grup üyesi şirket ya da teşebbüs tarafından Türkiye'den yurt dışına yönelik gerçekleşecek kişisel veriler için uygulama alanı bulmaktadır. Dolayısıyla Türk hukukuna göre bağlayıcı şirket kurallarının konusunu Türkiye'de bulunan ve işlenen kişisel veriler oluşturmaktadır ve bu kurallar ile söz konusu kişisel verilerin güvenliğine ilişkin taahhütlerde bulunulmaktadır. Bununla birlikte Tüzük uyarınca bu kurallar AB ve AEA sınırları dışında bulunan ve Komisyon'un hakkında yeterlilik kararı vermiş olmadığı üçüncü ülkelere yapılacak aktarımlarda bir güvenlik tedbiri olarak kullanılmaktadır[237].

https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf, Erişim Tarihi: 30.03.2022.

[235]Bowman, Gufflet, s. 257-261.

[236]Moerel, s.100.

[237] Claudia Quelle, ''Enhancing Compliance Under The GDPR: The Risky Upshot Of The Accountability And Risk Based Approach' European Journal of Risk Regulation, C. 9, S. 3, s. 502-526.

Ancak Türk hukukundan farklı olarak Tüzük uyarınca veri sorumlusu ya da veri işleyen olduğuna bakılmaksızın Tüzük'e tabi grup üyesi şirketler ya da teşebbüsler bağlayıcı şirket kuralları hazırlayarak yurt dışına veri aktarımında bulunabilmektedir.

Bu durumda Tüzük uyarınca hazırlanacak bağlayıcı şirket kurallarının konusunu AB ve AEA sınırları dahilinde işlenen ve yurt dışına aktarılacak olan kişisel veriler oluşturmakta ve bu kurallar ile söz konusu verilerin korunması adına taahhütlerde bulunulmaktadır. Belirli durumlarda topluluk üyesi şirketler gerek kendi kararları gerekse ilgili veri otoritesinin talimatı uyarınca aktarıma tabi tutacakları kişisel veri kategorilerinde belirli sınırlamalara gidebilir. Örneğin topluluk içerisinde yapılacak kişisel veri aktarımlarına yalnızca tedarikçi ve müşteri verileri dahil edilebilir ve bağlayıcı şirket kuralları bu veri kategorileri için uygulanacak şekilde hazırlanabilir. Böyle bir durumda grup üyesi şirketlerin çalışanlarına ait kişisel veriler için bağlayıcı şirket kuralları uygulama alanı bulmayacaktır. Ancak topluluk içerisinde çalışan verilerinin de aktarımı gündeme gelecekse aktarımın tarafı olacak şirketlerin söz konusu bağlayıcı şirket kurallarının kapsamına çalışan verilerini de dahil etmesi ya da bağlayıcı şirket kuralları dışında mevzuatta öngörülen diğer veri aktarım tedbirlerinden birini alması gerekmektedir.

Bununla birlikte bağlayıcı şirket kuralları yalnızca şirketler topluluğuna ya da ortak bir ekonomik amaç çerçevesinde birlikte hareket eden teşebbüsler arasında yapılacak kişisel veri aktarımlarında uygulama alanı bulmaktadır[238]. Bağlayıcı şirket kurallarının kişi bakımından uygulama alanı, topluluk dahilinde bulunan grup üyesi şirketler ya da bunların veri sorumlusu veya veri işleyen olarak faaliyet gösteren şubeleri, temsilcilikleri ya da bu kapsamda hareket eden yapıları ile ya da ortak bir ekonomik amaç uğruna düzenli bir veri alışverişinde olan adi ortaklıklar, ortak girişimler, konsorsiyum üyeleri, distribütörlük ağı gibi oluşumlar ile sınırlıdır. Buna karşılık alelade bir hizmet sözleşmesi ya da ilişkisi içinde sınırlı ve geçici

[238] Toparlak, s.45

olarak aralarında kişisel veri aktarımında bulunan taraflar, bu kuralların uygulama kapsamı ve amacıyla doğrudan örtüşmemektedir.

Öte yandan bağlayıcı şirket kurallarının kişi bakımından uygulama alanı bulduğu şirket toplulukları ve teşebbüsler Türk hukuku uyarınca Türkiye'de kurulmuş ve faaliyet gösteren ve Tüzük uyarınca ise yine yalnızca AB sınırları içerisindeki üye ülkelerden birinde kurulmuş ve faaliyet gösteren yapılardan biri olmalıdır. Şu kadar ki topluluk içerisinde bulunmasına rağmen hazırlanan bağlayıcı şirket kurallarına taraf olmayan bir grup üyesi şirkete yapılacak aktarımlarda yine mevzuatta öngörülen diğer şartların yerine getirilmesi gerekecektir. Bağlayıcı şirket kurallarının yeterli sayılmayacağı ve mevzuattaki veri aktarımına ilişkin diğer tedbirlerin de alınması gerekmesi durumu bağlayıcı şirket kurallarının uygulama alanı dışında bulunan ve gerekli olması halinde veri aktarımının gerçekleşeceği üçüncü kişilere yönelik yapılacak veri aktarımları için de geçerlidir.

Çok uluslu grup şirketlere özgü olarak hazırlanıp ilgili otoritenin onayına sunulan bağlayıcı şirket kurallarının topluluk genelinde hayata geçirilmesi belli bir süreç istemektedir. Bu süreç sonunda topluluk bünyesinde uygulamaya konulan bağlayıcı şirket kurallarının zaman içerisinde topluluğun ve/veya her bir grup üyesi şirketin ortaya çıkan yeni gereksinimleri çerçevesinde uyarlanması veya değişikliğe tabi tutulması ihtiyacı gündeme gelebilir. Bu sebeple bu kuralların topluluğun ileride ortaya çıkabilecek ihtiyaçları göz önünde bulundurularak düzenlenmesi ve kısa vadede yeniden düzenleme gerektirecek hususlar üzerinde kapsamlı bir inceleme ve karar süreci geçirilmesi faydalı olacaktır. Öyle ki bu kuralların yeniden düzenlenmesi ve topluluğun oluşturulan yeni kurallara uyum sağlaması uzun bir süre gerektirdiğinden bağlayıcı şirket kurallarının hazırlanırken uzun vadede topluluğa ve grup üyesi şirketlerin kişisel veri aktarım faaliyetlerine yönelik ihtiyaçları karşılayacak şekilde düzenlemeye gidilmesi önem taşımaktadır. Aksi takdirde topluluk ve ilgili grup üyesi şirketler için maliyetli ve uzun süre alan bir değişim süreci ortaya çıkabilecektir ki bu sürecin topluluğu ve gerçekleşmesi planlanan kişisel veri aktarım faaliyetlerini olumsuz yönde etkileme riski yüksek

görülmektedir[239]. Unutmadan belirmek isteriz ki Çalışmamızda Tüzük uyarınca hazırlanacak ve uygulamaya konulacak bağlayıcı şirket kurallarına da yer verilmiştir. Bunun sebebi Türk hukuku uyarınca düzenlenecek bağlayıcı şirket kurallarında da büyük oranda Tüzük ile belirlenen söz konusu bağlayıcı şirket kuralları taahhütlerine yer verilmesinin aranmasıdır.

3.2.2. Bağlayıcı Şirket Kurallarının Tarihsel Gelişimi

Bağlayıcı şirket kurallarıyla birlikte farklı ulusal mevzuatlara tabi olan grup üyesi şirketlerin kendi aralarındaki kişisel veri aktarımları şeffaf ve tek bir düzene tabi olacak şekilde yürütülebilmektedir. Bu sebeple uluslararası ticaretin yoğun veri aktarımı gerçekleştiren aktörlerinden topluluk şirketlerinin kendi aralarındaki kişisel veri aktarımlarını hukuki bir düzene oturtma amacı kanun koyucular için kişisel veri mevzuatının oluşturulmasından beri büyük önem taşımıştır. Teknolojinin hızlı bir şekilde gelişmesi ile birlikte fiziki ortamların ve sabit hatların da ötesinde internet ve özel ağlarla da kişisel veriler hızlı ve kolay bir şekilde aktarılabilir hale gelmiştir[240]. Öyle ki kişisel verilerin bir havuzda tutulduğu bulut sistemlerinin kullanılmaya başlamasıyla söz konusu sitemlerin veri tabanlarının farklı ülkelere yayılmasıyla birlikte kişisel veri aktarımlarının sınırlarını belirlemek oldukça zor bir hal almıştır. Özellikle sürekli bir şekilde ticari faaliyetlerini yürüten ve devamlı bir etkileşim içerisinde olan grup şirketler de kendi aralarında düzenli ve daimi veri akışını sağlayabilmek adına kendi ihtiyaçlarını karşılayabilecek uzun vadeli ve sürdürülebilir farklı kanallar ve ağlar geliştirmiştir. Kişisel veri aktarımlarının bu denli artışı ve yoğunlaşması üzerine ülkeler için bu alanın belirli yasal düzenlemelere ve sıkı şartlara tabi kılmak ilgili kişilerin temel hak ve özgürlüklerinin korunması için bir zorunluluk haline gelmiştir.

[239]Kulezsa, s. 298 – 306; Moerel, s.108.
[240] Moerel Lokke, Binding Corporate Rules: Corporate Self Regulation of Global Data Transfers, Oxford University Press, Birleşik Krallık 2012.

Kişisel veri aktarımlarının belirli bir hukuki düzene oturtulması çabası ile birlikte bu alanda öncü çalışmalara ilk kez Direktif döneminde başlanmıştır. Direktif'te çok uluslu grup şirketlerin kendi aralarındaki kişisel veri aktarımlarının yarattığı bu sorunlara çözüm bulmak amacıyla belirli düzenlemelere yer verilmiştir. Ancak bağlayıcı şirket kuralları adı altında ayrıntılı ve toplu düzenlemelerin ilk kez Tüzük ile getirildiği görülmektedir[241]. Buna rağmen Direktif'in söz konusu düzenlemeleri doktrin ve uygulamada da bağlayıcı şirket kuralları olarak yorumlanmakta ve uygulama alanı bulmaktaydı. Bu düzenlemelerin Direktif'in 29. maddesi uyarınca kurulan ve bağımsız bir danışma kurulu olarak kişisel verilerin korunması ve gizliliği üzerine çalışmalarını yürüten 29. Madde Çalışma Grubu'nun çalışmaları sayesinde geliştirilmesi ile birlikte Tüzük'te bağlayıcı şirket kuralları adıyla bu alandaki ayrıntılı düzenlemelere yer verilebilmiştir. 29. Madde Çalışma Grubu'nun yayımladığı katalog ve kılavuzların bu alandaki düzenlemelerin şekillenmesinde büyük bir etkisi bulunmaktadır. Bu kapsamda 2013 ve 2015 yıllarında WP 204 içerisinde yayınlanan "Veri İşleyen Bağlayıcı Şirket Kuralları'na Dair Açıklayıcı Evraklar", 2014 yılında WP 212 içerisinde yayınlanan 02/2014 sayılı Görüş, 2012 yılında WP 195 içerisinde yayınlanan "Veri İşleyen Bağlayıcı Şirket Kuralları'nda Bulunması Gereken İlkeler Ve Nitelikler Tablosunu İçerir 02/2012 sayılı Bildiri Çalışması" ve 2012 yılında WP 195a içerisinde yayınlanan "Veri İşleme Faaliyetleri İçin Yapılacak Veri Aktarımlarına Dair Hazırlanan Bağlayıcı Şirket Kuralları İçin Standart Başvuru Formu" konulu ve 01/2012 sayılı Tavsiye 29. Madde Çalışma Grubu tarafından çok uluslu grup şirketler arasındaki kişisel veri aktarımlarının düzenlenmesi ve mevzuat kapsamına dahil edilmesi adına önemli rol oynamış çalışmalardan bazılarıdır.

Bununla birlikte grup şirketleri arasındaki kişisel veri aktarımlarına ilişkin olarak Daimler Crysler[242] şirketinin taahhütleri, ilk bağlayıcı şirket kuralları olarak

[241] Direktif döneminde hazırlanıp onaylanan bağlayıcı şirket kuralları listesi için bkz. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841 Erişim Tarihi: 14.07.2021.

[242]2017 yılında Daimler ve Chrysler şirketleri bölünmüştür ve şirketin ticaret unvanı Daimler AG olarak değiştirilmiştir. https://tr.wikipedia.org/wiki/Daimler_AG

onaylanan kurallar olma özelliğini taşımaktadır. Öyle ki ilk elden devletin organları yerine ilk kez özel sektör aktörleri arasında bu yönde uyum çalışmasının başlatılması bağlayıcı şirket kurallarının oluşum süreci için büyük önem arz etmektedir. Özel sektör aktörlerinden şirketlerin kendi aralarındaki aktarım dinamiklerini gözeterek oluşturduğu bu taahhütler kamu ve özel sektörün iş birliği ile ortaya çıkardığı önemli bir hukuki kurum olarak karşımıza çıkmaktadır. Bu noktada devlet kurumları çıkardığı veri koruma hukuku kuralları ile her hususu tek seferde ve ayrıntılı olarak düzenleyemese de şirketler, kendi girişimleriyle aralarındaki kişisel veri aktarımları için gerekli olan önlemlerin alınmasını sağlayacak nitelikteki taahhütleriyle adeta bir hukuka uygunluk mekanizması oluşmasına fayda sağlamıştır. Bağlayıcı şirket kuralları ile artık teşebbüsler kendi tabiatlarına uygun kurallar ile kişisel veri aktarımlarını düzenlemekte, aktarılan kişisel veriler için gerekli önlemleri almakta ve kendilerini denetlemektedir, ancak aynı zamanda devletin belirli aralıklarla kendilerinden aktarımlar özelinde hesap sorma, bilgi talep etme, denetim ve herhangi bir aykırılık halinde bunun karşısında yaptırım uygulama hakkının olduğunun da bilincinde hareket etmektedir. Bu anlamda hesap verilebilirlik bağlayıcı şirket kurallarının en temel ilkesini teşkil etmektedir.

Her ne kadar Tüzük'ün kabul edilmesiyle birlikte 29. Madde Çalışma Grubu ortadan kaldırılmış ve yerine Avrupa Birliği Veri Koruma Kurulu ("Birlik Kurulu") getirilmiş olsa da Tüzük döneminde de Birlik Kurulu'nun yayınladığı dokümanlarla bu alandaki çalışmalara devam edilmiştir. Öyle ki Direktif döneminde onaylanan bağlayıcı şirket kuralları Tüzük döneminde de hukuka uygun olarak geçerliliğini korumaktadır[243] ve Birlik Kurulu da bağlayıcı şirket kurallarına ilişkin değerlendirmelerinde 29. Madde Çalışma Grubu'nun yayınladığı dokümanlardan yararlanmaya devam etmektedir. Bu dokümanlara ek olarak Tüzük döneminde Birlik Kurulu tarafından 2018 yılında sırasıyla WP 263 rev.01 içerisinde yayınlanan

[243]Avrupa Konseyi BCR Bilgi Metni https://ec.europa.eu/info/law/law-topic/data-protection/internationaldimension-data-protection/binding-corporate-rules-bcr_en Erişim Tarihi: 19.03.2020.

"Tüzük Altında Veri Sorumluları Ve İşleyenleri Bağlayıcı Şirket Kuralları'nın Onayı İçin İşbirliği Süreci" konulu Bildiri Çalışması, WP 264 içerisinde yayınlanan "Veri Sorumlusu Bağlayıcı Şirket Kuralları'nın Onay Başvuru Formuna Dair Tavsiyeler", WP 265 içerisinde yayınlanan "Veri İşleyen Bağlayıcı Şirket Kuralları'nın Onay Başvuru Formuna Dair Tavsiyeler" ve WP 256 rev.01 içerisinde yayınlanan "Bağlayıcı Şirket Kuralları'nda Yer Alacak İlke Ve Nitelikleri İçerir Tablo" konulu Bildiri Çalışması bu alana ışık tutan ve rehber niteliğindeki önemli dokümanlar arasında yer almaktadır.

3.2.3. Bağlayıcı Şirket Kurallarının Faydaları

Çok uluslu grup şirketler arasındaki kişisel veri aktarımında uygun güvenlik tedbirlerinden biri kullanılan bağlayıcı şirket kuralları, farklı ülkelerde bulunan ve birbirlerinden farklı mevzuatlara tabi olarak faaliyet gösteren grup üyesi şirketlerinin kişisel veri aktarımlarını tek bir çatı altında toplamakta ve bu aktarımların tabi olacağı yeni bir hukuk düzeni yaratmaktadır. Aktarımın tarafı olan grup üyesi şirketlerin her birinin bu kurallarla bağlı olması sayesinde bir ülkeden diğer bir ülkeye aktarılan kişisel veriler, aktarıldığı ülkede de aynı koruma düzeyinden faydalanır. Bu durum ilgili kişilerin kişisel verilerine bağlı temel hak ve özgürlüklerinin korunması açısından büyük bir önem taşır. Bununla birlikte onaylanmış bağlayıcı şirket kuralları üzerinden yapılan kişisel veri aktarımları, grup üyesi şirketlerin kendi mevzuatlarından doğan ve yurt dışına veri aktarımı için gerekli görülen ilgili kişinin açık rızasının alınması gibi diğer şartların yerine getirilmesi yükünden de kurtarır. Bir kere usulüne uygun bir şekilde hazırlanmış bağlayıcı şirket kurallarının ilgili veri koruma otoritesine onaylatılması ile birlikte artık aynı veri aktarım faaliyetleri için yeniden ilgili otoriteden onay alınmasına gerek bulunmamaktadır[244]. Bununla birlikte ilgili otoritenin takdirine bağlı olarak uygunluğu konusunda onay verilecek olması yönüyle eleştirilebilecek olsa da bu kuralların mutlak ve tek bir şekli olmamasından hareketle topluluğun yapısına ve

[244]Moerel, s.100.

dinamiklerine göre hazırlanabilmektedirler. Bu bakımdan ilgili şirketler topluluğunun kişisel veri aktarımlarına ilişkin olarak o topluluğa özgür bir biçimde hazırlanmış birer kurumsal politika niteliği taşırlar. Bağlayıcı şirket kurallarının hazırlanması ve uygulamaya konulması ile topluluk içerisindeki her bir grup üyesi şirketin ve çalışanlarının veri gizliliği ve veri koruması konularında farkındalığı artmakta[245] ve olası veri ihlallerine karşı veri her bir şirket çok daha bilinçli ve tedbirli hareket etmesine yardımcı olmaktadır. Ayrıca bu kurallar, grup üyesi şirketlerin aktarımlardan doğabilecek muhtemel hukuki ihlalleri önlemesinde büyük bir rol oynayacağından veri sorumlusu grup üyesi şirkete ilişkin idari inceleme ve yaptırım ihtimallerini de azaltacaktır[246].

İçerdiği veri güvenliği taahhütleri ile birlikte bağlayıcı şirket kuralları, grup üyesi her bir şirket için kişisel veri koruma mevzuatına uyum sürecini güçlendirir ve aktarımın taraflarının mevzuata uygun bir şekilde veri işleme ve aktarım faaliyetlerini yürütmesini sağlar. Bu sayede aktarıma tabi tutulan kişisel verilerin sahibi olan ilgili kişiler için de kişisel verilerin işlenmesinden ve aktarımından doğan yasal haklarını etkili bir şekilde kullanmaları için gerekli mekanizmaların kurulmasını sağlar. Bununla birlikte söz konusu metinlerin topluluğun internet sitesi gibi ilgili kişilerin erişebileceği alanlarda paylaşılması ile birlikte bu kurallar ilgili kişileri aktarıma dair bilgilendirmekte ve bir aydınlatma metni ya da gizlilik politikası rolü oynamaktadır[247]. Öyle ki çok uluslu grup şirketlerin kendine has bir biçimde oluşturduğu bu kurallar, topluluğun tümünde şeffaf bir veri işleme uyum sürecinin esasını oluşturmakta[248] ve ilgili grup üyesi şirketler için veri işleme ve aktarım faaliyetlerinde hesap verilebilir bir yapıyı beraberinde getirmektedir[249]. Bu kurallar, hesap verilebilirliğin ortaya konması bakımından herhangi bir ihlal ya da uyuşmazlık halinde topluluğun veri işleme prensiplerinin ortaya konması

[245]Masoch, "Why Should Companies Invest in Binding Corporate Rules?', 2019, https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, Erişim Tarihi: 30.12.2021.
[246] Toparlak, s.46.
[247] Toparlak, s.45.
[248]Bowman, Gufflet,s. 257-261.
[249]Moerel, s.175.

noktasında geçerli bir ispat vasıtası olarak da kullanılabilecektir[250]. Diğer taraftan ayrıntılı hazırlanan ve etkili bir şekilde uygulanan bağlayıcı şirket kuralları ile veri işleme politikalarında hesap verilebilir bir yapı kazanan şirketler hizmet kalitesi bakımından da rakiplerine göre piyasada fark yaratabilmekte ve gerek ihale süreçlerinde gerekse serbest pazarlarda müşterileri ve kamu idareleri için daha iyi bir seçenek olarak görünebilmektedir[251].

Bağlayıcı şirket kurallarının yurt dışına kişisel veri aktarımı halinde Tüzük uyarınca başvurulabilecek standart sözleşme maddelerine ya da KVKK uyarınca veri sorumluları tarafından hazırlanabilecek taahhütnamelere göre de belirli avantajları bulunmaktadır. Komisyon tarafından Tüzük çalışmaları esnasında standart sözleşme maddeleri güncellenirken bu maddelerin grup şirketlerin kendine özgü ve yerleşik veri aktarımı sistemleri bulunmasından hareketle çok uluslu grup şirketler için yeterli olmadığı belirtilmiş ve bu maddelerin grup şirketlerin veri aktarım gereksinimlerine cevap vermediği ifade edilmiştir. Benzer bir açıklama Kurum tarafından kendi internet sitesinde yayımlanan bağlayıcı şirketlere ilişkin 10 Nisan 2020 tarihli duyuruda da yapılmıştır. Öyle ki standart sözleşme maddelerinin ve veri aktarım taahhütnamelerinin tek bir veri işleme amacı için hazırlanmasının gerekmesi ve farklı amaçlarla yürütülecek veri işleme ve aktarım faaliyetleri için aynı metinlerin tekrardan hazırlanarak ilgili otoritenin onayına sunulması gerekliliği sürekli etkileşim içinde olan topluluk şirketleri için taahhütnamelerin ve standart sözleşme maddelerinin kullanımını zorlaştırmaktadır. Bu hallerde çok uluslu grup şirketlerin kendi kurallarına uygun olarak düzenleyebildikleri ve tek bir metin üzerinden bir kere alınacak onay ile hemen her türlü veri aktarımı sürecini taahhüt edebildikleri bağlayıcı şirket kuralları daha avantajlı görünmedir[252].

[250] Toparlak, s.46.
[251]Masoch, "Why Should Companies Invest in Binding Corporate Rules?', 2019, https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, Erişim Tarihi: 30.12.2021.
[252]Bowman, Gufflet, s. 257-261; Moerel, s.26.

3.2.4. AB Hukuku'nda Bağlayıcı Şirket Kuralları

AB hukukunda bağlayıcı şirket kuralları Tüzük'te düzenleme altına alınmıştır. Tüzük öncesi dönemde yürürlükte olan Direktif'te de bağlayıcı şirket kuralları ismiyle belirtilmemiş olsa da çok uluslu grup şirketler arasındaki kişisel veri aktarımını düzenleyen mekanizmalardan biri olarak bu yönde kuralların hazırlanabileceğine dair hükümler bulunmaktaydı. Ancak Tüzük'ün kabul edilmesiyle birlikte bağlayıcı şirket kurallarına ilişkin ayrıntılı hükümler getirilmiş ve bu alanda sistematik düzenlemelere yer verilmiştir. Bağlayıcı şirket kuralları ya da diğer bir deyişle bağlayıcı kurumsal kurallar Tüzük'ün "Tanımlar" başlıklı 4.maddesinde "ortak bir ekonomik faaliyetle iştigal eden bir teşebbüsler grubu veya bir işletmeler grubu içerisinde bir veya daha fazla sayıda üçüncü ülkedeki bir kontrolör veya işleyiciye kişisel veri aktarımları veya aktarım dizisiyle ilgili olarak Birliğin üye devletlerinden birinin topraklarında kurulmuş olan bir kontrolör veya işleyici tarafından uyulan kişisel veri koruma politikaları" olarak tanımlanmıştır. Bu tanıma göre Tüzük uyarınca bağlayıcı şirket kuralları, AB sınırları içerisinde kurulu olan bir veri sorumlusu ya veri işleyen şirket ya da işletme veya teşebbüs tarafından AB sınırları dışında bulunan diğer bir üye şirket, işletme ya da teşebbüse kişisel veri aktarımlarında taraflarca hazırlanabilecek veri koruma politikaları olarak görülmektedir.

Bununla birlikte bu tanım ile dikkat çekilmesi gereken diğer bir nokta Tüzük uyarınca bağlayıcı şirket kurallarının sınır ötesi kişisel veri aktarımını gerçekleştirecek veri sorumluları gibi veri işleyenler tarafından da hazırlanabilecek olmasıdır. Her ne kadar 29. Madde Çalışma Grubu tarafından hazırlanan ilk bağlayıcı şirket kuralları taslağı veri sorumlularına yönelik olsa da zamanla müşteri ve tedarikçi faaliyetleriyle gerçekleşebilen grup içi veri aktarımına yönelik olarak veri işleyen bağlayıcı şirket kurallarının da hazırlanıp uygulanabileceği kabul edilmiştir ve buna uygun taslaklar hazırlanmıştır. Diğer taraftan Tüzük'ün 110. gerekçe maddesinde içerdiği veri koruma ilkeleri ve yöntemleri göz önünde

bulundurulduğunda AB içerisindeki grup üyesi şirketler arasında da bağlayıcı şirket kuralları uygulanmak üzere hazırlanabileceği düzenleme altına alınmıştır.
Bağlayıcı şirket kurallarına ve bu kurallar uyarınca tarafların tabi olacağı taahhütlere Tüzük m.47'de yer verilmiştir. Bu taahhütlerin başında bağlayıcı şirket kuralları ile tarafların veri işleme ve aktarım faaliyetlerinde şeffaflık ilkesine riayet etmesi yer almaktadır. Bu nedenle bağlayıcı şirket kurallarını düzenlenirken ve uygulamaya konulmasıyla birlikte bu kurallara tabi her bir grup üyesi şirketin grup içi aktarımlarında şeffaflığı sağlaması beklenmektedir. Tüzük m.47'de de bu aktarım süreçlerinde şeffaflığın sağlanması adına grup üyesi şirketlerce verilmesi gereken taahhütler on dört fıkra halinde hüküm altına alınmıştır[253]. Bu kuralların hazırlanması ve uygulanması ile birlikte temin edilecek şeffaf veri aktarım süreçleri ayrıca her bir grup üyesi şirketin Tüzük uyarınca öngörülen veri işleme düzenlemelerine de uyum sağlamasına ve AB hukuku düzenlemeleri ile tutarlı veri aktarım faaliyetlerinde bulunmalarına yardımcı olurken aynı zamanda bu süreçlerin ilgili kişilerce ve yetkili otoritelerce de takip edilebilir olmasını sağlamaktadır. Öyle ki bağlayıcı şirket kurallarının hazırlanmasının ardından onay süreçlerinin yürütülmesi, her bir grup üyesi şirketin yerleşik olduğu üye devlete göre farklı veri koruma otoritesi tarafından yerine getirileceğinden tutarlılık, kolay idare edilme ve takip edilebilirlik hususları bağlayıcı şirket kuralları uygulamasında büyük önemli taşımaktadır.

Bağlayıcı şirket kurallarının şeffaflığını sağlamak için içermesi gereken bu on dört fıkralık taahhütler serisinin yanı sıra Tüzük'te veri sorumlusu ve veri işleyen için yerine getirilmesi gerektiği öngörülen diğer yükümlülükler ile genel veri işleme ilkelerini de kapsaması gerektiği unutulmamalıdır. Örneğin Tüzük m.28 uyarınca AB içerisinde bulunan bir veri sorumlusu şirket namına üçüncü ülkede veri işleyen olarak bir şirket atanacaksa veri işleyenler tarafından Tüzük m. 28 uyarınca öngörülen yükümlülüklerin de bu kapsamda bağlayıcı şirket kurallarında

[253] Md. 29 Çalışma Grubu görüşleri için arşiv, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec21, Erişim Tarihi: 15.12.2021.

belirtilmesi gerekmektedir[254]. Söz konusu genel yükümlülükler dışında Tüzük m.47/2 uyarınca bağlayıcı şirket kurallarında bulunması gereken içerik ve taahhütler aşağıda sıralanmıştır.

3.2.4.1. Bağlayıcı Şirket Kurallarına Tabi Şirketlerin Yapısı ve Bilgileri

Tüzük m. 47/2 (a) uyarınca bağlayıcı şirket kuralları hazırlanırken bu kurallara tabi olacak şirketlerin ticaret unvanlarının ve adres, ticaret sicil numarası vb. gibi temel sicil bilgilerinin açık ve anlaşılır bir şekilde bu kuralların giriş bölümünde her bir grup üyesi şirket için belirtilmesi gerekmektedir. Bu bilgiler grup üyesi şirketlerin kurulu oldukları ülkelerdeki resmi ticaret sicil kayıtlarıyla birebir örtüşmeli ve ilgili şirketi ayırt edici gerekli hususları içermelidir. Bu bilgilerin açık bir şekilde yazılması ile birlikte bu kurallara tabi olacak her bir grup üyesi, kişisel verileri aktarılacak ilgili kişilerce ve bu kuralların onaylanması ve uygulanması esnasında gerekli denetimleri yapma yetkisini haiz yetkili veri koruma otoriteleri tarafından kolaylıkla takip edilebilir hale gelmekte ve şeffaflığın sağlanması adına önemli bir adım atılmış olmaktadır. Ayrıca bu şirketlerin ticaret sicil bilgilerinin bağlayıcı şirket kurallarından yazılması ile birlikte bu kuralların kişi bakımından uygulama alanları açık bir şekilde ortaya konulmakta ve bu kurallara tabi olacak şirketlerin kimlikleri de belirlenmiş olmaktadır.

Bu kapsamda mümkünse şirketin pay sahipliği yapısının, yönetim organında bulunan kişilerin ve imza yetkililerinin de belirtilmesi önem arz etmektedir. Diğer taraftan Tüzük 47/2 (a) uyarınca şirket yapılarının yanı sıra yetkili veri koruma otoritesi tarafından herhangi bir denetim yapılması ya da bilgi veya belge talebi veyahut ilgili kişilerce ya da üçüncü kurum veya kuruluşlarca bağlayıcı şirket kurallarının uygulanması ve/veya kişisel veri aktarımları ile ilgili olarak grup üyesi şirketlerden herhangi biri ile temasa geçilmesi gerektiği durumlarda başvurulacak iletişim kanallarına ve bilgilerine de yer verilmesi gerekmektedir. Bu irtibat

[254]Working Paper, Md. 29 Çalışma Grubu, 256, 257.

bilgilerine topluluğun üçüncü ülkelerde yer alan grup üyesi şirketlerine ait bilgiler de dahildir. Şirketlerin yapısına ve iletişim bilgilerine yer verilmesi ile birlikte ilgili kişilerce yapılacak başvuruların ve yetkili veri koruma otoritelerince sorumlu tutulacak tarafların hızlı ve etkili bir şekilde tespit edilmesini kolaylaştırmakta ve bu durum olası uyuşmazlıkların çözümü için de büyük fayda sağlamaktadır.

3.2.4.2. Kişisel Veri Aktarımları ve Aktarım Dizisi

Tüzük'ün yürürlüğe girmesinden sonra öngörülen bağlayıcı şirket kuralları, normal şartlarda her bir kişisel veri aktarımı için gerekli olan bağımsız onay sürecine duyulan ihtiyacı ortadan kaldırmış ve bu kurallar için yetkili veri koruma otoritesi tarafından verilecek tek bir onayın yeterli olduğunu öngörmüştür. Bu noktada yetkili veri koruma otoritesi tarafından söz konusu onayın verilmesinden önce aktarıma tabi olacak her bir grup üyesi şirket tarafından aralarında gerçekleşecek veri işleme ve aktarım faaliyetlerinin neler olduğunun ve bu faaliyetlerin amaçlarının açık ve anlaşılır bir şekilde bağlayıcı şirket kurallarında belirtilmesi gerekmektedir[255]. Bu sayede kişisel veri işleme ve aktarım faaliyetlerinin hukuka uygunlukları değerlendirilebilecek ve hangi veri işleme ve aktarım faaliyetine uygun olarak aktarımın gerçekleştiği ortaya konulabilecektir.

Öte yandan bu işleme ve aktarım faaliyetleri ile amaçları süresince işlemeye ve aktarıma tabi tutulacak kişisel verilerin özel nitelikli veriler de dahil olmak üzere hangi veri kategorileri (kimlik, iletişim, sağlık, finans, meslek vb.) altında yer aldığı tek tek sıralanmalıdır. Örneğin ABD'deki grup üyesi şirkete Almanya'daki diğer grup üyesi şirketçe yapılan satışlara ilişkin müşterilerin ad, soyadı, telefon numarası, e-posta adresi, satın aldıkları ürünler ve bunların adedi, fiyatı vb. bilgilerin aktarılması halinde Almanya'dan ABD'ye aktarılan bu verilerin bağlı oldukları kategori ile birlikte bağlayıcı şirket kurallarında belirtilmesinde fayda bulunmaktadır. Özellikle aktarımın sağlık, cinsel hayat, din vb. gibi özel nitelikli

[255]Working Paper, Md. 29 Çalışma Grubu, 256.

kişisel veriler üzerinden gerçekleşmesi halinde hassas veriler için alınması gereken tedbirlerin belirlenmesi anlamında da önem arz etmektedir. Diğer taraftan grup üyesi şirket ayrıca bu verilerin sahibi olan ilgili kişilerin türleri de belirtilmelidir[256]. Buna göre veri işleme ve aktarım faaliyetlerinden etkilenecek ilgili kişilerin ve bu kişilerin olası taleplerinin belirlenmesi ile bağlayıcı şirket kurallarının onay süresi esnasında yetkili veri koruma otoritesi tarafından buna bağlı olacak yapılacak risk analizlerinin gerçekleşmesi açısından önemli rol oynamaktadır. Ayrıca AB sınırları içerisinden kişisel veri aktarımın yöneleceği ve AB sınırları dışında bulunan üçüncü ülkelerin de yine bu bölümde sıralanması gerekmektedir. Bu sayede ilgili ülkelerin yeterlilik kararının bulunup bulunmadığı ülkeler olup olmadığının tespiti yapılabilecek ve bağlayıcı şirket kurallarının yer bakımından uygulanma alanı da açık bir şekilde ortaya konmuş olacaktır.

3.2.4.3. İç ve Dış Bağlayıcılık

Tüzük m.47/2 (c) uyarınca bağlayıcı şirket kurallarının iç ve dış bağlayıcılık unsurlarını içermesi gerektiği düzenlenmiştir. Buna karşılık iç ve dış bağlayıcılık kavramları Tüzük'te tanımlanmamıştır. Bu kavramlar için Tüzük'te herhangi bir açıklama yer almasa da Birlik Kurulu tarafından verilen görüşlerde bağlayıcı şirket kurallarına taraf olan grup üyesi şirketler için iç ve dış bağlayıcılık kriterlerinin ne anlama geldiği ve bu taahhütler ile şirketlerden nelerin beklendiği ayrıntılı bir şekilde açıklanmıştır. Birlik Kurulu'nun bağlayıcı şirket kurallarına ilişkin kendisine iletilen başvurular süresince yaptığı değerlendirmeler ve muhtelif zamanlarda paylaştığı görüşlerine göre bağlayıcı şirket kuralları için iç bağlayıcılık, bağlayıcı şirket kurallarına taraf olan her bir grup üyesi şirketin bu kurallarla hukuken bağlı olması anlamına gelmektedir. İç bağlayıcılık ile bağlayıcı şirket kurallarının her bir grup üyesi için geçerli bir şekilde uygulanması için söz konusu grup üyesi şirketlerin bu kurallarla bağlı olduğuna yönelik açık taahhütlerde

[256]Direktif'in yürürlükte olduğu dönemde üçüncü ülkelere veri aktarımı, aktarıldığı AB üyesindeki veri koruma makamının onaylamasına bağlı idi. Bu onay süreci, verilerin aktarımının yapıldığı ülkeye ilişkin gerekli bütün bilgilerin elde edildiği kabulüne dayanmaktaydı bkz. Toparlak, s.54.

bulunması ve bu bağlılığı sürdürebilmesi için belirli yükümlülükleri yerine getirmesi gerekmektedir. Bu kapsamda her bir grup üyesi şirket tarafından bu taahhütler ve yerine getirilecek yükümlülükler ile alınacak tedbirler bağlayıcı şirket kurallarında düzenlenmelidir. Bu yükümlülüklerin tam olarak yerine getirilmesi için her bir grup üyesi şirket kendi çalışanlarının da tabi olacağı belirli kurallar ve talimatlar oluşturarak şirketin başlı başlına bağlayıcı şirket kuralları ile uyumlu olması ve topluluk içerisinde iç bağlayıcılığın sağlanmasına yönelik taahhütlerde bulunmaktadır. Grup üyesi şirketin bu kapsamda kendi çalışanlarına ne şekilde talimat vereceği ve kurallarla uyum sürecini hangi tedbirleri alarak yürüteceği ise kendi takdirine bırakılmıştır. Ancak her halde ilgili grup üyesi şirket tarafından bu yapının ne şekilde oluşturulduğunun ve alınacak tedbirler ile verilen taahhütlerin bağlayıcı şirket kurallarında belirtilmesi gerekmektedir[257]. Şirket içerisinde çalışanların tabi olacağı bir veri koruma politikası oluşturulması ve bu politikaya uyumun belirli disiplin hükümleri ile teminat altına alınması iç bağlayıcılığın sağlanması için alınabilecek tedbirler arasında yer almaktadır. Bununla birlikte düzenli eğitimler ve periyodik denetimler de yine grup üyesi şirket tarafından bu kurallara uyumu sürekli kılabilmek ve çalışanlarını da dahil edebilmek adına alınabilecek tedbirler arasında yer almaktadır.

İç bağlayıcılığın yanı sıra dış bağlayıcılık ise grup üyesi şirketlerin kendileri diğer bir deyişle topluluk dışındaki unsurlarla olan etkileşime ilişkin taahhütleri içermektedir. Bağlayıcı şirket kurallarının uygulanma alanıyla bağlantılı olarak topluluk dışında taahhütte bulunacak ilk kitle söz konusu grup üyesi şirketlerin aktarıma tabi tuttukları kişisel verilerin sahibi ilgili kişilere yöneliktir. Dış bağlayıcılık taahhütleri ile grup üyesi şirketler ilgili kişilerin kişisel verilerinin korunmasından doğan yasal haklarını ne şekilde kullanabileceğini açık ve anlaşılabilir bir şekilde bağlayıcı şirket kurallarında belirtmelidir. Bu hakların etkili bir şekilde kullanılması ve ilgili kişi taleplerinin hızlı bir şekilde yerine getirilmesi için alınabilecek tedbirler dış bağlayıcılık taahhütlerinin başında yer almaktadır. Bu

[257]Working Paper, Md. 29 Çalışma Grubu, 256, 257.

mekanizmaların öngörülebilir ve kesin bir şekilde düzenlenmesi kurallar ile amaçlanan şeffaflık ilkesine riayet edilmesi için büyük önem arz etmektedir. Bu hakların kullanımına imkân tanıyan tedbirlere yer verilmesinin yanı sıra aksi halde diğer bir deyişle bu hakların etkili bir şekilde kullanımına olanak tanınmaması ya da tanınsa da hukuken amaçlanan sonuçlara ulaşılamamış olması halinde ortaya çıkacak zararlardan dolayı sorumluluğun grup üyeleri tarafından üstlenilmesi de dış bağlayıcılık taahhütleri arasında yer almaktadır. Grup üyesi şirketlerin bu şekilde ortaya çıkabilecek ihlallerden doğan sorumluluğu ne şekilde üstlendiklerini, bu sorumluluğun hangi grup üyesi şirket tarafından üstlenileceği ve zararların nasıl tazmin edileceğini de açık bir şekilde bu kurallar dahilinde belirtmesi gerekmektedir. Özellikle AB sınırları dışında ortaya çıkan veri ihlalleri halinde bu ihlalin hangi grup üyesi şirket tarafından ne şekilde telafi edileceği AB sınırları dışında bu kuralların etkili bir şekilde uygulama alanı bulabilmesi ve ilgili kişi haklarının korunabilmesi için önemli bir rol oynamaktadır[258].

3.2.4.4. Veri İşleme İlkeleri, Hukuka Uygunluk Sebepleri ve Veri Güvenliği

Tüzük m. 47/2 (d) uyarınca grup üyesi şirketlerin bağlayıcı şirket kuralları kapsamında alacakları topluluk özelindeki veri koruma tedbirlerinin yanı sıra gerçekleştirecekleri her bir veri işleme ve aktarım faaliyetleri için Tüzük'te öngörülen veri işlemenin genel ilkelerini yerine getirmeleri gerekmektedir. Bu kapsamda grup üyesi şirketlerin yalnızca aktarımın amacıyla uyumlu verileri aktarıma dahil etmesi ve veri minimizasyonunun sağlanması için gerekli tedbirleri alması beklenmektedir. Verilerin en alt düzeye indirilmesi ile bağlantılı olarak söz konusu verilerin saklanma sürelerinin de yine asgari olarak düzenlenmesi ve amaçlarının ötesinde saklanmaya devam edilmemesi gerekmektedir. Bununla birlikte kişisel verilerin Tüzük'te öngörülen yasal dayanaklardan en az birine tabi olacak şekilde işlenmesi ve aktarılması gerekmektedir. Aksi halde bağlayıcı şirket kuralları ile öngörülmüş dahi olsa hukuki dayanaktan yoksun bir veri işleme ve

[258]Working Paper, Md. 29 Çalışma Grubu, 74, 108, 152.

aktarım faaliyeti gündeme gelecektir. Genel veri işleme ilkelerinin ve hukuka uygunluk sebeplerinin ışığında gerçekleşecek veri işleme ve aktarım faaliyetleri süresince veri güvenliğinin temin edilmesi için de gerekli tedbirlerin alınması ve bu tedbirlerin başta özel nitelikli kişisel veriler için olmak üzere neler olduğunun açık bir şekilde bağlayıcı şirket kurallarında belirtilmesi gerekmektedir[259]. Çalışmamızın ikinci bölümünde söz konusu hukuka uygunluk sebepleri ile grup üyesi şirketlerin aktarım süresince tabi olacakları genel veri işleme ilkeleri ile alabilecekleri veri güvenliği ilkelerine ayrıntılı bir şekilde yer verildiğinden bu bölümde açıklamalarımızı bu haliyle sınırlı tutuyoruz.

3.2.4.5. İlgili Kişilerin Hakları

Tüzük m.47/2 (e) uyarınca kişisel verileri grup içi aktarımlara tabi tutulan ilgili kişilere Tüzük m. 15 (erişim hakkı), m. 16 (düzeltilmesini ve değiştirilmesini talep etme hakkı), m. 17 (unutulma/silinmesini talep etme hakkı), m. 18 (işleme faaliyetinin kısıtlanmasını talep etme hakkı), m. 20 (veri taşınabilirliği hakkı), m. 21 (itiraz hakkı), m. 22 (profil çıkarma da dahil olmak üzere otomatik münferit karar verme hakkı) ve m. 82 (tazminat talep etme hakkı) uyarınca sağlanan yasal hakların bağlayıcı şirket kuralları kapsamında ilgili kişilerce etkin bir şekilde kullanılabileceğine dair taahhütlerin ve bu amaçla oluşturulan mekanizmaların yer alması gerekmektedir.. Bunun yanı sıra, ilgili kişinin bulunduğu ülkenin ulusal veri koruma mevzuatında Tüzük'te belirtilenler dışında farklı ilgili kişi hakları bulunuyorsa bu hakların da bağlayıcı şirket kurallarında düzenlenmesi beklenmektedir.

Bağlayıcı şirket kurallarında Tüzük uyarınca ilgili kişilere tanınan yasal hakların neler olduğunun yanı sıra bu hakların kullanımı için topluluk dahilinde her bir grup üyesi şirket tarafından oluşturulan ve bu hakların kullanma yöntemlerini içeren mekanizmaların da belirtilmesi gerekmektedir. Bu noktada ilgili kişilerin taleplerini

[259]Toparlak, s.55.

hangi kanallarla söz konusu grup üyesi şirkete ulaştıracağının, bu taleplerin ne kadar süreyle ve ne şartlarda değerlendirme altına alınarak cevaplanacağının, ilgili kişinin söz konusu cevabı yeterli bulmaması halinde yetkili veri koruma otoritesine şikâyet hakkının ve/veya kendi ülkesindekiler de dahil olmak üzere yetkili mahkemelere başvurarak dava hakkını kullanabileceğinin de açık bir şekilde belirtilmesi gerekmektedir[260]. Özellikle grup üyesi şirketlerin ilgili kişi taleplerinin alınması ve incelenmesi ile yerine getirilmesine ilişkin usul ve esasları düzenleyen topluluk politikaları ve prosedürleri oluşturması önemli rol oynayacaktır.

3.2.4.6. AB'deki Grup Üyesinin Sorumluluğu Üstlenmesi

Bağlayıcı şirket kurallarında, Tüzük m.47/2 (f) uyarınca AB'de kurulu olan grup üyesi şirketlerden en az birinin kişisel verilerin aktarımının yapıldığı üçüncü ülkedeki muhtemel ihlaller ve bu ihlallerin yol açacağı zararlar bakımından sorumluluğu açık bir şekilde üstlendiğinin belirtilmesi gerekmektedir. Bu düzenleme sorumluluğun AB sınırları içerisinde kurulu olan grup üyesi şirketin sorumluluğuna gidileceğinin ve tazminat gibi belirli taleplerin muhatabı olacağının açık bir şekilde ortaya konulması ile birlikte kuralların şeffaflık ilkesine uygun bir şekilde hazırlanmasına ve uygulanmasına da yardımcı olmaktadır. Bu hüküm uyarınca AB'deki grup üyesi şirketin sorumluluğu üstlenmesi ile birlikte ortaya AB sınırları dışındaki üçüncü ülkede kurulu grup üyesi şirket ile birlikte ortak sorumluluk mekanizması oluşturulmaktadır[261]. Bu durum ilgili kişilerin taleplerinin yerine getirilmesinde ve zararların tazmini ile ihlallerin telafi edilmesinde AB'deki ve üçüncü ülkedeki grup üyesi şirketlerin ortak şekilde hareket etmesini ve sorumluluğu paylaşmalarını zorunlu kılmaktadır. Ancak AB'deki üye şirketin AB sınırları dışında üçüncü ülkede ortaya çıkan söz konusu ihlalin meydana gelmesinde hiçbir şekilde kusuru bulunmuyorsa sorumluluktan muaf olabilecektir.

[260]Working Paper, Md. 29 Çalışma Grubu, 256.
[261]Moerel, s.219.

Görüldüğü üzere AB'de kurulu üye şirketin ortak sorumluluğa katılımı kusuruyla bağlantılı olarak gündeme gelmektedir. Kendisinin bu zararın ortaya çıkmasından herhangi bir kusuru olmadığının ispatı ise yine AB'deki grup üyesi şirkete aittir. Bu durum adeta AB'de kurulu grup üyesi şirket için bir kurtuluş beyyinesi teşkil etmektedir[262]. AB'de kurulu grup üyesi şirketin bağlayıcı şirket kurallarının topluluk içinde her bir grup üyesi şirketçe usulüne uygun bir şekilde uygulama alanı bulup bulmadığının belirli aralıklarla denetlenmesi ve gözetlenmesi gerekmektedir. Bu kapsamda AB'de kurulu grup üyesi şirketin bir özen ve gözetim yükümlülüğünün bulunduğunu söylemek yanlış olmayacaktır. Tüzük kapsamında AB'de kurulu olan hangi grup üyesi şirketin AB dışındaki üçüncü ülkede bulunan diğer grup üyesi ile müştereken sorumlu olacağı düzenlenmeyerek bu konuda topluluk üyelerine bir takdir yetkisi verilmiştir. Ancak uygulamada üçüncü ülkedeki diğer grup üyesi şirket ile sorumluluğu paylaşan grup üyesi şirketin genellikle topluluktaki AB'de kurulu olan hâkim şirket olduğu görülmektedir[263].

AB'de kurulu grup üyesi şirketin söz konusu özen ve gözetim yükümlülüğü bağlayıcı şirket kurallarının her bir grup üyesi şirketçe uygulanıp uygulanmadığının ve uygulanıyorsa ne şekilde uygulandığının belirli aralıklarla denetlenmesi ve raporlanmasının yanı sıra aynı zamanda AB dışında kurulu olan grup üyesi şirketlerin kendi ülkelerinde tabi oldukları veri koruma mevzuatlarının söz konusu bağlayıcı şirket kurallarının uygulanması için ne kadar uygun olduğunun ve bu kurallarla çelişecek hükümler içerip içermediğinin araştırılması ve incelenmesini de kapsamaktadır. Öyle ki belirli durumlarda bağlayıcı şirket kurallarına aykırılık üçüncü ülkede kurulu olan ilgili grup üyesi şirketin kendi iç hukukundan kaynaklı belirli yükümlülükleri yerine getirmesinden dolayı da ileri gelebilecektedir. Üçüncü ülkenin iç hukukunda yer alan bir düzenlemenin bağlayıcı şirket kurallarının uygulanması ile çelişip çelişmediğine ilişkin ihtiyaç halinde AB'deki yetkili veri koruma otoritelerinden de görüş alınması mümkündür. Bu hükümlerin tespiti ile

[262] Çekin, '6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanununun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 74, S. 2, 2016, s.638.
[263] Toparlak, s.56.

birlikte bağlayıcı şirket kurallarının iç hukuk düzenlemelerine rağmen uygun bir şekilde uygulamaya konulabilmesi için gerekli tedbirlerin alınması gerekmektedir. Ayrıca bu sebeplerle ortaya çıkabilecek olası ihlal durumlarının olabildiğince erkenden tespit edilmesi ve bağlayıcı şirket kurallarının da söz konusu mevzuat hükümlerine uygun olarak hazırlanması ve şekillendirilmesi bu kuralların uygulanabilirliğini olumlu yönde etkilemekte ve ileride ortaya çıkabilecek uyuşmazlıkların önüne geçilmesinde katkı sağlamaktadır.

3.2.4.7. Bağlayıcı Şirket Kurallarına İlişkin Bilgilerin İlgili Kişilere Bildirilmesi

Tüzük m. 47/2 (g) uyarınca grup üyesi şirketlerin hazırladıkları bağlayıcı şirket kurallarının temel konusu olan aktarıma tabi kişisel verilere ilişkin Tüzük m. 13 ve m. 14'te öngörülen hususlarda ilgili kişileri bilgilendirmesi gerekmektedir. Tüzük m. 13 ve m. 14 uyarınca kişisel verilerin ilgili kişiden temin edilmiş olup olmaması göre veri sorumlusunun (kontrolürün) ilgili kişiyi bilgilendirme yükümlülüğü öngörülmüştür. Bu yükümlülük tıpkı KVKK m. 12 uyarınca ilgili kişilerin gerçekleşen kişisel veri işleme ve aktarım faaliyetlerine ilişkin bilgilendirilmesi şeklindedir. Tüzük m. 13 ve m. 14 uyarınca bağlayıcı şirket kuralları hazırlayan ve bu kurallara uygun olarak sınır ötesi veri aktarımı gerçekleştirecek her bir grup üyesi şirketin kendisi ya da varsa temsilcisinin kimlik ve irtibat bilgilerini ve gerekli ve uygun olması halinde kontrolörün veri koruma görevlisinin bilgilerini, kişisel veri işleme ve aktarım amaçları ile bunların hukuka uygunluk sebeplerini, işlenecek kişisel verilerin kategorilerini, bunların toplanma ve elde edilme yöntemlerini ve kaynaklarını, kişisel verilerin saklanacağı süreyi, ilgili kişinin söz konusu veri işleme ve aktarım faaliyetleri karşısındaki yasal haklarının neler olduğunu, aktarıma tabi tutulan bu verilerin alıcı gruplarını, bu aktarımların AB sınırları dışındaki üçüncü bir ülkeye yönelik gerçekleşeceğini ve bu ülke için Komisyon'un yeterlilik kararı vermiş olmadığını ve aktarımın bağlayıcı şirket kuralları çerçevesinde gerekli veri güvenliği tedbirleri alınması suretiyle gerçekleştirilecek olduğunu ilgili kişilere bildirmelidir.

Veri sorumlusunun bu bilgileri kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde ancak kişisel verilerin elde edilmesinden itibaren en geç bir ay içerisinde veya kişisel verilerin ilgili kişi ile iletişime geçilmek amacıyla işlenecek olması halinde en geç ilgili kişi ile ilk kez temasa geçildiği zamanda ya da kişisel verinin veri sorumlusu dışında farklı bir alıcıya açıklanacak olması halinde en geç kişisel verinin ilk kez söz konusu alıcıya açıklandığı zamanda bildirmesi gerekmektedir. Söz konusu bilgilerin ne şekilde ilgili kişilere aktarılacağının da bağlayıcı şirket kuralları kapsamında belirtilmesi gerekmektedir. Bu noktada grup üyesi şirketler ilgili kişilere e-posta yoluyla ya da internet siteleri üzerinden veya uygun buldukları farklı yöntemlerle ilgili kişileri aydınlatma yükümlülüklerini yerine getirebilirler. Bu yükümlülüğün yerine getirilmesi esnasında ilgili kişilerin bağlayıcı şirket kuralları ile gerçekleştirilecek veri aktarım faaliyetleri hakkında açık ve anlaşılır bir şekilde bilgi sahibi olması, Tüzük'ten doğan haklarını tam olarak kavrayabilmeleri ve bu haklarını kullanabilmek amacıyla başvurabilecekleri yöntemlerden tam olarak haberdar olabilmeleri amaçlanmalıdır[264].

3.2.4.8. Veri Koruma Görevlisi Atanması

Tüzük m. 47/2 (h) uyarınca bağlayıcı şirket kuralları ile sınır ötesine veri aktarımı gerçekleştirecek topluluk üyelerinin söz konusu kuralların topluluk bünyesinde uygulanmasını takip edecek, gerekli hallerde eğitimlerin organizasyonu ve ilgili kişi taleplerinin ve şikayetlerinin alınması ve incelenmesi gibi konularda gerekli çalışmaları yürütecek veri koruma görevlisi ataması gerekmektedir. Söz konusu görevlinin Tüzük m. 37'de öngörülen şartlar gözetilerek seçilmesi ve bu kişinin irtibat bilgileri ile görevlerinin neler olduğunu bağlayıcı şirket kurallarında açık ve anlaşılır bir şekilde belirtilmesi gerekmektedir. Veri koruma görevlisinin görevi topluluk dahilindeki grup üyesi şirketlerin kişisel verileri korumasına yönelik yerine getirmesi gereken yasal yükümlülükleri düzenli olarak takip etmek ve alınması gereken veri güvenliği tedbirlerine ilişkin süreçleri yönetmektir. Bu

[264] Toparlak, s.57.

amaçla grup üyesi şirketler kurumsal yapıları dahilinde veri koruma görevlisinin de aralarında bulunduğu kişisel veri mevzuatına uyum adına ayrı bir departman da kurma yoluna gidebilirler. Bu kapsamda grup üyesi şirketlerin bağlayıcı şirket kurallarına ve kişisel veri koruma mevzuatına uyum sağlanması ve her bir grup üyesi şirketin çalışanlarının bu konuda bilgilendirilmesi noktasında veri koruma görevlisi önemli bir rol oynamaktadır[265]. Tüzük m. 37 uyarınca veri koruma görevlisinin veri koruma hukuku ve uygulamasına ilişkin bir uzmanlık bilgisi taşıması gerekmektedir. Ayrıca veri koruma görevlisinin topluluk bünyesindeki grup üyesi şirketlerden herhangi birinin çalışanları arasından ya da şirket dışından üçüncü bir kişi ile yapılacak hizmet sözleşmesine bağlı olarak seçilmesi mümkündür.

3.2.4.9. Şikâyet Usulleri

Tüzük 47/2 (i) uyarınca bağlayıcı şirket kurallarında grup üyesi şirketlerce gerçekleştirilen veri işleme ve aktarım faaliyetlerine yönelik verileri işlenen ve aktarılan ilgili kişilerin yasal haklarını kullanabileceği ve gerektiğinde söz konusu işleme ilişkin olarak itiraz ve şikâyet başvurusunda bulunabileceği mekanizmaların belirtilmesi gerekmektedir. Bu mekanizmalar ilgili kişilerin yasal haklarını etkili, hızlı ve kolay bir şekilde kullanmalarına olanak tanımalıdır. Bununla birlikte bağlayıcı şirket kurallarında bu mekanizmaların ve başvuruda izlenmesi gereken yöntemlerin neler olduğunun belirtilmesi gerekmektedir. Topluluk bünyesinde bu amaçla bir birim veya departman kurulması ya da mevcut departmanlar arasında bu görevi yürütecek birimlerin belirlenmesi, başvuruların ne şekilde alınacağı, değerlendirileceği ve sonuçlanacağına dair bir kurumsal topluluk politikası hazırlanması, internet sitesi üzerinden ilgili grup üyesi şirketlere yönelik şikayet başvurularının iletilebileceği herhangi bir sayfa ya da şikayet portalı oluşturulması, şikayetlerin alınacağı özel bir e-posta adresi oluşturulması ve/veya şikayet başvuru formlarının hazırlanarak ilgililer ile paylaşılması bu kapsamda topluluğun

[265]Mc Kay Cunningham, Complying with International Data Protection Law, University of Cincinnati Law Review, S.84 (2), 2018, s.439.

belirleyebileceği şikayet yolları arasında yer almaktadır. Ayrıca ilgili grup üyesi şirkete iletilen bu şikâyet başvurularının başvurunun niteliğine göre bir ila üç ay içinde incelenerek cevaplanması gerekmektedir[266].

3.2.4.10.Denetim ve Raporlama Süreçleri

Tüzük m.47/2 (j) ve (k) uyarınca bağlayıcı şirket kurallarına taraf olan her bir grup üyesi şirketin bu kurallardan ve kişisel veri mevzuatından doğan yükümlülüklerini sürekli bir şekilde yerine getirmesi ve bu uyum sürecinin düzenli olarak belirli aralıklarla denetlenmesi gerekmektedir. Söz konusu denetim ve kontrollerin yeterli uzmanlığa sahip topluluk dışından üçüncü kişiler aracılığıyla gerçekleştirilmesi de mümkündür[267]. Bu denetimler ile ileride ortaya çıkabilecek ve ciddi zararlara sebep olabilecek aykırılıkların erkenden tespit edilmesi sağlanır. Bu kapsamda her bir grup üyesi şirketin faaliyetlerinin bağlayıcı şirket kurallarına ve mevzuat hükümlerine uyumlu olduğunun denetlenmesi ve bu denetimler sonucu tespit edilen eksikliklerin ve/veya aykırılıkların şirketin üst birimlerine raporlanarak giderilmesi için gerekli çalışmaların gecikmeksizin yürütülmesi beklenmektedir. Öyle ki bağlayıcı şirket kuralları ile kişisel veri güvenliği ve gizliliği konusunda topluluk dahilindeki her bir grup üyesi şirketin sürekli bir uyumluluk içerisinde olması amaçlanmaktadır.

Bu çerçevede grup üyesi şirketler için uyumluluk sürecinin süreklilik teşkil etmesi adına şirketlerin veri güvenliğine ilişkin aldığı tedbirlerin yeterliliklerinin ve güncelliklerinin belirli aralıklarla test edilmesi, çalışanlara düzenli olarak veri koruma alanındaki yeniliklere ilişkin eğitimler verilmesi, periyodik denetimlerin gerçekleştirilmesi ve bu denetimlerde görülen eksiklik ve/veya aykırılıkların usulüne uygun bir şekilde raporlanması ve gerekli iyileştirme çalışmalarının yapılması büyük bir önem arz etmektedir. Bununla birlikte söz konusu raporlar[268]

[266]Working Paper, Md. 29 Çalışma Grubu, 268, 257, 74, 108.
[267]Working Paper, Md. 29 Çalışma Grubu, 256-257.
[268]Toparlak, s.58.

ileride ortaya çıkabilecek uyuşmazlıklarda ispat aracı olarak kullanılabilecektir. Ayrıca bu çalışmalar bağlayıcı şirket kurallarının da amaçladığı şeffaf bir yapının oluşmasına ve bu kuralların sürekli güncel ve geçerli bir şekilde yürürlükte kalmasını sağlamaya yardımcı olacaktır. Çalışmamızın ikinci bölümünde ayrıntılı olarak açıklamalarına yer verdiğimiz grup üyesi şirketlerin kişisel veri aktarımlarında alabilecekleri veri güvenliği önlemleri denetim ve denetimler faaliyetleri, bağlayıcı şirket kurallarının düzenlenmesi ve uygulanması esnasında da göz önünde bulundurulmalıdır.

3.2.4.11. Yetkili Veri Koruma Otoritesiyle Koordinasyon ve İş Birliği

Bağlayıcı şirket kurallarına taraf olan grup üyesi şirketlerin gerek kendi ortalık yapılarında gerekse ticari faaliyetlerinde zaman içinde belirli değişiklikler gündeme gelebilir. Bu şirketler grup içi veya grup dışı birleşme veya devralma işlemlerine taraf olarak ortaklık yapılarında değişim gösterebilirler. Bununla birlikte grup üyesi şirketlerin topluluk dahilinde ya da birel olarak almış olduğu kararlar ve belirledikleri stratejiler uyarınca ticari faaliyetlerinde de değişiklikler meydana gelebilir. Söz konusu değişikliklerin grup üyesi şirketlerin taraf olduğu bağlayıcı şirket kurallarında da değişikliğe gidilmesine sebep olması durumunda bu kuralların gecikmeksizin değiştirilmesi ve yeni şartlara uygun bir şekilde güncellenmesi gerekmektedir. Yapılan güncellemelerin ise Tüzük m. 47/2 (k) uyarınca bağlayıcı şirket kurallarını onaylayan yetkili veri koruma otoritesine bildirilmesi beklenmektedir. Şayet söz konusu değişiklik bağlayıcı şirket kurallarında esaslı bir değişikliğe sebep oluyorsa bu durumda yetkili veri koruma otoritesine yapılacak bildirimin yanı sıra bağlayıcı şirket kurallarının yapılan değişikliklerle geçerliliğinin yeniden değerlendirilmesi için yetkili otoritenin onayına da ihtiyaç duyulabilecektir.

Grup üyesi şirketlerin ortaklık veya yönetim yapılarında ya da ticari faaliyetlerinde meydana gelen değişiklikler kişisel verilerin aktarılacağı ülkelerin ve/veya alıcı taraftaki grup üyesi şirketin ve/veya yürütülen kişisel veri aktarım faaliyetinin ya

da aktarıma tabi tutulan kişisel verilerin değişmesine yol açabilir. Buna bağlı olarak değişiklik sonrası başlanan kişisel veri aktarım faaliyetlerinin ve yeni aktarım amaçlarının irdelenmesi ve bu amaçlara karşılık gelecek hukuka uygunluk sebeplerinin varlığının incelenmesi gerekecektir. Ayrıca aktarımına başlanan kişisel verilere yönelik alınması gereken veri güvenliği tedbirlerinin de yapılan yeni aktarım faaliyeti için uygunluklarının ve yeterliliklerinin yeniden değerlendirilmesi faydalı olacaktır. Örneğin söz konusu değişiklik ile grup üyesi şirketlerin sağlık verilerini işleme başlaması halinde hassas veri kategorisinde bulunan sağlık verilerinin güvenliklerinin ve gizliliklerinin sağlanması için ilgili grup üyesi şirketlerce kriptografik koruma yöntemlerinin benimsenmesi ve bu kapsamda topluluk içerisinde gerekli tedbirlerin alınarak bunların bağlayıcı şirket kurallarında da belirtilmesi gerekmektedir. Diğer taraftan şirketlerdeki ortaklık ve yönetim yapılarındaki değişikliklerin de gecikmeksizin bağlayıcı şirket kurallarına ve özellikle grup şirketlerin kimlik ve irtibat bilgilerine yansıtılması ve akabinde yetkili veri koruma otoritesine yazılı olarak bildirilmesi gerekmektedir.

Bununla birlikte gündeme gelen değişikliğe göre bağlayıcı şirket kuralları güncellense de ve bu değişiklik yetkili veri koruma otoritesine bildirilse de belirli durumlarda yalnızca söz konusu bildirimin yapılması yeterli görülmeyebilir. Bu durumda bildirimin yanı sıra bağlayıcı şirket kurallarının yapılan değişiklikler ile yeniden uygulamaya konulabilmesi için yeniden yetkili veri koruma otoritesinin onayının alınması gerekmektedir. Yetkili veri koruma otoritesinin onayına yeniden başvurulmasının gerektiği durumlar genellikle bağlayıcı şirket kurallarının esaslı bir şekilde değiştirilmesinin gerektiği hallerdir. Yapılan değişikliğin bağlayıcı şirket kurallarının yeniden düzenlenmesini gerektirmesi durumunda da hazırlanacak yeni bağlayıcı şirket kuralları için ilgili grup üyesi şirketlerin yetkili veri koruma otoritesinden onay almaları gerekecektir. Bu değişikliğin bağlayıcı şirket kurallarını esaslı bir şekilde etkileyip etkilemediği konusunda grup üyeleri arasında bir şüphe varsa böyle bir durumda gecikmeksizin yetkili veri koruma otoritesine bildirimde bulunulmalıdır. Aksi halde yapılan değişikliğin bağlayıcı şirket kurallarına yansıtılmaması ya da geç yansıtılması veya yansıtılmasına rağmen

bu değişikliğin yetkili otoriteye bildirilmemesi ya da bildirilse de yetkili otoriteden bu değişikliler için onay alınmaması halinde hukuka uygunluk temelinden yoksun bir şekilde sınır ötesi aktarımlar gündeme gelebilecek ve bu durum ilgili grup üyesi şirketler için hukuka aykırı sonuçların ortaya çıkmasına yol açabilecektir. 29. Madde Çalışma Grubu bağlayıcı şirket kurallarında hangi hallerde esaslı değişikliğe gidilmesi gerektiğine görüşlerinde yer vermektedir[269]. Buna göre grup içi veri aktarım süreçlerinde herhangi bir değişiklik meydana gelmişse ya da topluluk dahiline aktarıma taraf olacak yeni bir grup şirket katılmışsa bağlayıcı şirket kurallarında da esaslı değişiklik yapılması gerekecektir. Bu sebeple grup üyesi her bir şirketin gerekli durumlarda hazırlanan bağlayıcı şirket kurallarını güncelleyebileceklerini ve bu güncellemeleri gecikmeksizin yetkili veri koruma otoritesine bildireceklerini bağlayıcı şirket kuralları dahilinde taahhüt etmeleri gerekmektedir.

Grup üyesi şirketlerin bağlayıcı şirket kurallarına ilişkin yapacakları bildirimlerden bir diğeri de Tüzük m. 47/2 (m) uyarınca öngörülen bildirim yükümlülüğüdür. Bu kapsamda yapılacak bildirimler bağlayıcı şirket kuralları hazırlanıp onay için yetkili veri koruma otoritesine sunulduğunda yapılabileceği gibi gerekli olması halinde söz konusu onay sürecinden sonra da yapılabilecektir. Tüzük m. 47/2 (m) uyarınca AB'de kurulu grup üyesi şirketin AB sınırları dışındaki üçüncü ülkelerde kurulu diğer grup üyesi şirketlerin tabi olduğu iç hukuk düzenlerini ve yerel mevzuatlarını inceleme ve bu mevzuat hükümlerinin bağlayıcı şirket kurallarının ilgili ülkede uygulanması önünde herhangi bir engel teşkil edip etmediğini tespit ederek bu durumu yetkili veri koruma otoritesine bildirme yükümlülüğü bulunmaktadır. Bu bildirimin yapılması gerekliliğinin yanı sıra ilgili grup üyesi şirketlerce bağlayıcı şirket kuralları uyarınca öngörülen yükümlülüklerin yerine getirilmesine engel olarak yerel mevzuat hükümlerinin sebep olduğu çelişkinin ne şekilde ortadan kaldırılabileceğini ve Tüzük ile uyumlu bir mekanizma ortaya çıkarılabileceğini araştırma ve bu kapsamda gerekli tedbirleri alarak bunları bağlayıcı şirket

[269]Working Paper, Md. 29 Çalışma Grubu, 256-257, 204 rev01.

kurallarında belirtme yükümlülükleri bulunmaktadır. Öyle ki söz konusu çelişik durum bağlayıcı şirket kuralları dahilinde açık bir şekilde ifade edilmekle birlikte bu durumun bağlayıcı şirket kurallarının ve bu kurallarla öngörülen yükümlülüklerin uygulanmasını sağlamak adına ne şekilde telafi edildiğinin ve telafi amacıyla alınan önlemlerin neler olduğunun da bağlayıcı şirket kurallarında düzenlenmesi gerekmektedir. Söz konusu çelişkili hükümlerin tespit edilmesi ardından bu durumların sebep olabileceği veri aktarımlarındaki kısıtlamaların değerlendirilmesinde Tüzük m. 23'te öngörülen menfaat testi kriterlerinin uygulanması faydalı olacaktır. Çalışmamızın birinci bölümünde değindiğimiz üzere Schrems II kararıyla AB'den ABD'ye yapılan aktarımlar esnasında aktarıma tabi tutulan kişisel verilerin ABD'deki yerel mevzuat hükümleri uyarınca istihbarat teşkilatıyla paylaşılmasının Tüzük hükümlerine aykırılık teşkil etmesi söz konusu çelişkili yerel mevzuat hükümlerine örnek niteliğindedir[270]. Bu kapsamda aktarıma tabi grup üyesi şirketlerce bu tür durumların yerel mevzuat hükümleri uyarınca dikkatli bir şekilde irdelenmesi ve Tüzük ile hazırlanan bağlayıcı şirket kurallarında öngörülen hükümlere aykırılık teşkil edebilecek durumların yetkili veri koruma otoritesine bildirilerek bu durumlara karşı gerekli ek veri güvenliği tedbirlerinin alınması gerekmektedir.

Söz konusu çelişkili düzenlemeler özellikle Tüzük uyarınca hazırlanan bağlayıcı şirket kurallarının Türkiye'deki bir grup üyesi şirket tarafından uygulanacağı sırada da belirli sorunlara sebep olabilecektir. Örneğin bağlayıcı şirket kuralları uyarınca belirli veri işleme ve aktarım faaliyetlerinin ilgili kişinin rızasına bağlı olarak gerçekleşeceği kabul edilmişse Tüzük ve KVKK uyarınca rıza kavramlarının farklı şekilde düzenlenmiş olması belirli aykırılıkları da beraberinde getirebilir. Öyle ki Tüzük uyarınca rızanın KVKK'da olduğu gibi açık rıza şeklinde öngörülmemiş olması ve açık rıza olmasa da veri işleme ve aktarım faaliyetine onay verildiğini gösteren bir hareketin de Tüzük uyarınca geçerli bir hukuka uygunluk sebebi olarak kabul edilmesi söz konusu farklılıkların başında gelmektedir[271]. Grup üyesi

[270]C-362/14.
[271]Buchner ve Petri'ye ait kısım, Kühling, Buchner, s. 220.

şirketlerin böyle bir farklılığı tespit etmeleri halinde hem bağlayıcı şirket kuralları ile uyumun sağlanması hem de KVKK hükümlerine aykırı sonuçların ortaya çıkmasının önlenmesi açısından Türkiye'deki ilgili kişilerden alınacak rızaların açık rıza şeklinde alınması ve bu rızanın hizmet şartına bağlanmaması vb. gibi açık rızaya bağlı diğer şartları da karşılaması gerektiğini kabul etmeleri bir çözüm yolu olabilecektir. Diğer taraftan bağlayıcı şirket kuralları uyarınca bir veri için belirlenen saklama süresinin Türk hukukunda belirtilen ve kanunlarda halihazırda öngörülen saklama süresine aykırılık teşkil etmediğinden de emin olunması gerekmektedir. Örneğin grup içi kesilen faturaların 9 yıllık sürenin sonunda silineceği yönünde bir düzenleme TTK'da yer alan ticari belgelerin 10 yıl boyunca saklanması yükümlülüğüne aykırılık teşkil edebilecektir. Dolayısıyla saklama sürelerinin iç hukuk düzenlemeleri göz önüne alınarak belirlenmesi bağlayıcı şirket kurallarının geçerli bir şekilde uygulanma alanı bulması açısından büyük önem arz etmektedir[272].

Yetkili veri koruma otoritesine yapılacak bildirimlerin yanı sıra belirli durumlarda bağlayıcı şirket kurallarına taraf olan grup üyesi şirketlerin bu kuralların uygulanması ile ilişkili olarak yetkili veri koruma otoritesi ile iş birliği içerisinde çalışması gerekmektedir. Tüzük m. 47/2 (l) uyarınca bağlayıcı şirket kurallarını hazırlayan topluluk şirketleri için öngörülen söz konusu iş birliği yükümlülüğü esasında bu kuralların her bir grup şirket üyesi için bağlayıcı ve geçerli bir şekilde süreklilik içerisinde uygulama alanı bulabilmesi adına yetkili veri koruma otoritesi ile ortaklaşa bir çalışma yürütmesi anlamına gelmektedir. Bu kapsamda söz konusu kurallara uyum derecesinin tespiti açısından belirli aralıklarla yürütülen denetim faaliyetleriyle ilgili raporların yetkili veri koruma otoritesine sunulması ve bu raporlardaki bulgulara göre yetkili otoritenin varsa talimatlarının alınarak bunların yerine getirilmesi bağlayıcı şirket kurallarının uygulanmasını kolaylaştırmak adına yetkili veri koruma otoritesiyle yapılan iş birliğine birer örnektir. Grup üyesi şirketlerin gördükleri ihtiyaçlar üzerine yetkili veri koruma otoritesinden görüş

[272]Kamp'a ait kısım, von dem Bussche, Voigt, s. 351.

alınması, yetkili veri koruma otoritesinin verdiği talimatların yerine gecikmeksizin yerine getirilmesi, yetkili veri koruma otoritesine yapılacak başvuru ve bildirim süreçleri gibi iş birliği yöntemlerinin her birini hazırladıkları bağlayıcı şirket kurallarında belirtmeleri beklenmektedir[273].

3.2.4.12. Farkındalık Eğitimleri

Bağlayıcı şirket kurallarını kabul eden grup üyesi şirketlerin her biri kendi içindeki şirket çalışanlarına belirli aralıklarla kişisel verilerin korunması ve bağlayıcı şirket kurallarının etkin bir şekilde uygulanabilmesi için alınabilecek önlemlere ilişkin farkındalık eğitimleri vermekle yükümlüdür. Söz konusu eğitimlerin grup üyesi şirketler arasındaki kişisel veri aktarımları için ne denli büyük önem arz ettiği halihazırda Çalışmamızın ikinci bölümünde anlatılmıştır. Tüzük m.47/2 (n) uyarınca öngörülen eğitimler özellikle aktarıma tabi kişisel verilere erişimi bulunan personellere yönelik düzenlenmeli ve bu eğitimlerin ne kadar sıklıkla verileceği, eğitimin detayları ve eğitim programı da öngörülebildiği ölçüde bağlayıcı şirket kurallarında belirtilmeli ve taahhüt edilmelidir.

3.2.4.13. Bağlayıcı Şirket Kurallarının Onaylanması

Bağlayıcı şirket kuralları, farklı ülkelerin ulusal mevzuatlarına bağlı birçok grup üyesi şirket açısından bağlayıcı ve geçerli olacak şekilde hazırlanmakta ve uygulamaya konmaktadır. Bu sebeple her bir grup üyesi şirketin bulunduğu ülkedeki yetkili veri koruma otoritesinin bu kuralların kendi ülkelerinde kurulu olan grup üyesi şirket tarafından uygulamaya konması hususunda karar verme yetkisi bulunmaktadır. Tüzük m. 58/3 (j) uyarınca bu husus bir yetki olarak düzenlenirken aynı şekilde kendisine yönelik başvuru yoluyla iletilen bağlayıcı şirket kurallarının incelenerek onaylanması konusunda karar verilmesinin Tüzük m. 57/1 (s) uyarınca AB sınırları içerisindeki üye ülkelerde bulunan yetkili veri koruma otoriteleri için

[273] Toparlak, s.58.

bir görev olduğu da hüküm altına alınmıştır[274]. Buna rağmen ilgili veri koruma otoritesi tarafından tek başına verilecek onay kararı birden fazla grup şirketin taraf olacağı bağlayıcı şirket kurallarının geçerli olmasında yeterli görülmemektedir. Bu sebeple AB'de kurulu olan grup üyesi şirketlerin bulundukları ülkelerdeki yetkili veri koruma otoritelerinin Tüzük m.60 uyarınca kendi aralarında iş birliği içerisinde hareket etmeleri gerektiği ve verdikleri onay kararlarının Tüzük m. 63 uyarınca birbirleri ile uyumlu ve tutarlı olması gerektiği öngörülmüştür[275]. Öyle ki Tüzük'ün ve bağlayıcı şirket kurallarının üye devletlerde tutarlı bir biçimde tatbik edilebilmesi için AB'deki grup üyesi şirketlerin bulunduğu ülkelerdeki yetkili veri koruma otoritelerinin Tüzük'teki tutarlılık sistemine uygun olarak iş birliği içerisinde bir karar vermesi beklenmektedir. Söz konusu tutarlılık mekanizması uyarınca baş yetkili veri koruma otoritesinin yetkili veri koruma otoritelerinin görüşleri ile zıtlaşacak şekilde karar vermesinin önüne geçilmektedir. Bu sayede herhangi bir yetkili veri koruma otoritesinin bir diğerinden farklı yönde karar vermesi ve bağlayıcı şirketin onay sürecini sürüncemeye bırakacak süreçlerin ortaya çıkması riskinin önüne geçilmiş olur ve verilecek tek karar ile bağlayıcı şirket kuralları onaylanır ya da verilen gerekçeli karar ile birlikte reddedilir. Şu kadar ki söz konusu ret kararında yetkili veri koruma otoritesinin belirttiği talimatlar yerine getirilerek başvurudaki eksikliklerin tamamlanması ve onay için yeniden başvuruda bulunulması mümkündür. Tutarlılık sisteminde AB'deki her bir grup üyesi şirketin bulunduğu ülkede yetkili olan veri koruma otoritesinin birbirleriyle ve gerekmesi halinde Komisyonla koordinasyon halinde olmaları, birbirlerine gerekli bilgi ve belgeleri aktarmaları ve ihtiyaç duymaları durumunda verecekleri kararlardan önce Birlik Kurulu'ndan görüş alabilecekleri düzenlenmektedir[276]. Görüldüğü üzere AB'de kurulu her bir grup üyesi şirket kendi ülkesinde bulunan yetkili veri koruma otoritesinden onay kararı alarak bağlayıcı şirket kurallarını geçerli bir şekilde uygulamaya koyabilmektedir.

[274]Toparlak, s.62.
[275]Toparlak, s.62.
[276] Paal'e ait kısım, Paal, Pauly, s. 584.

Bununla birlikte Tüzük, grup şirketlerin yapısını ve bu sürecin zaman alıcı yanını göz önünde bulundurarak topluluk dahilinde bulunan şirketlerin merkezlerinin bulunduğu ülkedeki yetkili veri koruma otoritesinin baş yetkili veri koruma otoritesi olarak kabul edilmesi ve yalnızca baş yetkili veri koruma otoritesine yapılacak başvuru ile de sürecin tamamlanabilmesine olanak tanımaktadır. Böyle bir durumda her bir yetkili veri koruma otoritesi baş yetkili veri koruma otoritesi ile temasa geçmekte ve yetkili veri koruma otoritelerinin baş yetkili veri koruma otoritesi ile birlikte yapacağı değerlendirme sonucunda mutabık kalınırsa Tüzük m. 56 uyarınca baş yetkili veri koruma otoritesi nihai yetkili merci olarak atanabilmektedir[277]. Fakat baş yetkili veri koruma otoritesi bu durumda dahi kendisine iletilen bağlayıcı şirket kuralları başvurusunu tek başına kabul etmeye yetkin görülmemekte ve Tüzük m. 60 ve m. 63 uyarınca merkez şirket dışındaki diğer grup üyesi şirketlerin bulunduğu AB ülkelerindeki yetkili veri koruma otoriteleriyle iş birliği halinde olması ve tutarlılık mekanizmalarını harekete geçirerek karar verilmesi beklenmektedir[278]. Baş yetkili veri koruma otoritesinin bağlayıcı şirket kurallarının kısmen ya da tamamen uygulanmadığına kanaat getirmesi durumunda vermiş olduğu onay kararını dilediği zamanda geri alma yetkisi bulunmaktadır. Böyle bir durumda ilgili grup üyesi şirketlerce yapılacak sınır ötesi veri aktarımlarının herhangi bir hukuka uygunluk sebebinden yoksun olması halinde hukuka ve Tüzük'e aykırı veri aktarım faaliyeti gerçekleştiği kabul edilebilecek ve bu hukuka aykırılıktan bahisle ilgili grup üyesi şirket için Tüzük'te öngörülen yaptırımların uygulanması gündeme gelebilecektir. Diğer taraftan Tüzük uyarınca AB'den AB dışına yapılacak kişisel veri aktarımlarının Tüzük kapsamındaki koruma mekanizmalarından yararlanması amaçlandığından AB sınırları dışında bulunan grup üyesi şirketlerin kendi ülkelerindeki (üçüncü ülkelerdeki) veri koruma otoritelerinin bağlayıcı şirket kurallarına ilişkin onay kararları aranmamaktadır.

[277] Schröder'e ait kısım, Kühlıng, Buchner, s. 871
[278] Toparlak, s.23

3.2.4.14. Bağlayıcı Şirket Kurallarının İhlali ve Sorumluluk

Tüzük kapsamında veri sorumlusu (kontrolör) ve veri işleyen (işleyici) için öngörülen yükümlülüklere aykırılıklar belirli sorumluluk mekanizmalarıyla birlikte düzenleme altına alınmıştır. Bu sorumluluk mekanizmaları temelinde aykırılığa sebep olan veri sorumlusu veya veri işleyenin idari para cezasına tabi tutulmasıdır. Uygulanacak idari para cezası aykırılığın türüne göre değişiklik göstermektedir. Tüzük uyarınca veri sorumlusu ve veri işleyenlerin veri işleme ilkelerinin, hukuka uygunluk hallerinin, ilgili kişiden alınacak rızaya dair öngörülen yükümlülüklerin ve özel nitelikli kişisel verilere dair düzenlemelerin yer aldığı Tüzük m. 5, m. 6, m. 7 ve m. 9'u ve ilgili kişilerin haklarının düzenlendiği Tüzük m. 12 ila 22'yi ihlal etmesi halinde yetkili veri koruma otoritesi tarafından 20.000.000 EUR'ya kadar ve şayet bir ticari teşebbüs söz konusu ise teşebbüsün global cirosunun %4'üne kadar idari para cezası uygulanabileceği öngörülmüştür. Bununla birlikte bağlayıcı şirket kuralları da dahil olmak üzere Tüzük m. 44 ila m. 49 arasındaki üçüncü ülkelere kişisel veri aktarımı için öngörülen yükümlülüklerden birine aykırılı davranılması halinde ise yine yetkili veri koruma otoritesi tarafından 20.000.000 EUR'ya kadar ve şayet bir ticari teşebbüs söz konusu ise bu teşebbüsün global cirosunun %4'üne kadar idari para cezasına hükmedilebileceği düzenlenmiştir. Bu hüküm uyarınca bağlayıcı şirket kurallarının ihlal edilmesi diğer bir deyişle bağlayıcı şirket kuralları uyarınca öngörülen yükümlülüklerin ve verilen taahhütlerin eksik veya gereğine uygun olmayan bir şekilde yerine getirilmiş olması ya da hiçbir şekilde yerine getirilmemiş olması halinde aykırılığa sebep olan grup üyesi şirketin AB sınırları içerisinde bulunsun ya da bulunmasın sorumluluğu gündeme gelecektir.[279]

Söz konusu sorumluluk hali bağlayıcı şirket kuralları ile birlikte sınır ötesi kişisel veri aktarımları için uygulama alanı bulan Tüzük'teki veri işleme ilkelerine, hukuka uygunluk sebeplerine ve diğer hükümlere aykırı davranılması halinde de gündeme gelecektir[280]. Öyle ki bağlayıcı şirket kurallarına taraf olunması ile birlikte ilgili

[279] Toparlak, s.56
[280] Zerdick'e ait kısım, Ehmann, Selmayr, s. 696.

grup üyesi şirketler Tüzük'teki bağlayıcı şirket kurallarının uygulanmasına dayanak teşkil edebilecek diğer temel veri koruma hükümlerine uygun hareket etme taahhüdü altına girmektedir. Örneğin bağlayıcı şirket kuralları uyarınca kendisine veri aktarımında bulunan AB dışında kurulu grup üyesi şirketin bu verileri üçüncü bir alıcıya iletmesi halinde Tüzük'teki ve bağlayıcı şirket kurallarındaki hükümlere riayet etmesi gerekmektedir. Bu kapsamda Tüzük uyarınca hazırlanan bağlayıcı şirkete taraf olan Türkiye'de kurulu bir grup üyesi şirket de bağlayıcı şirket kuralları uyarınca kendisine aktarılan kişisel verileri üçüncü kişilere aktarırken KVKK'nın yanı sıra bağlayıcı şirket kurallarını ve Tüzük hükümlerini de gözeterek hareket etmelidir. Bu sebeple üçüncü bir ülkede kurulu grup üyesi şirketin bağlayıcı şirket kurallarına taraf olmakla birlikte Tüzük kapsamındaki yükümlülüklerini de ayrıntılı bir şekilde araştırması gerekmektedir. Ayrılığa AB dışındaki grup üyesi şirketin sebep olması halinde ilgili grup üyesi şirketin yanı sıra bağlayıcı şirket kuralları uyarınca bu kuralları taahhüt eden AB sınırları içerisinde kurulu olan grup üyesi şirketin de bu aykırılıktan ilgili grup üyesi şirket ile birlikte sorumluluğu gündeme gelmektedir. Bu sebeple AB sınırları dışındaki grup üyesi şirketlerinde AB'den AB sınırları dışına yönelik gerçekleşen veri aktarımları için taraf oldukları bağlayıcı şirket kurallarına tam anlamıyla itibar etmesi büyük önem arz etmektedir. Aksi halde AB sınırları dışındaki grup üyesi şirketin sebep olduğu aykırılıktan dolayı bu kuralları taahhüt eden AB sınırları içerisindeki grup üyesi şirket için de kendi ülkesinde yetkili veri koruma otoritesi tarafından idari para cezasına hükmedilebilecektir.

Tüzük m. 83 uyarınca yetkili veri koruma otoritesi tarafından idari para cezası kararı verilirken bu ceza tutarı aykırılığa sebep olan grup üyesi şirketlerin ilgili kişilerin zararını azaltmak için herhangi bir telafi çalışması yapıp yapmadığı, yaptıysa bu çalışmanın ne derece etkili olduğu, daha önce aykırılığa sebep olan konuya ilişkin yetkili veri koruma otoritesi uyarınca ilgili grup şirketin ikaz edilip edilmediği ve genel olarak aykırılığın ortaya çıktığı veri işleme faaliyeti için ilgili grup üyesi şirketlerce gerekli veri güvenliği tedbirlerinin alınıp alınmadığı göz

önünde bulundurulmaktadır[281]. Bu noktada sınır ötesi veri aktarım faaliyetlerine yönelik olarak veri güvenliğinin sağlanması adına uygun bir güvenlik tedbiri olarak gereğine uygun bir şekilde düzenlenen ve onaylanmış bir bağlayıcı şirket kurallarının varlığı yetkili veri koruma otoritesi tarafından verilecek idari para cezası tutarında ilgili grup üyesi şirketin lehine bir etki doğuracaktır. Öyle ki Tüzük hükümleriyle uyumlu olarak hazırlanan ve grup üyeleri tarafından sürekli olarak uygulamaya konulan bağlayıcı şirket kuralları çoğu zaman ilgili grup üyesi şirketlerin kusur oranlarının azalmasına ve sorumluluk kapsamlarının daralmasına sebep olabilecektir. Diğer taraftan AB sınırları dışında kurulu olan grup üyesi şirketin bağlayıcı şirket kurallarını ihlal edilmesinde bu kuralları taahhüt eden ve sorumluluğu üstlenen AB'de kurulu grup üyesi şirketin hiçbir şekilde kusuru bulunmuyorsa müşterek sorumluluk gündeme gelmeyecek ve ilgili grup üyesi şirket tek başına söz konusu aykırılıktan dolayı sorumlu olacaktır. Öte yandan AB sınırları dışında bulunan grup üyesi şirketten söz konusu idari para cezasının ne şekilde tahsil edileceği ayrı bir sorun teşkil etmektedir.

Bağlayıcı şirket kurallarını ihlal eden üçüncü ülkedeki grup üyesi şirketin sorumluluğu belirli durumlarda bağlayıcı şirket kuralları kapsamında AB'de kurulu grup üyesi şirket tarafından üstlenilse de bu durum üçüncü ülkedeki grup üyesi şirketin sorumluluğunu ortadan kaldırmaz[282]. Öyle ki bu durumda üçüncü ülkedeki grup üyesi şirketin bağlayıcı şirket kurallarını ihlal etmesi ile birlikte kendi iç hukukundan doğan kişisel veri yükümlülüklerini de ihlal etmiş olması söz konusu olabilecektir. Örneğin bağlayıcı şirket kurallarının büyük oranda KVKK hükümleri ile de paralel olduğu göz önünde bulundurulduğunda bağlayıcı şirket kurallarına aykırı olarak veri aktarımı gerçekleştiren Türkiye'de kurulu grup üyesi şirketin KVKK uyarınca da sorumluluğu gündeme gelebilecektir. Böyle bir durumda Kurul, aydınlatma yükümlülüğüne, veri güvenliği tedbirlerine ya da KVKK'da anılan diğer sebeplerden birine aykırı davranan Türkiye'de kurulu grup üyesi şirket için

[281] Toparlak, s.64.
[282] Golla'ya ait kısım, AUERNHAMMER Herbert, Datenschutz-Grundverordnung Bundesdatenschutzgesetz und Nebengesätze Kommentar, 7. Auflage, Carl Heymanns Verlag, Köln, Almanya 2020, s. 1210.

KVKK m. 17 ve m.18'de öngörülen yaptırımlara hükmedebilecektir. Diğer taraftan Türkiye'de kurulu olmasa dahi bağlayıcı şirket kurallarına tabi olan ve Türkiye'deki ilgili kişilere yönelik veri işleme faaliyeti gerçekleştiren AB'deki ya da üçüncü bir ülkedeki grup üyesi şirketin KVKK'ya aykırı hareket etmesi halinde de Kurul söz konusu yaptırımlardan birine hükmedebilecektir. KVKK uyarınca sorumluluğun ancak bir hukuki kişiliği bulunan yapılara atfedileceği göz önüne alındığında bağlayıcı şirket kurallarına taraf olan topluluk üyelerinin Türkiye'deki üyelerinin bir şirket yerine şube olarak karşımıza çıktığı durumlarda söz konusu şubenin de KVKK'ya aykırı hareket etmesi halinde sorumluluğu gündeme gelebilecektir. Öyle ki Kurul Çalışmamızın ikinci bölümünde de belirttiğimiz gibi 23/07/2019 tarih ve 2019/225 sayılı kararında şubelerin de merkezleri yurt dışında bulunsa da Türkiye'de gösterdikleri veri işleme faaliyeti uyarınca belirli durumlarda veri sorumlusu olarak kabul edileceğini belirtmek ve yabancı veya Türk ya da şirket veya şube olsun Türkiye'de veri işleme faaliyeti gerçekleştiren yapıların KVKK'ya ve KVKK'daki yaptırımlara tabi olacağının altını çizmektedir. Şu kadar ki taraf olduğu bağlayıcı şirket kurallarına rağmen KVKK hükümlerine ve iç hukuk düzenlemelerine aykırı olarak yurt dışındaki diğer bir grup üyesine yönelik veri aktarım faaliyeti gerçekleştiren Türkiye'de kurulu grup üyesi şirketin bu sebeple ortaya çıkan aykırılıklardan dolayı da sorumlu olmaya devam edeceği unutulmamalıdır. Böyle bir durumda Türkiye'deki grup üyesi şirket KVKK uyarınca sorumlu olabileceği gibi bu şirketin KVKK dışında TBK, TTK, elektronik ticaret mevzuatı, iş mevzuatı vb. gibi Türk hukukundaki farklı mevzuat hükümlerine göre de sorumluğu doğabilecektir. Bu durum bağlayıcı şirket kuralları hazırlanırken bu kuralların grup üyesi şirketlerin iç hukuk düzenlemeleriyle uyumlu hareket edilmesi gerekliliğini de bir kere daha ortaya koymaktadır.

3.2.5. Türk Hukukunda Bağlayıcı Şirket Kuralları

Çalışmamızın üçüncü bölümünün başında belirttiğimiz üzere bağlayıcı şirket kuralları Türk hukukuna Kurum'un 10 Nisan 2020 tarihli duyurusu ile getirilmiştir. Bu duyuruyla bağlayıcı şirket kurallarının tanımı ve uygulama alanına ilişkin

açıklamalar ve bu kuralların hazırlanması ve Kurum'a başvuru süresince veri sorumlularına yardımcı olacak ek belgeler yayımlanmıştır. Duyuruda yer alan bu düzenlemeler dışında bağlayıcı şirket kuralları henüz KVKK ve alt mevzuat hükümlerinde düzenleme alanı bulmamıştır. Kurum bağlayıcı şirket kuralları uygulamasını Tüzük hükümlerinden hareketle Türk hukukuna dahil etmiştir[283] ve bağlayıcı şirket kurallarını taahhütnamelerin alternatifi olarak yurt dışına veri aktarımında kullanılabilecek bir güvenlik tedbiri olarak tanımlamıştır[284]. Buna karşılık Kurum Tüzük'ten farklı olarak bağlayıcı şirket kurallarının yalnızca veri sorumluları tarafından kullanılabilecek bir veri aktarım mekanizması olduğunu açıklamıştır. Bu sebeple veri işleyenlerin bağlayıcı şirket kurallarını kullanarak yurt dışına veri aktarımı Türk hukuku uyarınca henüz mümkün görünmemektedir. Ancak KVKK'nın hazırlığa ve yürürlüğe girmesi sırasında Direktif hükümlerinden faydalanılırken Kurul'un bağlayıcı şirket kuralları ile Tüzük hükümlerini örnek alması kişisel verilerin korunması alanında Türk hukukunda atılan önemli adımlardan biri olarak görülebilecektir. Bu anlamda bağlayıcı şirket kurallarının kabulü ile Türk veri koruma hukukunun AB veri koruma hukukuna uyum sağlaması yolunda da önemli bir adım atılmış olmaktadır[285].

Bağlayıcı şirket kurallarına ilişkin duyurusunda Kurum, taahhütnamelerin yalnızca iki taraflı veri aktarımlarımda kullanılabildiğini ve bu mekanizmanın çok uluslu şirket toplulukları için uygulama pratiğini sağlamakta yetersiz kalabildiğini ifade etmiştir. Bu noktada bağlayıcı şirket kuralları çok uluslu grup şirketler arasındaki uluslararası veri aktarımlarında kullanılabilecek temel veri aktarım yöntemlerinden biri olarak karşımıza çıkmaktadır. Söz konusu duyuruda bağlayıcı şirket kurallarına ilişkin yayımlanan belgeler arasında bağlayıcı şirket kuralları "Bir şirketler topluluğuna bağlı olarak Türkiye'de yerleşik bir veri sorumlusu tarafından, bu

[283] Dülger, KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, s.4
[284]Bağlayıcı Şirket Kuralları Hakkında Duyuru https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINAKISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU Erişim Tarihi: 20.01.2022.
[285] [285] Dülger, KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, s.5

şirketler topluluğuna bağlı olarak yurt dışında bir veya daha fazla ülkede faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularına yapılacak olan kişisel veri aktarımları veya aktarım setlerinde uyulması gereken kişisel veri koruma kuralları" olarak tanımlanmıştır. Bu tanımdan hareketle bağlayıcı şirket kurallarının Türkiye'de kurulu bir veri sorumlusu tarafından yine yurt dışında bulunan ve aynı grup içerisinde yer alan farklı bir veri sorumlusuna yapılacak aktarımlarda kullanılabileceği sonucu çıkarılmaktadır. Görüldüğü üzere Türk hukukuna tabi şirketlerce hazırlanacak bağlayıcı şirket kuralları taahhütnamelerden farklı olarak yalnızca veri sorumluları arasındaki veri aktarımları için kullanılabilmektedir. Bu durum bağlayıcı şirket kurallarının uygulama alanının daralmasına ve uygulamada veri işleyen olarak da faaliyet gösterebilmekte olan grup üyesi şirketlere yapılabilecek aktarımlarda bağlayıcı şirket kurallarının uygulama alanı bulamamasına yol açmaktadır. Diğer taraftan bu tanım ile birlikte bağlayıcı şirket kurallarının çok uluslu grup şirketlerin yanı sıra ortak bir karar alma mekanizması bulunan ya da ekonomik faaliyet gösteren veri sorumluları tarafından ve teşebbüslerce de yurt dışına yapılacak veri aktarımlarında uygulanabileceği anlaşılmaktadır. Bu durum veri işleyenlere yönelik aktarımlar için bağlayıcı şirket kuralları kullanılamayacaksa da yalnızca şirket olarak yapılanma göstermeyen ve fakat ekonomik veya yönetsel bir iş birliği içerisinde olan yapıların da veri sorumlusu sıfatıyla gerçekleştirdikleri yurt dışına veri aktarım faaliyetlerinde bağlayıcı şirket kurallarına başvurulabilmelerine imkân tanımaktadır. Bununla birlikte Türk hukuku uyarınca hazırlanacak bağlayıcı şirket kurallarının özellikle merkezi Türkiye'de bulunan şirketler topluluğu tarafından düzenleme altına alınacağını belirtmek yanlış olmayacaktır.

Bağlayıcı şirket kuralları ile Kanun'un yurt dışına kişisel veri aktarımı için aradığı yeterli koruma tesis edilmektedir. KVKK m.9 uyarınca yeterli korumanın bulunmadığı ülkelere yapılacak veri aktarımlarında başvurulan bağlayıcı şirket kuralları içerdiği taahhütler ile birlikte aktarıma tabi tutulan kişisel verilerin KVKK uyarınca öngörülen koruma ve gizlilik düzeyine tabi olmasını sağlamaktadır. Buna

karşılık ne yazık ki Kurul'un onay verdiği ve bu sayede uygulamaya konulan herhangi bir bağlayıcı şirket kuralları örneği olduğu henüz bilinmemektedir. Bu kapsamda bağlayıcı şirket kurallarının Türk hukukunda gelişim kazanması çok uluslu grup şirketlerin yurt dışına veri aktarımında bulunurken bu yola başvurması ve özellikle Kurul'un bu alanda vereceği onay kararlarında bir artış yaşanması için büyük bir önem arz etmektedir[286]. Öyle ki bağlayıcı şirket kurallarının henüz mevzuat düzeyinde bir düzenleme ile hüküm altına alınmamış olması bu kuralların uygulama alanına yönelik belirli soru işaretlerini de beraberinde getirmektedir. Örneğin KVKK uyarınca öngörülen yaptırımlara bakıldığında bağlayıcı şirket kurallarına tabi olan şirketlerin herhangi bir hukuka aykırılık ortaya çıkmamış olsa da yalnızca bu kurallarda belirtilen taahhütlere aykırı davranması halinde ne tür bir yaptırım ile karşılaşacağı henüz bilinmemektedir. Dolayısıyla bağlayıcı şirket kuralları uygulamalarının hukuka uygun bir zeminde yürütülebilmesi adına bu alanda kanuni düzenlemelere yer verilmesi büyük bir ihtiyaç olarak karşımıza çıkmaktadır.

Bağlayıcı şirket kurallarının sağlıklı bir şekilde uygulamaya konması yurt dışına veri aktarımının ilgili kişinin açık rızanın alınması gibi her an ilgili kişi tarafından geri alınabilir bir beyana ya da taahhütnameler gibi yalnızca iki taraflı veri aktarımlarında kullanılan mekanizmalara bırakılmaması ve veri aktarımlarına bağlı olarak gerçekleştirilebilecek ticari faaliyetlere ivme kazandırılmasında da önemli bir rol oynamaktadır. Yurt dışına kişisel veri aktarımlarında hukuka uygun bir alternatif mekanizma olarak kullanılacak bağlayıcı şirket kuralları, Türkiye'ye yabancı sermayenin çekilmesinde ve yapılacak yatırımların artış göstermesinde de dolaylı olarak olumlu etki gösterecektir. Diğer taraftan bu kurallar ile tıpkı Tüzük uyarınca hazırlanan ve uygulamaya konan bağlayıcı şirket kuralları gibi grup üyesi şirketler arasında standart ve uluslararası uygulanabilirliği olan kişisel veri işleme ve aktarım politikası hazırlanmış olmakta ve bu kurallara tabi olan her bir grup üyesi şirket için olası veri ihlallerinin ortaya çıkmasını engellemeye ve kişisel veri

[286] Dülger, KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, s.6

mevzuatına uyum sağlanmasına yönelik çeşitli veri koruma tedbirlerinin önceden şirket bünyesinde tesis edilmesine imkan tanınmaktadır. Bununla birlikte bağlayıcı şirket kurallarının Türkiye'de kurulu veri sorumlusu grup üyesi şirketler tarafından kabul edilmesi ile birlikte şirketler KVKK ve alt mevzuat hükümlerinde yer alan yükümlülüklerini yazılı bir metin altında taahhüt etmekte ve bu durum şirketlerin hesap verilebilir ve şeffaf bir veri koruma düzenine geçişi sağlamalarında önemli bir rol oynamaktadır.

KVKK ve alt mevzuat hükümleri tahtında kişisel verilerin korunması mevzuatına uyum sağlanması konusunda taşıdığı önem göz önünde bulundurulduğunda Türk hukuku uyarınca hazırlanacak bağlayıcı şirket kuralları ile başta Türkiye'de kurulu veri sorumlusu grup üyesi şirket olmak üzere bu kurallara tabi olan grup şirketlerce üstlenilen yükümlülüklerin ve verilen taahhütlerin incelenmesi faydalı olacaktır. Gereğine uygun bir şekilde hazırlanan bağlayıcı şirket kuralları, bu kurallardaki taahhütleri tevsik eden ek belgeler ve Kurum tarafından Çalışmamızın bu bölümün belirteceğimiz çeşitli taahhütleri içeren başvuru formunun Kurul'a ibraz edilmesi ile Kurul'un değerlendirmesine sunulur ve ancak Kurum talimatlarına uygun bir şekilde gerekli taahhütleri içerecek şekilde hazırlanan ve Kurul tarafından onaylanan bağlayıcı şirket kuralları geçerli bir şekilde uygulama alanı bulur. Bu sebeple Çalışmamızın bu bölümünde Kurum'un bağlayıcı şirket kurallarına ilişkin yayımladığı duyurusunun ekinde yer alan yardımcı belgeler ile ortaya koyduğu söz konusu yükümlülükler ve taahhütler incelenecektir. Bu kapsamda Kurum tarafından bağlayıcı şirket kurallarında bulunması gereken sekiz temel unsur olduğu açıklanmıştır. Bunlar sırasıyla bağlayıcılık unsuru, etkili uygulama, Kurum ile koordinasyon, kişisel verilerin işlenmesi ve aktarılması, raporlama ve kayıt değişikliği mekanizmaları, veri güvenliği, hesap verebilirlik ve diğer araçlar ile yardımcı bilgi ve belgelerdir. Bu unsurlardan bazılarının bağlayıcı şirket kurallarında bazılarının ise bağlayıcı şirket kuralları ile Kurul'a ibraz edilecek başvuru formunda taahhüt edilmesi zorunlu tutulmuştur. Kurul tarafından başvurunun olumlu sonuçlanması için başvuruda bulunan grup üyesi şirketin söz konusu unsurların başvuru formunda ve bağlayıcılık unsurunda gereğine uygun bir

şekilde taahhüt edildiğinden emin olması gerekmektedir. Şu kadar ki bu yükümlülükleri ve taahhütleri içerecek şekilde Türkiye'de merkezi bulunan bir şirketler topluluğu tarafından Türk hukuku uyarınca bağlayıcı şirket kuralları hazırlanabileceği gibi halihazırda Tüzük uyarınca hazırlanan ve yetkili otorite tarafından onaylanmış bağlayıcı şirket kuralları da Türkçe'ye çevrilerek Kurul'a yapılacak başvurularda kullanılabilecektir. Bu durumda aynı bağlayıcı şirket kuralları üzerinden hem Türkiye'den AB'ye hem de AB'den Türkiye'ye geçerli bir şekilde veri aktarımları yapılabilecektir. Ayrıca bu durum Tüzük ve KVKK mevzuatlarının bir sentez olarak uygulama alanı bulmasına imkân tanıyarak kişisel verilerin korunmasına ilişkin Türk hukuku düzenlemelerinin AB hukukuyla uyum sürecini de hızlandırmaktadır. Ancak AB hukuka uygun olarak hazırlanan bağlayıcı şirket kurallarının Türkçe'ye tercüme edilerek Kurum'a sunulmasından önce söz konusu bağlayıcı şirket kurallarının KVKK ve alt mevzuat hükümleri ile aşağıda belirtmiş olduğumuz Kurum'un duyurusunda ifade edilen unsurlar ile uyumlu olup olmadığının teyit edilmesi ve uyumlu olmadığı tespit edilen noktalarda bu kurallar için gerekli düzenlemelerin yapılması gerektiği de unutulmamalıdır.

3.2.5.1. Bağlayıcılık Unsuru

Türk Hukukunda bağlayıcı şirket kurallarının ilk unsuru bağlayıcılıktır. Bağlayıcı şirket kurallarında bağlayıcılık unsuru tıpkı Tüzük'te olduğu gibi iç bağlayıcılık ve dış bağlayıcılık olarak ikiye ayrılır. İç bağlayıcılık bu kuralları hazırlayan grup üyesi her bir şirketin ve bu şirketlerin çalışanlarının söz konusu kurallara tabi olması anlamına gelir. İç bağlayıcılığın sağlanması adına bağlayıcı şirket kurallarına tabi olan şirketlerin bu kurallardan doğan yükümlülüklerini yerine getireceklerini ve bu kurallara uyacaklarını açık bir şekilde hem bağlayıcı şirket kuralları metninde hem de başvuru formunda açık bir şekilde taahhüt altına alması gerekmektedir. Bu taahhütleriyle birlikte her bir grup üyesi şirketin kendi çalışanlarının da bu kurallara uygun davranmasını sağlayacak talimatları bu kurallar ile birlikte belirtmesi beklenmektedir. Çalışanların bu kurallara itibar etmesi için alınacak tedbirlerden her biri iç bağlayıcılığın sağlanması adına önem arz eder.

Kurum yayımladığı duyuruda ve bu duyurunun ekinde yer alan yardımcı belgelerde iç bağlayıcılık ve dış bağlayıcılık kavramlarını tanımlamasa da bu kavramların sağlanması adına her bir grup üyesi şirket tarafından bağlayıcı şirket kuralları ile birlikte alınabilecek tedbirlerin neler olduğuna örnekler vermiştir. Bu kapsamda iç bağlayıcılığın her bir şirketçe sağlanması adına her bir grup üyesi şirketin bu kurallara açık bir şekilde uyacağının ve aksi halde bu kurallara aykırılık halinde tabi olacakları topluluk içi yaptırımların belirlenmesi büyük önem arz etmektedir. Bununla birlikte grup üyesi şirketlerin çalışanları ile aralarındaki iş sözleşmesinde, gizlilik sözleşmelerinde ve/veya diğer anlaşmalarında bu kurallara çalışanlarca itibar edilmesini sağlamak adına gerekli hükümlere yer vermesi, şirket içerisinde çalışanların tabi olacağı veri politikaları ve prosedürleri ile etik kuralları oluşturması ve yayımlaması, iş yeri ve disiplin yönetmeliklerinde bağlayıcı şirket kurallarına aykırı davranışların da yaptırıma tabi olacağı düzenlemelere yer verilmesi bu kapsamda işveren sıfatıyla her bir grup üyesi şirket tarafından alınabilecek tedbirler arasında yer almaktadır. Grup üyesi şirketler bakımından söz konusu tedbirlerin her biri bağlayıcı şirket kuralları dahilinde belirtilmese de başvuru formunda açık ve Kurul'u ikna edecek bir şekilde ifade edilmelidir.

İç bağlayıcılığın yanı sıra dış bağlayıcılık unsuru ise yine Tüzük'te de belirtildiği gibi bağlayıcı şirket kurallarının üçüncü kişiler üzerinde bağlayıcı etki doğurmasını ifade etmektedir[287]. Dış bağlayıcılığın sağlanması adına her bir grup üyesi şirket üçüncü kişiler üzerinde bu kuralların etkin bir şekilde uygulama alanı bulması için gerekli taahhütlere yer vermeli ve mekanizmaları oluşturmalı ve bu taahhütler ile mekanizmaların neler olduğuna hem bağlayıcı şirket kurallarında hem de başvuru formunda yer verilmelidir. Bu kapsamda üçüncü kişilerin başında ilgili kişiler ve grup içi aktarıma tabi olan kişisel verileri işleyen veri sorumlusu ve veri işleyenler gelmektedir. İlgili kişiler bağlayıcı şirket kuralları uyarınca kişisel verileri Türkiye'den yurt dışına aktarılan ilgili kişileri ifade eder. Bağlayıcı şirket kurallarında her bir grup şirketçe ilgili kişilerin aktarıma tabi tutulan kişisel verileri

[287] WP 256, WP 257.

üzerinde KVKK m. 11'den doğan haklarını hızlı ve kolay bir şekilde kullanabilmeleri ve KVKK m. 13 uyarınca veri sorumlusu şirkete başvurulabilmesi için gerekli tedbirlerin alındığının taahhüt edilmesi beklenmektedir. Bu kapsamda bağlayıcı şirket kuralları nezdinde ilgili kişilere tanınan hakların açıkça tanımlanması ve hatta bağlayıcı şirket kurallarında bir aydınlatma metninde bulunması gereken ve ilgili kişinin bilgisine sunulabilecek gerekli açıklamalara yer verilmesi, bağlayıcı şirket kurallarının grup üyesi şirketlerin kendi internet siteleri gibi ilgili kişilerin kolaylıkla erişebileceği platformlarda paylaşılması, veri sorumlusuna yapılan başvurudan yeterli faydanın alınamaması halinde Kurum'a ve/veya yetkili mahkemelere başvuru hakkının bulunduğunun belirtilmesi ve kişisel verisinin aktarıldığı ülkede, bağlayıcı şirket kurallarına uymayı engelleyen ulusal bir mevzuatın bulunup bulunmadığı ve bulunması halinde bunun açıkça belirtilmesini talep hakkı olduğuna yer verilmesi verilebilecek dış bağlayıcılık taahhütleri arasında yer alabilir. Bağlayıcı şirket kurallarına tabi olan grup üyesi şirketlerin dış bağlayıcılığı unsurunu temin etmek adına alabilecekleri önlemlerden bir diğeri de grup içi aktarımlara tabi olan kişisel verileri işleyen üçüncü kişi veri sorumlusu ve veri işleyenler ile aralarındaki sözleşmelerinde bu verilerin korunmasına dair bağlayıcı şirket kuralları ile paralel veri güvenliği hükümlerine yer vermeleri ya da bu sözleşmelere ek protokoller akdederek bu kuralların getirdiği standartları tesis etmeye çalışmalarıdır[288].

Tüzük ile uyumlu olarak gerek bağlayıcı şirket kurallarında gerekse başvuru formunda topluluğun Türkiye'de bulunan ve merkez görevini yürüten grup üyesi şirketinin ya da kişisel verilerin korunması konusunda topluluk içinde yetkilendirilmiş Türkiye'deki grup üye şirketin veyahut Türkiye'den yurt dışına kişisel veri aktarımında bulunan Türkiye'deki grup üyesi şirketin veri sorumlusu sıfatıyla bu kurallara aykırı davranılmasından kaynaklı olarak ortaya çıkacak ihlallere karşı tazminat ödemesi ve ihlallerin giderilmesi gibi yükümlülükleri üstlenmesi ve kabul etmesi beklenmektedir. Sorumluluğun üstlenmesi konusunda

[288] WP 204.rev01

bağlayıcı şirket kuralları ve başvuru formunda yapılan düzenlemeler ve verilecek taahhütler bağlayıcılık unsurunun temin edilmesi adına büyük bir öneme sahiptir. Öyle ki bu sayede bağlayıcı şirket kuralları uyarınca yurt dışına aktarılan kişisel verilere yönelik herhangi bir ihlal meydana gelmesi halinde Kurum, Türkiye'de kurulu bulunan grup üyesi şirketlerden birine doğrudan başvurabilecek ve zararların giderilmesini sağlamak adına gerekli yaptırımları uygulayabilecektir. Bu kapsamda Kurum tarafından yayımlanan bağlayıcı şirket kurallarına ilişkin duyurunun ekindeki yardımcı belgede de Türkiye dışında bulunan ve bağlayıcı şirket kurallarına tabi olan diğer grup üyesi şirketlerden birinin sebep olduğu zararın Türkiye'deki bir grup üyesi şirketçe üstlenilmesi gerektiği ve bağlayıcı şirket kurallarının uygulanmasından kaynaklı olarak ortaya çıkabilecek ihlallerde yetkinin Türkiye'deki mahkemeler ve yetkili makamlarda olacağının açıkça belirtilmesi gerektiği vurgulanmaktadır. Burada Kurum tarafından amaçlanan esasında ihlale maruz kalan ilgili kişinin, ihlal yurt dışında değil de sanki Türkiye'de gerçekleşmiş gibi sorumluluk ve yükümlülüğü kabul etmiş olan Türkiye'deki grup üyesi şirkete karşı hak ve tazminatlarını talep etme yetkisine sahip olmasıdır.

Sorumluluğun Türkiye'deki grup üyesi şirket tarafından üstlenilmesinin mümkün olmaması halinde Kurum, Türkiye dışındaki diğer grup üyesi şirketlerce gerçekleştirilebilecek ihlallerden kaynaklı olarak kendisine Türkiye'den doğrudan veri aktarımının yapıldığı ve bağlayıcı şirket kurallarına tabi olan diğer tüm grup üyesi şirketlerin birlikte sorumlu kabul edilmesini de uygun bulmaktadır. Bu düzenleme uyarınca ilgili grup üyesi şirketler arasında bir birlikte sorumluluk düzeni oluşmasını zorunlu kılan Kurum, ilgili kişiye bu grup şirketlerden herhangi birine söz konusu ihlalin giderilmesi için başvurulabilme imkânı tanımaktadır. Söz konusu sorumluluğun üstlenilmesiyle bağlantılı olarak Kurum, Türkiye dışında bulunan grup üyesi şirketlerin bağlayıcı şirket kurallarının ihlal edilmesinden doğan sorumluluğu üstlenen her bir grup üyesi şirketin bu ihlallerden kaynaklı zararların tazmin edilebilmesi için yeterli malvarlığına sahip olduğunu da başvuru formunda taahhüt etmesi gerektiğini belirtmektedir. Bu kapsamda grup üyesi şirketlerce

sermayelerini ve/veya malvarlıklarında bulunan ticari işletmeleri, gayrimenkulleri ve diğer unsurları gösteren tevsik edici belgeleri de Kurul'a başvururken sunacakları başvuru formunun ekinde bulundurması faydalı olacaktır. Diğer taraftan Kurum tarafından sorumluluğu üstlenen grup üyesi şirketlerin ilgili kişi tarafından herhangi bir zararın tazmini talebinde bulunulduğunda, bu zararın zarara sebep olduğu iddia edilen yurt dışındaki grup üyesi şirketten kaynaklanıp kaynaklanmadığını ispat etmeleri ve ispat külfetinin açık bir şekilde kendi üzerlerinde olduğunu hem bağlayıcı şirket kurallarında hem de başvuru metninde taahhüt etmeleri gerektiği beklenmektedir. Buna göre sorumluluğu üstlenen grup üyesi şirketin zararın yurt dışındaki üyenin zarara yol açacak olayda sorumluluğu olmadığını ispat etmesi halinde sorumluluktan kurtulacağı kabul edilmektedir[289].

3.2.5.2. Etkili Uygulama Unsuru

Bağlayıcı şirket kurallarının bu kurallara tabi olan grup üyesi şirketler için bağlayıcı bir etki doğurabilmesi ve geçerliliği bir şekilde uygulama alanı bulması için etkili uygulama unsurunu taşıması gerekmektedir. Kurum bağlayıcı şirket kurallarına ilişkin duyurusunun ekinde yayımladığı yardımcı belgede bağlayıcı şirket kurallarının etkili uygulamasını sağlayabilmek adına veri sorumlusu grup üyesi şirketlerin yerine getirmesi gereken belirli yükümlülükler olduğunu belirtmektedir. Bu yükümlülükler grup üyesi şirketlerce bağlayıcı şirket kurallarına ilişkin çalışanlarına farkındalık eğitimleri verilmesi, ilgili kişilerce veri sorumlusuna şikayet başvurularının yapılabilmesi için gerekli mekanizmaların oluşturulması, grup üyesi şirketlerin bağlayıcı şirket kurallarına uyum sürecinin sürekli ve düzenli bir şekilde denetime tabi tutulması ve etkili uygulamanın sağlanabilmesi için anılan söz konusu yükümlülüklerin organizasyonunun yürütülebilmesi amacıyla topluluk dahilinde görevli bir personel atanması şeklindedir. Görüldüğü üzere Kurum, Tüzük'te bağlayıcı şirket kurallarının etkin bir şekilde uygulama alanı bulması için öngörülen yükümlülükler ile benzer bir anlayış benimsemiş ve bu unsurların gerek

[289] WP 152, WP 74, WP 108.

bağlayıcı şirket kuralları gerekse başvuru formunda açık bir şekilde taahhüt edilmesi gerektiğini belirtmiştir.

Etkili uygulama yöntemlerinden ilki olan farkındalık eğitimleri kişisel verilere erişim sağlayan ve veri işleme ve aktarım faaliyetlerine dahil olan personellere yönelik olarak verilmeli ve bu eğitimlere ilişkin programlar açık bir şekilde başvuru formunda ve bağlayıcı şirket kurallarında belirtilmelidir. Bu kapsamda veri sorumlusu sıfatıyla bağlayıcı şirket kurallarına taraf olan grup üyesi şirketlerin başvuru formlarının ekinde söz konusu eğitimlere ait plan ve programları Kurul'a sunması bu eğitimlerin grup üyesi şirketler tarafından ciddiye alındığına dair Kurul'un ikna olması ve başvurunun olumlu bir şekilde sonuçlanması adına faydalı olabilir. Ayrıca Kurum bağlayıcı şirket kurallarına onay vermiş olsa dahi bu kuralların uygulanması esnasında kurallar nezdinde taahhüt edilen eğitimlere dair kayıtların incelenmek üzere kendisine sunulmasını da talep edebilecektir. Personellerine gerekli eğitimleri vermediğinden bahisle yeterli veri güvenliği tedbirlerinin alınmadığı sonucuna varan ve bu sebeple veri sorumlusuna 450.000 TL idari para cezasının hükmedildiği Kurul'un 20/04/2021 tarihli kararından da görülebileceği üzere Kurul tarafından farkındalık eğitimlerinin verilmesi mevzuata uyum sağlanması bakımından da büyük bir önem arz etmektedir. Bu kapsamda bağlayıcı şirket kuralları hazırlayan ve bu kurallara taraf olan grup üyesi şirketlerce de bu alanda gerekli çalışmaların yürütülmesi gerekmektedir.

Farkındalık eğitimlerinin yanı sıra bağlayıcı şirket kuralları ile kişisel verileri yurt dışına aktarılan ilgili kişilerin grup üyesi şirketlere başvuruda bulunarak KVKK'dan doğan ilgili kişi haklarını kullanabilmesi için öngörülen şikâyet yönetim sürecinin bağlayıcı şirket kurallarında ve başvuru formunda açık bir şekilde düzenlenmiş olması gerekmektedir. Oluşturulacak şikâyet yönetim süresi uyarınca söz konusu yasal hakların ilgili kişi tarafından ilgili veri işleme ve aktarım sürecine dahil olan herhangi bir grup üyesi şirkete yönelik kullanılabiliyor olması beklenmektedir. Şikâyet kapsamında ilgili kişilerin başvuruları ve talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırılmalıdır.

Bununla birlikte söz konusu şikâyet ve başvuru sistemi oluşturulurken KVKK m.13 ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[290]'de yer alan hükümlerin de gözetilmesi gerektiği unutulmamalıdır. Grup üyesi şirketler tarafından Kurul'a sunulacak başvuru formunda, söz konusu şikâyet yönetim sürecine ilişkin ilgili kişilerin ne şekilde bilgilendirileceğinin açıklanması beklenmektedir. Kurum, bağlayıcı şirket kurallarına ilişkin yayımladığı duyurunun ekindeki yardımcı belgede bu kapsamda başvuru formunda özellikle aşağıdaki konularda gerekli bilgilendirmenin sağlanması gerektiğini belirtmektedir:

- Başvurunun hangi grup şirketlere ve kanallar ile yapılacağı,
- Başvurunun azami olarak ne kadar süre içerisinde cevaplanacağı ve cevabın başvurana ne şekilde iletileceği,
- Cevabın hangi şartlarda gecikebileceği ve bu gecikmeyle ilgili durumlar,
- Başvurunun reddedilmesi halinde meydana gelecek sonuçlar,
- Başvuru haklı bulunduğunda meydana gelecek sonuçlar,
- İlgili kişinin cevabı yetersiz görmesi halinde meydana gelebilecek sonuçlar (Kurul'a şikâyet, yetkili mahkemeye başvuru)

Etkin uygulamanın bir diğer unsuru ise grup üyesi şirketlerce bağlayıcı şirket kuralları hükümlerine topluluk içi veri işleme ve aktarım süreçlerinde uyum sağlanıp sağlanmadığının denetlenmesidir. Bu kapsamda gerek bağlayıcı şirket kurallarında gerekse başvuru formunda söz konusu denetimlerin ne sıklıkla gerçekleştirileceği, denetimlerin kapsamının ne olduğu ve bu denetimin kimler tarafından yürütüleceğinin açık bir şekilde ortaya konması gerekmektedir. Bununla birlikte Kurum bu denetimlerin sonuçlarının ilgili grup üyeleri ile paylaşılması ve bu sonuçlara bağlı olarak her bir şirketçe gerekli iyileştirme çalışmasının yapılması gerektiğini belirtilmektedir. Kurum tarafından yayımlanan bağlayıcı şirket kurallarına ilişkin yardımcı belgede belirtilen hususlardan biri de grup üyesi şirketlerce bağlayıcı şirket kurallarında Kurum'un da belirli durumlarda söz konusu

[290] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm, Erişim Tarihi: 30.12.2021.

denetim sonuçlarına erişim sağlama hakkı bulunduğu ve gerekli görmesi halinde Kurum'un da grup şirketler nezdinde bir denetim gerçekleştirmeye yetkili olduğudur. Bununla birlikte Kurum, bağlayıcı şirket kurallarına uyumluluğun denetlenmesine ilişkin başvuru formunda özellikle aşağıdaki açıklamalara yer verilebileceğini belirtmektedir:

- Denetim için hangi yöntem ve mekanizmaların oluşturulduğu,
- Bu mekanizmaların belirli aralıklarla güncellenip güncellenmediği ve güncelleniyorsa hangi aralıklarla güncellendiği,
- Şirketin hangi departmanının denetim kararı verdiği,
- Denetimin kimin tarafından gerçekleştirileceği,
- Denetimin hangi aralıklarla gerçekleştirileceği ve denetimin süresi,
- Denetimin kapsamının ne olduğu (şirketin veri işleyenleri, alt yapı ve bilgi teknolojileri sistemleri, yönetim tarafından alınan idari tedbirlerin yeterliliği vb.),
- Denetim sonucu raporlamaların yapılıyor olup olmadığı.

Son olarak bağlayıcı şirket kurallarının etkin bir şekilde uygulama alanı bulması için grup üyesi şirketler tarafından en az bir adet görevli personel atanması gerekmektedir. Bu noktada grup üyesi şirketlerin her biri kendi şirketleri için farklı bir görevli personel belirleyebilecekleri gibi topluluğun geneli için görev alacak tek bir görevli personelin belirlenmesi de mümkündür. Bu kapsamda atanacak görevli personel bağlayıcı şirket kurallarının grup üyesi şirketlerce uygun bir şekilde uygulamaya konup konmadığını takip etmekle görevlidir ve bir bakıma uyum takip elemanı olarak faaliyet göstermektedir[291]. Görevli personelin yürüttüğü takip faaliyetleri sonucunda gördüğü aksaklık ve/veya eksiklikleri raporlaması ve şirketlerin üst yönetimine aktarması beklenmektedir. Grup üyesi şirketlerin bağlayıcı şirket kurallarında söz konusu personelin kimlik ve iletişim bilgilerine,

[291] Toparlak, s.106-107.

görev tanımına ve sorumluluklarına ve ne kadar süreyle görevli olduğuna dair gerekli açıklamalara yer vermesi gerekmektedir.

3.2.5.3. Kurumu ile Koordinasyon

Bağlayıcı şirket kurallarının Kurul tarafından onaylanması ardından uygulama konması halinde dahi Kurum'un bağlayıcı şirket kurallarını uygulamaya koyan şirketler ile koordinasyonu sona ermemekte ve belirli aralıklarla bağlayıcı şirket kurallarına tabi olan grup üyesi şirketler üzerinde denetim faaliyetleri gerçekleştirebilecektir. Bu denetim faaliyetinin kural olarak Türkiye'de kurulu grup üyesi şirketler üzerinde gerçekleşeceği kabul edilse de Türkiye'den aktarılan kişisel verileri işleyen üçüncü ülkelerdeki grup üyesi şirketlere yönelik de farklı şekillerde denetim faaliyetleri yürütülebilecektir. Kurum gerekli görmesi halinde (re'sen) ilgili grup üyesi şirketten aktarıma ve yürüttüğü işleme faaliyetine ilişkin gerekli açıklamalarda bulunmasını ya da belirli belgelerin kendisine ibraz edilmesini talep edebilir. Bununla birlikte Kurum tarafından yapılan inceleme ve/veya denetim sonrasında ilgili grup üyesi şirkete yönelik belirli talimatlarda bulunulması da mümkündür. Söz konusu talimatların ilgili grup üyesi şirket tarafından gecikmeksizin yerine getirilmesi gerekmektedir. Her bir grup üyesi şirketin de hem bağlayıcı şirket kurallarında hem de başvuru formunda Kurum tarafından gerekli görüldüğü durumlarda tüm üyelerin Kurum tarafından denetlenebileceğini ve bu kurallarla ilgili herhangi bir konuda Kurum'un tavsiyelerine ve talimatlarına uymayı kabul ettiğini açık bir şekilde taahhüt etmesi gerekmektedir.

3.2.5.4. Kişisel Verilerin İşlenmesi ve Aktarılması

Grup üyesi şirketler tarafından bağlayıcı şirket kuralları ve başvuru formunda bu kurallara tabi olacak grup üyesi şirketlerin ticaret sicili ve iletişim bilgilerine, başta Türkiye'deki veri sorumlusu grup şirketin olmak üzere grup üyesi şirketlerin her birinin irtibat kişilerine ait iletişim bilgilerine ve yurt dışına yapılacak aktarım ve gerçekleşecek veri işleme faaliyetlerine ilişkin açıklamalara yer verilmelidir.

Bununla birlikte bu bilgilerde yapılacak değişikliklerin de gecikmeksizin bağlayıcı şirket kurallarına yansıtılacağı ve gerekmesi halinde Kurul'a da yeniden bildirileceğinin taahhüt altına alınması gerekmektedir. Öyle ki bağlayıcı şirket kuralları yurt dışına yapılacak kişisel veri aktarımlarının hukuka uygunluğunun temin edilmesi adına hazırlanmakta ve uygulamaya konmaktadır. Dolayısıyla gerek başvuruda gerekse bu kurallar dahilinde yurt dışına yapılacak aktarım faaliyetinin, bu aktarıma tabi kişisel verilerin, aktarımın amaçlarının, aktarımın yapılacağı alıcı tarafların, aktarımın yapılacağı kanalların açık bir şekilde Kurul'un değerlendirilmesine sunulacak şekilde belirtilmesi beklenmektedir. Grup üyesi şirketler tarafından hangi aktarımların bağlayıcı şirket kurallarına tabi olacağının belirlenmesi ve bu aktarıma ilişkin detaylı açıklamalara yer verilmesi gerekmektedir. Kurum da bağlayıcı şirket kurallarına ilişkin yayımladığı duyurunun ekindeki yardımcı belgede grup üyesi şirketlerin bağlayıcı şirket kuralları ve başvuru formu kapsamında aktarıma konu kişisel verinin niteliğinin (genel veya özel nitelikli kişisel veri), kategorisinin (kimlik, iletişim, lokasyon, özlük gibi) aktarım amaçlarının ve sürelerinin, veri konusu kişi grubu veya gruplarının (çalışan, stajyer, ziyaretçi, ürün veya hizmet alan kişi gibi), veri aktarımının hangi yöntemle gerçekleştirileceğinin, veri aktarımının hukuki sebebi/sebeplerinin, aktarılacak verilerin grup içerisindeki dağılımının diğer bir deyişle alıcı grubunda yer alan her bir grup üyesi şirketin (tam unvanları ve iletişim bilgileri ile birlikte) ve varsa sonraki aktarımlarının açıklanması gerektiğini belirtmektedir.

Söz konusu hususların ayrıntılı bir şekilde açıklanması ile birlikte Kurul tarafından bu aktarım ve işleme faaliyetlerinin hukuka uygunlarına ilişkin kapsamlı değerlendirmeler yapılabilmektedir. Örneğin bağlayıcı şirket kurallarında grup üyesi şirketin personellerine ait özlük verilerinin yurt dışındaki grup üyesi şirkete aktarılmasından sonra yurt dışında 20 yıl boyunca saklanacak olduğunun belirtilmesi halinde Kurul söz konusu saklama süresinin KVKK'da öngörülen genel ilkelere uygun olmadığı ya da aktarıma tabi kişisel veriler arasında personellerin din verilerine yer verilmesi halinde bu verinin aktarımının işleme amaçlarıyla

bağlantılı olmadığı gerekçesiyle aktarıma onay vermeyebilecektir. Ayrıca söz konusu bilgilerin açık bir şekilde belirtilmesi ile bu verilere ilişkin alınabilecek veri güvenliği tedbirlerinin ve bağlayıcı şirket kuralları nezdinde verilen taahhütlerin yeterliliği ve uygunluğu da daha etkili bir şekilde değerlendirilebilecektir. Son olarak başvuruda bulunan grup üyesi şirketlerce Türkiye'den yurt dışına yapılan aktarımlar sonraki yurt dışındaki grup üyesi şirket tarafından yapılabilecek aktarımlar (ileriki aktarımlar) için de bağlayıcı şirket kurallarının geçerli olacağı taahhüdüne yer verilmesi gerektiği unutulmamalıdır.

3.2.5.5. Raporlama ve Kayıt Değişikliği Mekanizmaları

Grup üyesi şirketlerin yapılarında ve/veya aktarım faaliyetlerine ilişkin unsurlarda meydana gelen değişikliklerin bağlayıcı şirket kurallarına da yansıtılması gerekmektedir[292]. Bu sebeple bağlayıcı şirket kurallarına tabi olan grup üyesi şirketlerin gerekli durumlarda bu kuralları değiştirmeyi ve güncellemeyi ve söz konusu değişikliği gerek topluluk içerisinde duyurmayı gerekse Kurum'a da bildirmeyi taahhüt etmesi gerekmektedir. Bu taahhüde hem bağlayıcı şirket kurallarında hem de başvuru formunda yer verilmelidir. Kurum bağlayıcı şirket kurallarına ilişkin duyurusunun ekinde yayımladığı yardımcı belgede bağlayıcı şirket kurallarına tabi olan grup üyesi şirketlerin tam ve güncel bir listesinin ve bu kurallarda yapılacak güncellemelerin topluluk içerisinde belirlenecek bir ekip veya birim tarafından kayıt altına alınması[293] ve belirli durumlarda bu değişikliklerin ilgili kişilere ve Kurum'a bildirilmesi gerektiğini belirtmektedir[294].

Bununla birlikte söz konusu yardımcı belgede bağlayıcı şirket kurallarına yeni bir grup üyesinin taraf olması halinde bu durumun Kurum'a bildirilmesi ve bu üyeye bağlayıcı şirket kurallarına tam olarak uyum sağlayıncaya kadar herhangi bir kişisel

[292] WP 257.
[293] Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formuhttps://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, Erişim Tarihi: 23.11.2021.
[294] Toparlak, s.108.

veri aktarımının yapılmaması gerektiği, ancak uyumun tam olarak sağlanması halinde bu üyeye kişisel veri aktarımına başlanabileceği gibi bu durumun da tekrar Kurum'a bildirilmesinin şart olmadığı düzenlenmiştir. Diğer taraftan Kurum'un yayımladığı yardımcı belgedeki açıklamalar uyarınca bağlayıcı şirket kurallarında ve/veya bu kurallara taraf olan üyelere ait bilgilerde herhangi bir değişiklik meydana gelmesi halinde bu değişiklik gerekçesi ile birlikte Kurum'a yılda bir kez bildirilmelidir. Ancak bağlayıcı şirket kuralları ile tesis edilen koruma seviyesinde ya da bu kuralları önemli şekilde etkileyen herhangi bir değişikliğin meydana gelmesi halinde ise bu durumun gecikmeksizin Kurum'a bildirilmesi gerektiği düzenlenmiştir.

3.2.5.6. Veri Güvenliğinin Sağlanması

Bağlayıcı şirket kurallarına tabi olan grup üyesi şirketlerden her birinin KVKK m. 12 uyarınca kişisel verilerin hukuka uygun bir şekilde işlenmesi, kişisel verilere hukuka aykırı bir şekilde erişim sağlanmaması ve gereğine uygun bir şekilde muhafaza edilmeleri için gerekli olan veri güvenliği tedbirlerini almakla yükümlüdür. Her bir grup üyesi şirketin bu tedbirleri eksiksiz bir şekilde almış olduğunu gerek bağlayıcı şirket kuralları gerekse başvuru formunda açık bir şekilde taahhüt etmesi gerekmektedir. Bu kapsamda Çalışmamızın ikinci bölümünde belirttiğimiz veri güvenliği tedbirlerinin bağlayıcı şirket kuralları ile grup içinde aktarıma tabi tutulacak kişisel veriler için de geçerli olacağını belirtebiliriz. KVKK m.4/2 uyarınca düzenlenen veri işlemenin temel ilkelerinin bağlayıcı şirket kuralları uyarınca gerçekleştirilecek her bir veri aktarımı ve işleme faaliyeti için temin edilmesi[295] ve Kurum tarafından yayımlanan idari ve teknik tedbirlerin aktarıma tabi tutulan kişisel verinin niteliğine uygun düştüğü ölçüde grup üyesi şirketler tarafından alınması bu kapsamda yürütülmesi beklenen çalışmalar arasında yer

[295] Toparlak, s.109.

almaktadır[296]. Söz konusu tedbirlerin gerek grup üyeleri arasındaki kişisel veri aktarımları için gerekse ilerideki aktarımlar için geçerli olduğu unutulmamalıdır[297].

Kurum yayımladığı yardımcı belgede grup üyesi şirketlerden her birinin bağlayıcı şirket kuralları uyarınca aktarıma tabi tutulan kişisel verilere ilişkin herhangi bir ihlal meydana gelmesi halinde bu ihlalin derhal diğer grup üyesi şirketler ile yetkili veri koruma otoritesine ve ilgili kişilere bildirilmesi gerektiği düzenlenmektedir. Öyle ki KVKK uyarınca bu bildirimin ihlalin meydana geldiğinin tespit edilmesinin ardından 72 saat içerisinde gerçekleştirilmesi beklenmektedir. Ayrıca gerçekleşen veri ihlallerinin yanı sıra ihlal şüphesi olan durumların da grup üyeleri arasında bildirilmesi faydalı olabilecektir. Diğer taraftan söz konusu veri ihlallerinin bu ihlalden zarar gören kişisel verilerin, bu ihlalin sebep olduğu etkilerin ve ihlalin giderilmesi için yapılan müdahalelerin neler olduğunun kayıt altına alınması ve söz konusu kayıtların da Kurum'a iletilmesi gerekmektedir.

Bağlayıcı şirket kuralları uyarınca grup üyesi şirketlerin yerine getirmesi gereken veri güvenliği yükümlülüklerinin herhangi bir yasal veya sözleşmesel engele takılmaksızın tam ve sürekli bir şekilde uygulama alanı bulması gerekmektedir. Bu kapsamda bağlayıcı şirket kurallarının uygulanması önünde bir engel de herhangi bir grup üyesi şirketin kendi ülkesinde geçerli olan iç hukuk kuralları olabilir. Dolayısıyla bağlayıcı şirket kuralları hazırlanırken her bir üyenin kendi iç hukukunda yer alan mevzuat düzenlemelerinin bu kurallar üzerindeki etkisinin göz önünde bulundurulması büyük önem arz etmektedir. Bu yönde yapılacak bir araştırma sonucunda bağlayıcı şirket kurallarındaki yükümlülüklerin yerine getirilmesini engelleyen veya bu kuralların uygulanmasını önemli ölçüde etkileyen iç hukuk düzenlemelerinin derhal topluluğun Türkiye'deki grup üyesi şirkete bildirilmesi gerekmektedir. Ayrıca bu iç hukuk düzenlemelerinin bağlayıcı şirket

[296] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesine İlişkin Rehberi, Sage Matbaacılık, Ankara, 2017, https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf, Erişim Tarihi: 30.12.2021.
[297] Dülger, s.405; Çekin, 2020, s.221.

kurallarının sağladığı garantiler üzerinde önemli bir olumsuz etkiye sahip olduğunun tespit edilmesi halinde bu düzenlemelerin Kurum ile de paylaşılması beklenmektedir[298].

Kurum, bağlayıcı şirket kurallarına ilişkin yayımladığı duyurunun ekindeki bağlayıcı belgede Schrems II kararında da değinildiği üzere ilgili grup üyesi şirketin kendi ülkesindeki kanunların milli güvenliği sağlamak veya farklı bir amaçla belirli otoritelere yetki vermesi ve bu yetkinin ilgili grup şirkete aktarılan kişisel verilere söz konusu otorite tarafından erişim sağlanması hakkını da kapsaması halinde bu düzenlemelerin de Kurum'a bildirilmesi gerektiğini ifade etmektedir. Kurum, ilgili ülkedeki otoritenin bu verilere erişim sağlamak yönünde grup üyesi şirkete herhangi bir talepte bulunması durumunda bu talebin, bu talep ile erişilmek istenen verilerin neler olduğunun, talep eden otoritenin kimliğinin, yasal dayanağının ve gerekli diğer bilgilerin de kendisine iletilmesi gerektiğini öngörmektedir. Bununla birlikte Kurum, ilgili grup üyesi şirketin tüm çabasına rağmen söz konusu talep hakkında Kurum'u bilgilendirebilecek bir konumda olmaması halinde, bağlayıcı şirket kurallarında kendisine gelen taleplere ilişkin olarak yıllık bazda Kurum'a genel nitelikte bir bilgilendirmeyi sağlamayı taahhüt etmesi gerektiğini belirtmektedir. Ancak Kurum böyle bir yasaklama halinde ilgili grup üyesi şirketin söz konusu yasaklamadan hukukun izin verdiği ölçüde feragat etmek adına gerekli çabayı göstermesi ve bunun ispatlanabilir olmasını aramaktadır. Öyle ki Kurum bu noktada Tüzük ile benzer bir anlayışla her bir grup üyesi şirketinin bağlayıcı şirket kuralları uyarınca aktarıma tabi tutulan kişisel verileri" demokratik bir toplumda gerekli olanın ötesine geçecek şekilde büyük, orantısız ve rastgele" aktarmaması gerektiğini ifade etmektedir. Ancak bu ifadenin muğlak olması sebebiyle uygulamada tıpkı Schrems II kararında da belirtildiği üzere kamu kurumlarına yönelik belirli hukuka aykırı veri aktarımları yapılması gündeme gelebilecektir.

[298] Bkz. aynı yönde Tüzük m.47/2 ve Toparlak, s.109-110.

3.2.5.7. Hesap Verebilirlik ve Diğer Araçlar

Hesap verebilirlik, KVKK ve alt mevzuat hükümleri içinde açık bir şekilde yer alan veri koruma ilkelerinden olmasa da[299] hesap verilebilirliğin içeriği ve kapsamının bağlayıcı şirket kurallarına dâhil edilmesi gerekmektedir[300]. Hesap verebilirlik, veri sorumlularının KVKK m.12'de yer alan veri güvenliğine dair sorumlulukları yerine getirmeleri ve bu çalışmalarını ispatlanabilir bir şekilde gerçekleştirmeleri anlamına gelmektedir. Bağlayıcı şirket kurallarının faydalarından biri de KVKK m. 12'de yer alan veri güvenliği yükümlülüklerine dair hesap verebilirliği arttırması ve bu kuralların grup üyesi şirketlerin verdikleri yazılı taahhütler ile birlikte ispat aracı olarak kullanılabilmesidir. Bağlayıcı şirket kuralları ile yurt dışına aktarılan kişisel verilerin güvenliğinin ve gizliliğinin sağlanması hususunda hesap verebilir ve şeffaf bir uyum süreci oluşturulması amaçlanmaktadır. Bu amaçla bağlayıcı şirket kurallarına tabi tutulan her bir veri işleme ve aktarım faaliyetlerinin yazılı olarak kayıt altına alınması ve herhangi bir talep ya da uyuşmazlık halinde bir ispat aracı olarak bu kayıtların kullanılabilmesi beklenmektedir. Bu sebeple her bir grup üyesinin bağlayıcı şirket kuralları ve başvuru formunda söz konusu veri işleme ve aktarım faaliyetlerini alacakları tedbirlerle yazılı halde tutacaklarını, talep halinde KVKK m. 15/3 uyarınca 15 gün içerisinde Kurum'a sunmakla yükümlü olduklarını ve Kurum'un da uygun bulması halinde grup şirketler nezdinde yerinde denetim ve inceleme yapabileceğini taahhüt etmeleri gerekmektedir. Kişisel veri işleme ve aktarım süreçlerinin yazılı bir şekilde kaydedilmesi ile bu süreçlerde meydana gelen veya gelmesi muhtemel olan risklerin analizi de kolaylaşmakta ve gerçekleşen veri işleme faaliyetleri sonuçları ile birlikte kolayla incelemeye tabi tutulabilmektedir. Bu risk incelemeleri ve değerlendirmeleri grup üyesi şirketler ve topluluk için hukuka aykırılık riski taşıyan veri işleme ve aktarım süreçlerinin de tespit edilmesine ve bu süreçlerin sona erdirilmesine fayda sağlamaktadır. Bu değerlendirmeler sonucunda riskli görülen veri işleme ve aktarım süreçlerine ilişkin

[299] Tüzük, m. 5/2 uyarınca veri sorumluları, veri işleme ilkelerine uyulduğuna dair hesap verebilirliği sağlamakla yükümlüdürler bkz. Dülger, s.139.
[300] Toparlak, s.110.

gerekli tedbirler alınmalı ve olası ihlal durumlarının önüne erkenden geçilmesi amaçlanmalıdır. Söz konusu değerlendirmeler sonucunda ilgili grup üyesi şirketlerin tavsiye ve görüş almak amacıyla Kurum'a başvuruda bulunması ve danışması da mümkündür. Bu kapsamda elektronik ortamda gerçekleşen veri işleme faaliyetlerinin log kayıtlarının alınması, şirketlerin teknik alt yapı sistemlerinin dönemsel olarak sızma testlerine tabi tutulması ve bu test sonuçlarının raporlanması ile her bir grup üyesi şirket için gerektiğinde hesap verebilir bir yapının oluşturulması sağlanabilecektir.

Şeffaflık ilkesi de hesap verebilirlik ilkesi ile birlikte ele alınması gereken ve Tüzük uyarınca temel veri işleme ilkelerinden biri olarak kabul edilen unsurlardan biridir. KVKK'da doğrudan şeffaflık ilkesi tanımlanmış olmasa ve temel veri ilkelerinden biri olarak düzenlenmese de doktrinde kişisel verilerin işlenmesinde KVKK m.4/2 (c) uyarınca düzenlenen işleme amacıyla bağlantılı, sınırlı ve ölçülü veri işleme ilkesi ile ve KVKK m.11'de yer alan ilgili kişinin haklarında ve özellikle KVKK m. 10'da yer alan veri sorumlusunun aydınlatma yükümlülüğünde Türk kanun koyucusu dolaylı olarak şeffaflık ilkesine uygun tedbirlerin alınması gerektiğini öngörmektedir[301]. Bağlayıcı şirket kuralları ile şeffaflığın sağlanması adına Kurum tarafından yayımlanan duyuruda da bağlayıcı şirket kurallarının grup üyesi şirketler tarafından etkili bir şekilde uygulanması ve etkili uygulamayı temin edecek uyumluluk denetimi içinde raporlamanın şeffaf bir biçimde yapılması gerektiği ifade edilmiştir. Bununla birlikte Kurum yine grup üyesi şirketlerin uygulayacağı uyumluluk denetim programında, düzenli şekilde denetim yapılması ve denetimi kimlerin gerçekleştireceği gibi konulardaki yöntemlerin bağlayıcı şirket kuralları içerisinde açıklanmış olmasını gerekli görerek şeffaf bir uyumluluk sürecinin oluşturulmasını amaçlamaktadır. Diğer taraftan ilgili grup üyesi şirketin kendi ülkesindeki mevzuat hükümlerinin bağlayıcı şirket kurallarındaki yükümlülüklerini yerine getirmesini engelleyip engellemediğini veya söz konusu iç hukuk düzenlemelerinin bu kurallar ile getirilen hükümlerin uygulanmasını ciddi anlamda

[301] Çekin, 2020, s.81.

etkileyen düzenlemeler olup olmadığını derhal topluluğun Türkiye'deki bulunan grup üyesine bildirilmesi gerektiği de yine şeffaflık ilkesinin yerine getirilmesi adına düzenlenen yükümlülükler arasındadır[302]. Son olarak KVKK m. 16 uyarınca düzenlenen VERBİS'e kayıt yükümlülüğü de şeffaflık ilkesinin bir yansımasıdır. Buna göre Türkiye'de veri işleme faaliyeti gösteren ve Türkiye'den aktarılan kişisel verileri işleyen grup üyesi şirketlerden her birinin Türkiye'de kurulu olsun ya da olmasın VERBİS kaydını gerçekleştirerek ve kişisel veri envanterlerini hazırlayarak veri işleme ve aktarım faaliyetlerinin şeffaflığını sağlamak adına gerekli çalışmaları yürütmesi gerektiği öngörülmüştür.

3.2.5.8. Yardımcı Bilgi ve Belgeler

Kurum, bağlayıcı şirket kurallarına ilişkin yayımlandığı duyurunun ekindeki yardımcı belgede grup üyesi şirketlerin bağlayıcı şirket kuralları başvurusunda bulunurken zorunlu olmasa da başvuruların değerlendirilmesi bakımından eklemelerinin faydalı bulunduğu belge ve bilgiler olduğunu belirtmekte ve bu belge ve bilgilere aşağıdaki örnekleri vermektedir. Buna göre bağlayıcı grup şirket başvurusunda bulunan grup üyesi şirketlerin imkanları ölçüsünde bu bilgi ve belgeleri de temin etmeleri başvurularının olumlu sonuçlanması için faydalı olabilecektir:

- Aktarımın yapılacağı yurt dışındaki grup üyesi şirketin bulunduğu ülkelerin taraf olduğu ve kişisel verilerin korunması hususunda hükümler içeren uluslararası sözleşmeler ve bu uluslararası sözleşmelerin kişisel verilere ilişkin ilgili kısımları

- Kişisel verinin aktarılacağı yurt dışındaki grup üyesi şirketin bulunduğu ülkede, kişisel verilerin korunması hususundaki ulusal mevzuat hükümleri ile

[302] Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman, https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, Erişim Tarihi: 01.01.2022.

yetkili bir kişisel verileri koruma otoritesinin var olup olmadığı bilgisi ve varsa bu otoritenin kuruluşu ve yetkileri ile ilgili mevzuat hükümleri ile uygulaması.

3.2.5.9. Başvuruya Dair Usul ve Esaslar

Bağlayıcı şirket kuralları Türk hukukunda henüz mevzuat hükümleri ile düzenleme altına alınmadığından bu kuralların ne şekilde hazırlanacağı ve içeriğinin ne şekilde belirleneceği konularında olduğu gibi bağlayıcı şirket kurallarına ilişkin başvurunun nasıl yapılacağı ve başvurunun usul ve esasları da Kurum'un bağlayıcı şirket kurallarına ilişkin 10 Nisan 2020 tarihinde yayımladığı duyuruda ve bu duyurunun ekinde yer alan başvuru formu ve yardımcı belgede açıklanmıştır. Kurum bu duyurusunda, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirket üyelerine yapılacak kişisel veri aktarımlarında yeterli korumanın yazılı olarak taahhüt edildiği bu kuralların duyurunun ekinde yer alan başvuru formu ve yardımcı belgedeki talimat uyarınca hazırlanması gerektiğini ve akabinde gerekli talimatların izlenerek Kurum'a, bağlayıcı şirket kuralları başvurusu yapılması gerektiğini belirtmektedir.

Kurum'a yapılacak başvurular Kurum içerisinde başvuruyu değerlendirmek üzere oluşturulan bir Kurul tarafından incelenmektedir. Kurul bağlayıcı şirket kuralları başvurusunu kabul edebilir, bu durumda başvuru onaylanır ve Kurul'un verdiği izin uyarınca bağlayıcı şirket kuralları uygulamaya alınarak yurt dışına veri aktarımı gerçekleşebilir. Bunun dışında Kurul'un başvuruyu reddetme yetkisi de bulunmaktadır. Kurul tarafından henüz herhangi bir bağlayıcı şirket kuralları başvurusuna onay verildiği yönünde bir karar yayımlanmamıştır. Ancak Kurul'un başvuruyu ilk etapta reddetse bile bunu gerekçesiyle başvuran şirkete bildireceği ve başvurunun tekrar değerlendirme altına alınabilmesi için tamamlanması gereken eksiklikleri belirttiği bir talimatlandırma kararı metni iletmesi de mümkün gözükmektedir. Bununla birlikte Kurul tarafından bir bağlayıcı şirket kuralları başvurusunun onaylanması halinde söz konusu bağlayıcı şirket kuralı aksi bu

kurallarda öngörülmediği müddetçe süresiz bir şekilde uygulama alanı bulmaktadır. Fakat gerekmesi halinde Kurul tarafından onaylanan bağlayıcı şirket kurallarının uygulanmasının askıya alınması ya da sona erdirilmesi de mümkündür.

- **Başvuru Yapma Yetkisi**

Kurum, bağlayıcı şirket kurallarının hazırlanmasından sonra kendisine başvuru yapma yetkisinin topluluğun Türkiye'de bulunan merkez şirkette olduğunu, ancak topluluğun merkezinin Türkiye'de bulunmaması halinde Türkiye'de bulunan herhangi bir grup üyesi şirket tarafından da başvurunun yapılabileceğini belirtmektedir. Bağlayıcı şirket kuralları, aktarımın Türkiye'den yurt dışına yönelmesi itibariyle Türkiye'den aktarımı sağlayacak ve Türkiye'de kurulu bir grup üyesi şirketin varlığını zorunlu kılmaktadır. Bu sebeple başvuruyu da topluluğun Türkiye'deki grup üyesi şirketin yapması gerekmektedir. Kurum tarafından başvurunun kural olarak yapılabileceği topluluğun Türkiye'deki merkez şirketi esasında topluluğun Türkiye'deki hâkim şirketini karşılamaktadır. Ancak topluluğun Türkiye'de kurulu bir hâkim şirketi bulunmuyorsa, diğer bir deyişle topluluğun hakim şirketi yurt dışında ise söz konusu hakim şirketin Türkiye'de bulunan bağlı şirketlerinden biri de başvuruyu yapabilecektir. Kurum, bağlı şirketin başvuruyu yapacak olması halinde söz konusu grup üyesi şirketi topluluk adına başvuruyu yapmak üzere yetkilendirilmiş grup üyesi ya da yetkili grup üyesi olarak tanımlamaktadır[303]. Kurum'a başvuru yapacak yetkili grup üyesinin topluluk tarafından hazırlanan bağlayıcı şirket kurallarının yanı sıra gerekli diğer bilgi ve belgeleri de başvuru esnasında Kurum'un bilgisine sunuyor olması gerekmektedir.

- **Başvuruda Sunulacak Bilgi ve Belgeler**

Kurum'a sunulacak bağlayıcı şirket kurallarının farklı dillerde hazırlanması ve topluluk içerisinde uygulamaya konması mümkündür. Ancak Kurum'a yapılacak

[303] Dülger, KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, s.6

başvurularda yetkili grup üyesi tarafından sunulacak bağlayıcı şirket kurallarının Türkçe hazırlanması gerekmektedir. Bağlayıcı şirket kurallarının yanı sıra bu kuralların içerdiği taahhütleri destekleyen yardımcı bilgi ve belgelerin de bulunması halinde Kurum'a ibrazı aranmaktadır. Öyle ki bağlayıcı şirket kuralları dahilinde belirtilen beyan ve taahhütlerin tevsik edildiği bilgi ve belgeler başvurunun olumlu değerlendirilmesinde büyük bir öneme sahiptir. Söz konusu bilgi ve belgeler ile hazırlanan bağlayıcı şirket kuralları Kurum'un duyurusunun ekinde yer alan başvuru formunun doldurulması ile birlikte Kurum'a sunulmaktadır. Başvuruda sunulacak evrakların tamamı Türkçe hazırlanmalı, yurt dışından temin edilen belgelerin ise Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesi'ne ya da buna muadil olacak şekilde apostil onayından geçirilerek Türkiye'de tercüme edilmesi ve akabinde noter onaylı bir şekilde Kurum'a sunulması gerekmektedir. Söz konusu başvuru evraklarının tamamı Kurum'a elden ya da posta yoluyla ulaştırılmalıdır. Bu noktada Kurum'un e-posta adresine ya da kayıtlı elektronik posta adresine yapılacak başvurular geçerli kabul edilmemektedir. Başvuru evraklarının yetkili grup üyesi şirketin temsil ve ilzama yetkili kişileri tarafından imzalanması ya da vekil marifetiyle yapılacak başvurularda da vekâletname aslı veya onaylı örneğinin bulunması gerekmektedir.

Bağlayıcı şirket kuralları başvurusunda Kurum tarafından yayımlanan duyurunun ekindeki matbu başvuru formunun kullanılması gerekmektedir. Bu formda başvurucu sıfatıyla yetkili grup üyesi kendisi ve dahil olduğu topluluğa dair bilgileri eksiksiz ve doğru bir şekilde doldurmalıdır. Topluluğun genel merkezinin ticaret unvanı ile merkez adresine ve Türkiye'de yer alan yetkili grup üyesine dair unvan ve adres gibi ticaret sicil bilgileri ile iletişim bilgilerinin (telefon numarası, faks, e-posta adresi vb.) tamamına başvuru formunda yer verilmesi gerekmektedir. Bununla birlikte başvuru formunda kişisel veri aktarımının Türkiye'den hangi ülkelere yönelik gerçekleşeceğinin ve bu ülkelerde yer alan grup üyesi şirketlerin ticaret unvanlarının ve adresleri ile iletişim bilgilerinin de belirtilmesi beklenmektedir. Ayrıca Çalışmamızın 3.2.5. Türk Hukukunda Bağlayıcı Şirket

Kuralları başlığı altında belirttiğimiz unsurların da başvuru formunda gereğine uygun bir şekilde taahhüt edilmesi gerekmektedir.

Bu form uyarınca başvuru için; veri sorumlusu/işleyen sıfatıyla grup üyesi şirketin adı/unvanı, genel merkezinin adresi ve genel merkezi Türkiye'de değilse Türkiye'de kurulu grup üyesinin adresinin yazılması zorunludur. Başvuru işlemini yapan yetkili gerçek kişi açısından başvurucu kişinin adı/unvanı, T.C. kimlik numarası, başvurucunun hukuki statüsü, irtibat kişisinin adı veya birimi, irtibat kişisinin adresi, telefon numarası, elektronik posta adresi gibi bilgiler de formda bulunmalıdır[304]. Bununla birlikte başvuru formunda, veri aktarımının yapılacağı ülke ve bu kuralların kapsadığı bütün grup üyeleriyle iletişim bilgilerinin de yer alması gerekmektedir.

- **Başvurunun Sonuçlandırılması**

Bağlayıcı şirket kurallarına ilişkin başvurular, Kurum tarafından başvuru tarihinden itibaren bir yıl içinde ele alınarak sonuca bağlanır. Kurum bu sürenin altı aylık süreler şeklinde uzatılabileceğini belirtmektedir. Başvurunun Kurulca onaylanması halinde bu durum, Kurum tarafından yetkili grup üyesine yazılı olarak bildirilir ve Kurum'un gerekli görmesi halinde ayrıca Kurum'un internet sitesinde ilan edilir[305]. Buna karşılık Kurum'un başvuruyu reddetmesi halinde yetkili grup üyesi şirket tarafından bağlayıcı şirket kurallarına dayanılarak yurt dışına veri aktarımı yapılamayacaktır. Ancak Kurum'un böyle bir durumda başvurunun olumlu bir şekilde değerlendirilebilmesi için başvurudaki eksiklikleri yetkili grup üyesi şirkete yazılı olarak ret kararının gerekçesinde belirteceği tahmin edilmektedir.

[304] Bağlayıcı Şirket Kuralları Hakkında Duyuru https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINAKISISEL- VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, Erişim Tarihi: 30.12.2021

[305] Bağlayıcı Şirket Kuralları Hakkında Duyuru https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINAKISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, Erişim Tarihi: 31.12.2021.

SONUÇ

Şirketler topluluğu bünyesindeki grup üyesi her bir şirket, gerçekleştirdiği veri işleme ve aktarım faaliyetleri ile aslında birer veri sorumlusu ve veri işleyen olarak hareket etmektedir. Bu kapsamda grup üyesi şirketlerin veri sorumlusu ve veri işleyen olarak gerçekleştirdikleri ve/veya taraf oldukları veri işleme ve aktarım faaliyetlerinden doğan yükümlülüklerini gereğine uygun bir şekilde yerine getirmesi gerekir. Bu yükümlülüklerin ifası ile esasında veri işleme ve aktarım faaliyetlerinin konusu olan kişisel verilerin sahibi ilgili kişilerin temel hak ve özgürlüklerin korunması ve kişisel verilerin gelişi güzel ve hukuka aykırı bir şekilde işlenmesinin önüne geçilmesi amaçlanmaktadır. Bu noktada çok uluslu grup şirketler arasındaki kişisel verilerin operasyonel olarak hangi amaçlarla aktarıma tabi tutulabileceğinin ve bu amaçların altında yatan gerekçelerin incelenmesi, söz konusu aktarım faaliyetlerinin kişisel verilerin korunması mevzuatı hükümlerine uygunluklarının anlaşılması açısından büyük önem arz etmektedir. Kişisel verilerin grup içinde aktarıma tabi tutulmasının amaçları ekonomik, ticari, hukuki, vergisel veya farklı bir sebeplere dayanabileceği gibi çok uluslu grup şirketlerin hukuki nitelikleri gereği tabi oldukları kanuni yükümlülüklerden, taraf oldukları sözleşmelerden, topluluğun menfaatlerini sağlamak adına kurumsal politikalarından veya yürüttükleri ticari faaliyetlerin bir gereği olarak gerçekleştirdikleri muhtelif işlemlerden ileri gelebilir.

Topluluğun ticari faaliyetlerinin ve karlılığının devamlılığı esas olsa da bu faaliyetler süresince aktarılan kişisel verilerin güvenliğinin ve gizliliğinin sağlanması da aktarıma taraf olan grup üyesi şirketlerce yerine getirilmesi gereken ciddi bir yükümlülük teşkil etmektedir. Kişisel verilerin güvenliğinin ve gizliliğinin sağlanması için KVKK ve alt mevzuat hükümlerinde öngörülen temel veri işleme ilkeleri ile veri işleme şartlarına eksiksiz bir şekilde itibar edilmesi ve aktarıma tabi verilerin korunması için gerekli idari ve teknik tedbirlerin grup üyesi şirketlerce alınması gerekmektedir. Bu kapsamda doğrudan KVKK ve alt mevzuat hükümlerinde açıkça düzenleme altına alınmasa da Kurum tarafından 10 Nisan

2020 tarihinde kendi internet sitesinde yayımlanan ve yurt dışına veri aktarım mekanizmaları arasında çok uluslu grup şirketler için bir alternatif teşkil eden bağlayıcı şirket kurallarının etkili bir rol oynadığını söylemek gerekir. Öyle ki aktarıma tabi kişisel verilerin korunması için aktarımın tarafı olan grup üyesi şirketleri ortak ve tam bir sorumluluğa çağıran, bu verilerin güvenliği ve gizliliğinin sağlanması için mevzuatta öngörülen asgari güvenlik tedbirlerinin gereğine uygun ve sürekli bir şekilde yerine getirileceği şeklinde her bir grup üyesinin taahhüdünü içeren ve aynı zamanda aktarıma tabi kişisel verilerin sahibi ilgili kişiler için mevzuattan doğan haklarını kullanabilmeleri ve gerektiğinde tazminat talebinde bulunabilmeleri için topluluk içerisinde normal şartlarda var olmayan ancak bu kurallar ile oluşturulan başvuru ve şikayet mekanizmaları kurulmasını şart koşan bağlayıcı şirket kuralları, grup üyesi her bir şirketin kişisel verilerin korunması mevzuatına uyum sağlamasını kolaylaştırmaktadır.

Bu vesileyle Çalışmamızda çok uluslu grup şirketlerin kendi aralarında gerçekleştirdikleri kişisel veri aktarımları, bu aktarımlar için alınabilecek tedbirler ve bağlayıcı şirket kurallarının bu aktarımlar için önemi anlatılarak ilerleyen dönemlerde BŞK başvurularında bulunan çok uluslu grup şirketler için bir rehber oluşturulması ve iyi uygulama örneklerine yer verilmesi amaçlanmıştır. Bununla birlikte bu konunun çok uluslu grup şirketlerce yürütülen operasyonel, hukuki ve ticari faaliyetler ele alınarak incelenmesi ile bu aktarımların önünün açılmasının ticaret hayatı ve ülke ekonomisi için ne denli önem arz ettiği de ortaya konmaya çalışılmıştır. BŞK'lerin hayata geçirilmesi ile birlikte bu sayede bu aktarımların hukuka uygunluklarının sağlanabileceği ve aktarımın tarafı olan grup üyesi şirketlerin her birinin kişisel veri mevzuatına uyum süreçlerinde ilerleme kat edebileceği düşüncesiyle Çalışmamızın ayrıca Kurul tarafından kabul alınan BŞK başvurularının onaylanması sürecini de olumlu şekilde etkileyeceği düşüncesindeyiz.

KAYNAKÇA

Akdağ, H., **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Adalet Yayınevi, 1. Baskı, 2013

Akgül, A., **Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi**, Beta Basım Yayın, İstanbul 2014.

Aksoy, H. C., **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması,** 1. Baskı, Ankara, Çakmak Yayınevi, 2010.

Anadolu, K., "**Avrupa Birliği Adalet Divanı**", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C.11, S.3, 2003, s.357-371.

Antalya, O. G./ Topuz, M., **Medeni Hukuk C. I,** Genişletilmiş 3. Baskı, Ankara 2019.

Article 29 Working Party, **working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites**, WP 56, http://www.interlex.it/testi/pdf/wd5035.pdf, (Erişim Tarihi: 05.12.2021).

Aşıkoğlu, Ş. İ., **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri,** İstanbul, On İki Levha Yayınları, 1. Baskı, 2018.

Avcı Braun, C., Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, Haziran 2018, s.13-34.

Aydın, M., **Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu ve Yargısal Denetimi**, Yayımlanmamış Yüksek Lisans Tezi, Ufuk Üniversitesi, Ankara, 2020.

Aydın, S. E., **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, On İki Levha Yayıncılık, İstanbul, 1. Baskı, 2015.

Ayözger Öngün, Ç., **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil,** İstanbul, Beta Yayınları, Genişletilmiş 2. Baskı, İstanbul, 2019.

Başalp, N., **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, Ankara, 2004.

Beytar, E., **İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması**, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2018.

Bozlak, A., **Kamusal Bağlamda Özel Hayatın Korunması: ABD Federal Yüksek Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Uygulaması Arasında Mukayeseli Bir İnceleme**, Türkiye Barolar Birliği Dergisi, (109), 2013, ss.55-92.

Cunningham, M., **Complying with International Data Protection Law**, University of Cincinnati Law Review, S.84 (2), 2018, s.421-450.

Çabuk, E., **Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması**, Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, İstanbul 2020.

Çakır Çelebi, F. B., "**Şirketler Topluluğunda Hâkim Teşebbüs**", Ticaret ve Fikri Mülkiyet Hukuku Dergisi C.4, S.1,2018, s.19-32.

Çekin, M. S., **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 3.Baskı, Oniki Levha Yayınları, İstanbul 2020.

Çekin, M. S., **6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanununun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi**, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 74, S. 2, ss. 629-644.

Dağ, G., **Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması,**Yayımlanmamış Doktora Tezi Marmara Üniversitesi, İstanbul, 2011.

Danailov, S., **The Accountability Of Non-State Actors For Human Rights Violations: The Special Case Of Transnational Corporations**, w. place., Institute Universitaire De Hautes Études Internationales, 1998.

Develioğlu, H. M., **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku**, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2017.

Dove, E., **The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era**, The Journal of Law, Medicine&Ethics, 46, 2018, ss. 1013-1030.

Dülger, M. V., **Kişisel Verilerin Korunması Hukuku,** Hukuk Akademisi Yayınları,1. Baskı, İstanbul, 2019.

Dülger, M. V., **KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları**, 11 Nisan 2020, s. 6, https://www.hukukihaber.net/kvkkdan-kisisel-verilerin-yurt-disina-aktariminda-onemli-bir-adim-baglayici-sirket-kurallari-makale,7685.html, (Erişim Tarihi: 01.12.2021).

Dündar, E., **Yeni Türk Ticaret Kanunu Çerçevesinde Çok Uluslu Şirketler**, Yayımlanmamış Doktora Tezi, İstanbul Kültür Üniversitesi, İstanbul 2013.

Eraslan Türkmen, S., **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**,1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019.

European Data Protection Board, **Frequently Asked Questions About the Judgement** C-311/18,https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf, (Erişim Tarihi: 01.12.2021).

European Union Agency For Fundamental Rights, **Handbook on European Data Protection Law**, Luxembourg, 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, (Erişim Tarihi:10.12.2021).

Göçmen Uyarer, S., **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, 2019.

Han, I. A., **Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası**, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt:18, Sayı:1, Ocak 2019, s.417-459.

Henkoğlu, T., **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara 2015.

Hocaoğlu, H./ Doğan, F. S. / Saltık, Z. S., **Bulut Yasası ve Schrems II Kararı Işığında Türkiye'de Müşteri Hizmeti Uygulamaları Hakkında Uygulamacı Perspektifinden Değerlendirmeler,** Terazi Hukuk Dergisi, C. 16, S. 174, Şubat 2021, ss. 364-368.

Information Commissioner's Office, **Guide to Codes of Conduct,** https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-thegeneral-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/ (Erişim Tarihi: 11.12.2021).

İspirli Armağan, M., **Uluslararası Hukukta Çok Uluslu Şirketler ve İnsan Hakları Yükümlülükleri**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul 2019.

Kalender, A. U., **Parçalı Bulutlar: Cloud Act ve Etkileri,** Kişisel Verileri Koruma Dergisi, S. 2(2), 2020, ss.73-106.

Kaya, A. E., **Kişilik Hakkı Olarak Kişisel Veriler ve Yeni Kişisel Verilerin Korunması Kanunu**, Terazi Hukuk Dergisi, Cilt:12, Sayı:125, Ocak 2017, s.67-80.

Kaya, C., **Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi,** İÜHFM, 2011, C. 69, S. 1-2, s. 317-334.

Kişisel Verileri Koruma Kurulu, **Bağlayıcı Şirket Kuralları**https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, (Erişim Tarihi: 01.12.2021)

Kişisel Verileri Koruma Kurumu, **6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar**, Yayın No: 31, Ankara 2020. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/28d8adba-2b41-41b2-bf36-d0ff0d845666.pdf, (Doğru Bilinen Yanlışlar), (Erişim Tarihi: 01.12.2021).

Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Ankara, 1. Baskı, 2018.

Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Rehberi**, Sage Matbaacılık, Ankara, 2017, https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf, (Erişim Tarihi: 30.12.2021).

Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,**

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF, s.57, (Erişim Tarihi:30.11.2021).

Kişisel Verileri Koruma Kurumu, **Veri Güvenliği Rehberi,** ISBN: 978-975-19-6834-O, KVKK Yayınları, Ankara, 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, (Erişim Tarihi: 30.12.2021).

Kişisel Verileri Koruma Kurumu, **Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman**, https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, (Erişim Tarihi: 10.12.2021).

Korkmaz, İ., **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması,** Seçkin Yayıncılık, Ankara, 1. Baskı, 2017.

Kulezsa, J., **Transboundary Data Protection And International Business Compliance,** International Data Privacy Law, C. 4, S. 4, 2014, s. 298 – 306.

Kuner, C., **European Data Protection Law (Corporate Compliance and Regulation),** Second Edition, Oxford University Press, 2007.

Küzeci, E., **Kişisel Verilerin Korunması,** Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara 2019.

Lambert, P., **Understanding the New European Data Protection Rules**, Taylor & Francis, 2017.

Masoch, D., **Why Should Companies Invest in Binding Corporate Rules?** 2019, https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, (Erişim Tarihi: 02.12.2021).

Memiş, T., **Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni**, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt:3, Sayı:6, Aralık 2017, s.9-23.

Moerel, L., **Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers,** Oxford University Press, 2012.

Özkan, O., **Kişisel Verilerin Korunması,** Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Ankara 2020.

Sullivan, C., **EU GDPR Or APEC CBPR? A Comparative Analysis of The Approach of The EU And APEC To Cross Border Data Transfers And Protection of Personal Data InTheIotEra**, Computer Law and Security Review, C. 35, 2019, ss. 380-397.

Şimşek, O., **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul 2010.

Taştan, F. G., **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, İstanbul, On İki Levha Yayınları, 2. Baskı, 2017.

Toparlak, R. T., **Genel Veri Koruma Tüzüğünde Bağlayıcı Şirket Kuralları: Avrupa Birliği Hukukunda Uygulama,** Yayımlanmamış Yüksek Lisans Tezi, Türk-Alman Üniversitesi İstanbul 2021.

Turan, M., **Karşılaştırmalı Hukukta Kişisel Verilerin Korunması**, Seçkin Yayınları, Güncellenmiş 2. Baskı, Ankara, 2019.

Uncular, S., **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, Seçkin Yayıncılık, Ankara, Güncellenmiş ve Genişletilmiş 2. Baskı, 2018.

Üçüncü, S. H., **Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması,** İstanbul, On İki Levha Yayınları, 1. Baskı, 2019.

Yeditepe Üniversitesi, **Avrupa ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Uluslararası Sempozyumu Bildiri Özeti**, Bkz: https://law.yeditepe.edu.tr/sites/default/files/kvkk_-_kitapcik-v3.pdf,(Erişim Tarihi:15.11.2021).

Yılmaz, S. S., **Kişisel Verilerin Korunması Regülasyonu ve Unutulma Hakkı**, Terazi Hukuk Dergisi, C:13, S.142, Haziran 2018, s.116-121.

Yılmaz, S. S., "KVKK Uyum Sorunsalı: Veri Sorumlusu ve Veri İşleyen Kavramlarını İyi Anlamak", 14.05.2020, https://blog.lexpera.com.tr/kvkk-uyum-sorunsali-veri-sorumlusu-ve-veri-isleyen-kavramlarini-iyi-anlamak/, Erişim Tarihi: 24.01.2022

Yörük, O. D., (**AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması**, Yayımlanmamış Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi, İzmir, 2019.

Yücedağ, N., **Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri**, İÜHFM, 2017, C. 75, S. 2, s. 765-790.