T.C.
TÜRK - ALMAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK YÜKSEK LİSANS PROGRAMI

GENEL VERİ KORUMA TÜZÜĞÜNDE BAĞLAYICI ŞİRKET KURALLARI: AVRUPA BİRLİĞİ HUKUKUNDA UYGULAMA

YÜKSEK LİSANS TEZİ

Rüya Tuna TOPARLAK

DANIŞMAN
Doç. Dr. Mesut Serdar ÇEKİN

İSTANBUL, Şubat 2021

ÖNSÖZ

Ülkemizde hakkında yeni çalışılmaya başlanmış bağlayıcı şirket kurallarını tez konusu olarak belirlememi öneren ve içinde bulunduğumuz bu zor pandemi sürecinde bile bana zaman ayıran, kıymetli yorumlarıyla doğru yolu gösteren pek değerli danışmanım Doç. Dr. Mesut Serdar Çekin'e;

Tez hazırlığı sürecinde daima yanımda olan, cesaretlendiren, dinleyen ve yardımını esirgemeyen kıymetli meslektaşım ve annem Av. Sunahan Develioğlu'na;

İhtiyaç duyduğum her an beni en iyi şekilde sakinleştiren ve hep yanımda olan babam Onur Toparlak'a;

Son olarak bu zor dönemde gerek telefon gerek bilgisayar kameraları aracılığıyla bütün sıkıntılarımı dinleyip, destek olan çok değerli dostlarıma teşekkür ederim.

İÇİNDEKİLER

SAYFA NO

ÖZET

GENEL VERİ KORUMA TÜZÜĞÜNDE BAĞLAYICI ŞİRKET KURALLARI: AVRUPA BİRLİĞİ HUKUKUNDA UYGULAMA

Teknolojik gelişmelerin taşıdığı pek çok avantaj, kişisel verilerden oluşan bir ekonomi yaratmıştır. Günümüzde kişisel verilere ekonomik bir değer biçilmekte ve büyük global kuruluşlar, bundan çıkar sağlamaktadır. Hedeflenen, veri alışverişine dayalı dijital ekosistemin işlerliğini sağlarken, kişisel veriler üstündeki kişilik haklarını da global ölçekte korumak olmalıdır.

Çalışmamızda Avrupa Birliği hukukunda bu dengeyi sağlamayı hedefleyen *Binding Corporate Rules* incelenmiştir. Bu kuralları düzenleyip taahhüt eden grup şirketler veya ekonomik iş birliği halindeki teşebbüsler, farklı ülkelerde yer alan üyeleri arasında serbest veri akışı sağlayabilmektedir. Düzenlemeler, şeffaflığı ve şirketlerin hesap verilebilirliğini arttırırken, kişilerin mahremiyetini korumayı da taahhüt etmektedir. *Binding Corporate Rules* sayesinde grup şirketin farklı ülkelerde yer alan tüm üyeleri aynı veri koruma kurallarını benimsemektedir. Dolayısıyla *Binding Corporate Rules* düzenlemeleri Türkiye açısından da önem taşımaktadır. Öyle ki uluslararası bir grup şirketin Türkiye'deki üyesi, kendisine iletilen *Binding Corporate Rules'u* taahhüt edecektir.

Binding Corporate Rules'un içinde taahhüt edilen hükümleri anlamak adına, çalışmamız ilk olarak Genel Veri Koruma Tüzüğü'ndeki temel ilkeleri incelemiştir. Devamında Tüzüğün Avrupa Birliği dışına veri aktarımları için öngördüğü yöntemler karşılaştırılmış ve *Binding Corporate Rules'un* yeri belirlenmiştir. Bu taahhüt metinlerinin tarihçesi incelenmiş ve *Binding Corporate Rules* ile yerel hukuk arasındaki uyuşmazlık halinde izlenecek yöntemler ortaya konmuştur. *Binding Corporate Rules*

düzenlemelerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ilişkisi ele alınmıştır.

Çalışmamızın üçüncü bölümünde ise, Türk kanunlarından doğabilecek sorumluluk halleri belirlenmiştir. Gerek ilgili kişilerin tazminat istemleri gerekse idari para cezaları incelenmiştir. Üçüncü bölümün devamında Kişisel Verileri Koruma Kurumu'nun 10.04.2020 tarihindeki duyurusuyla Türk kanunları çerçevesinde düzenlediği Bağlayıcı Şirket Kuralları değerlendirilmiştir. Türk hukukuna uygun şekilde düzenlenecek Bağlayıcı Şirket Kurallarının avantajları, ne koşullarda ve hangi yöntemlerle uygulanacağı ortaya konulmuştur. Özellikle ispat aracı olarak kullanılabilmelerinin üzerinde durulmuştur. Tez çalışmasında Avrupa Birliği hukuku temel alınmıştır. Uluslararası nitelikteki İngilizce ve Almanca kaynaklar taranmıştır. İlgili görülen Avrupa Adalet Divanı, Avrupa Birliği Komisyonu, Çalışma Grupları, Avrupa Birliği Veri Koruma Kurulu ve üye devletlerin veri koruma otoriteleri kararları incelenmiştir.

Anahtar Kelimeler: *BCR, Yurtdışı Veri Aktarımı, Veri Koruması, Hesap Verilebilirlik*

Tarih:

ABSTRACT

BINDING CORPORATE RULES UNDER THE GENERAL DATA PROTECTION REGULATION: IMPLEMENTATION OF THE EU LAW

The technological advancements carry many advantages. However, these advantages have created a new economy based on personal data. In this current age, an economic value is assigned to personal data and global corporations are benefitting from it. The aim shall be to ensure a safe development in the digital ecosystem whilst providing adequate protection for personality rights.

This study focuses on Binding Corporate Rules in European Union Law, which aim to establish the above-mentioned balance. The group of undertakings or enterprises in joint economic activity that regulate the Binding Corporate Rules, benefit from the free movement of personal data within their group. Binding Corporate Rules provide accountability and ensure transparency in every member of the group, while also committing to protect data subjects' privacy. By virtue of Binding Corporate Rules, same binding data protection rules are adopted in every member of said group of undertaking, regardless of them being subject to differing local regulations. Thusly the importance of Binding Corporate Rules in Turkey becomes apparent. As the compliance of the Turkish member to such Binding Corporate Rules is also going to be obligatory.

In order to better grasp the individual commitments to be made under Binding Corporate Rules, this study shall begin with a general explanation regarding data protection principles. Following that, the data transfer rules under the General Data Protection Regulation shall be reviewed. Parallels between different options for appropriate safeguards for data transfers to third countries shall be drawn. In this regard, Binding Corporate Rules shall be compared to other appropriate safeguards. The history of Binding Corporate Rules shall be inspected and procedures to be followed in case of an incompatibility between the Binding Corporate Rules and local law, shall become

apparent. This point shall exhibit the relation between the Binding Corporate Rules and the Turkish Law on Protection of Personal Data numbered 6698.

The third chapter of this study shall focus on the liability. The data subjects' claim for damages as well as administrative fines shall be reviewed. The third chapter shall continue with the Binding Corporate Rules as they are adopted in the Turkish Law. Such that on 10.04.2020, Turkish Data Protection Authority has introduced Binding Corporate Rules as an adequate safeguard for data transfers under the Turkish Law on Protection of Personal Data numbered 6698. Our study shall inspect the advantages of this new safeguard under Turkish Law and the requirements they shall meet to be considered legally valid. In that, their use as an evidence for compliance shall be introduced. This study is focused mainly on European Union Law. For this purpose, the international literature both in English and in German have been reviewed. Decisions from European Court of Justice have been referred to, where needed. The relevant decisions and opinions to several data protection authorities as well as European Data Protection Board have been inspected.

Key Words: *BCR, Data Transfer to Third Parties, Data Protection, Accountability*

Date:

KISALTMALAR

AAD **:** Avrupa Adalet Divanı *(ing. European Court of Justice)*

ABA **:** Avrupa Birliği Antlaşması *(ing. Treaty on European Union)*

ABİHA **:** Avrupa Birliğinin İşleyişi Hakkında Antlaşma *(ing. Treaty on the Functioning of the European Union)*

ABTHB **:** Avrupa Birliği Temel Haklar Bildirgesi *(ing. EU Charter of Fundamental Rights)*

AEA **:** Avrupa Ekonomik Alanı *(ing. European Economic Area)*

AİHS **:** Avrupa İnsan Hakları Sözleşmesi *(ing. European Convention on Human Rights)*

APEC **:** Asia-Pacific Economic Cooperation (Asya-Pasifik Ekonomik İş birliği)

ASTB **:** Avrupa Serbest Ticaret Birliği *(ing. European Free Trade Assosiation)*

BCR **:** Binding Corporate Rules. Söz konusu kısaltma çalışmamızda Birlik hukuku açısından geçerli olarak düzenlenen Bağlayıcı Şirket Kurallarını ifade etmektedir.

BDSG **:** Bundesdatenschutzgesetz (Alman Federal Veri Koruma Kanunu)

BGB **:** Bürgerliches Gesetzbuch (Alman Medeni Kanunu)

BŞK **:** Bağlayıcı Şirket Kuralları. Söz konusu kısaltma çalışmamızda, Türk hukuku açısından geçerli olarak düzenlenen Bağlayıcı Şirket Kurallarını ifade etmektedir.

BVerfG **:** Bundesverfassungsgericht (Alman Federal Anayasa Mahkemesi)

CBPR **:** Cross Border Privacy Rules (Sınırötesi Gizlilik/Mahremiyet Kuralları)

Direktif **:** Gerçek kişilere ait kişisel verilerin korunması ve verilerin serbest dolaşımı hakkında 95/46/EC sayılı Avrupa Parlamentosu Direktifi

DSG **:** Bundesgesetz über den Datenschutz (19 Haziran 1992 tarihli ve 235.1 sayılı İsviçre Veri Koruma Yasası)

DSK **:** Konferenz der unabhängigen Datenschutzbehörden des Bundes und Länder (Federal Devlet ve Eyaletlerin Bağımsız Yetkili Veri Koruma Otoriteleri Konferansı)

EDÖB **:** Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (İsviçre Konfederasyonu Veri Koruma ve Kamu Görevlisi)

ETK **:** 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

GVKT **:** 2016/679 sayılı Avrupa Parlamentosu Genel Veri Koruma Tüzüğü

İK **:** 4857 sayılı İş Kanunu

Kurul **:** Kişisel Verilerin Korunması Kurulu

Kurum **:** Kişisel Verilerin Korunması Kurumu

KVKK **:** 6698 sayılı Kişisel Verilerin Korunması Kanunu

MMR **:** Multimedia und Rechts Zeitschrift (Alman Multimedya ve Hukuk Gazetesi)

TBK **:** 6098 sayılı Türk Borçlar Kanunu

TCK **:** 5237 sayılı Türk Ceza Kanunu

TMK **:** 4721 sayılı Türk Medeni Kanunu

TTK **:** 6102 sayılı Türk Ticaret Kanunu

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

WP **:** Working Paper (Avrupa Komisyonu Çalışma Raporu)

GİRİŞ

Verilerin toplanması, saklanması ve ekonomik açıdan değerlendirilmesi fikri çağlar öncesine kadar uzanmaktadır.[1] Dijitalleşmeyle işletmeler, devletler ve toplum şiddetli veri akışının yarattığı muazzam imkânlara erişmiş ve dünya ekonomisi, veri odaklı bir modele dönmüştür.[2] Güncel hızımızla günde 2.5 kentilyon bayt veri ürettiğimiz ve tarih boyu kaydedilen verilerin 90%'ının son iki yıl içerisinde üretildiği göz önüne alındığında[3], Nikola Tesla'nın ünlü sözü akla gelmektedir; *'Kablosuz teknoloji mükemmel şekilde uygulanabilir hale getirildiğinde, dünyanın tamamı kocaman bir beyne dönüşecek ve her şey gerçek, ritmik bir bütünün parçaları haline gelecektir. Bunu gerçekleştirmek için kullandığımız cihazlar ise son derece basit ve küçük aletler olacaktır.'*[4]

Bilgi toplumu içerisindeki büyük ve hızlı veri akışı, şüphesiz ki toplumsal ilerleme ve ekonomik gelişim açısından pek çok fayda sağlamıştır. Ancak söz konusu toplumsal ilerleme, ne yazık ki kişilerin mahremiyetine dair endişeleri de beraberinde getirmiştir. Gelişen dünyanın getirdiği endişelere cevap vermek için, kişisel verilerin korunması hukuku açısından yapılan ilk düzenleme, 1981 yılındaki 108 sayılı 'Kişilerin Otomatik Yollarla Verilerin İşlenmesine Karşın Korunmasına Dair Avrupa Konseyi Konvansiyonu' olmuştur.[5] Konvansiyon sonrasında, kişisel verilerin anayasal olarak temel hak mertebesinde korunması ise Alman Anayasa Mahkemesi ('BVerfG') Nüfus Sayımı Kararı[6] ile sağlanmıştır. Kişisel veriler için self-determinasyon *(alm. informationelles Selbstbestimmungsrecht)* olarak belirlenen bu hak, kişilerin kendilerine

[1] A Brief History of Big Data Everyone Should Read https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/ Erişim Tarihi: 09.01.2020
[2] The Data Deluge https://www.economist.com/leaders/2010/02/25/the-data-deluge Erişim Tarihi: 09.01.2020
[3] How Much Data Do We Create Everyday? https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#26747cd960ba Erişim Tarihi: 09.01.2020
[4] KENNEDY, B. John *'When Woman is Boss: An Interview with Nikola Tesla'*, Colliers, January 30, 1926.
[5] Personal Data Protection Factsheet of the European Parliament https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection (Erişim Tarihi: 18.04.2020)
[6] BVerfG 65,1 Sayılı 15.12.1983 tarihli karar.

ait verilerin akıbetine karar verebilme haklarını anayasal olarak düzenlemiştir. Nüfus sayımı kararından sonra, 2000 yılında ilan edilen Avrupa Birliği Temel Haklar Bildirgesi ('ABTHB') ile kişisel verilerin korunması, Avrupa Birliğinin ('Birlik') genelinde temel hak olarak tanınmıştır.

Birlik hukukundaki veri koruması mevzuatlarına bakıldığında, gerek mülga 95/46 sayılı Avrupa Parlamentosu Direktifi ('Direktif)[7], gerek güncel Genel Veri Koruma Tüzüğü'nü ('Tüzük' 'GVKT')[8] kısıtlayıcı düzenlemeler olarak değerlendirmek yanlıştır. Şöyle ki, korunması amaçlanan kişilik hakkı yanında kişilerin mahremiyetidir. Mahremiyet kavramı, Birlik hukukunca benimsenmiş temel insan hakları değerlerini gözeten, etik bir veri akışını gerektirmektedir.[9] Nitekim çalışmamızda inceleneceği üzere, Tüzüğün önemli amaçlarından biri de budur.[10]

Ekonomik ilerlemeyi sağlarken etik kurallarını korumak adına getirilen Birleşmiş Milletler'in 2008 tarihli İşletme ve İnsan Hakları Çerçeve Önerisi[11], üç temel nokta içermektedir. Buna göre devletlerin, işletmeler dahil üçüncü kişilerin insan hakkı ihlali teşkil edebilecek faaliyetlere karşı koruma; şirket ve işletmelerin kişilik ve insan haklarına saygı duyma; mağdurlar için işler bir hukuki çare ve tazminat sistemi öngörme yükümlülükleri vardır.[12]

Bu çerçeve öneriyi izleyen yıllarda, özellikle veri ekonomisi ve uluslararası ticaretin hız kazanmasıyla kişisel verilerin uluslararası aktarımları çoğalmıştır. Böylece yukarıda bahsi geçen çerçeve önerinin, veri odaklı ekonomide de geçerliliğinin sağlanması gündeme gelmiştir. Tüzüğün yürürlüğe girmesiyle de Birleşmiş Milletler'in çizdiği çerçevenin uygulanmasını sağlayan somut ilke ve mekanizmalar benimsenmiştir.[13]

---

[7] 24 Ekim 1995 Tarihli ve 95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi.
[8] 27 Nisan 2016 Tarihli ve 2016/679 sayılı Avrupa Parlamentosu ve Konseyi Tüzüğü.
[9] RICHARDS, M. Neil, KING, H. Jonathan (2014), 'Big Data Ethics', Wake Forest Law Review, C. 49, s. 395-432.
[10] MARTIN, Nicholas, FRIEDEWALD, Michael (2019), 'Warum Unternehmen Sich Nicht an Recht und Gesetz Halten', Datenschutz und Datensicherheit, C. 43, s. 493-497.
[11] The UN "Protect, Respect and Remedy" Framework for Business and Human Rights https://www.business-humanrights.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf Erişim Tarihi: 07.06.2020.
[12] Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği, 'Guiding Principles on Business and Human Rights', New York and Geneva 2011 https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf Erişim Tarihi: 07.06.2020.
[13] KULEZSA, Joanna (2014), 'Transboundary Data Protection and International Business Compliance', International Data Privacy Law, C. 4, S. 4, s. 298 – 306.

Şüphesizdir ki, şirketlerin hesap verebilirliğinin bir yükümlülük olarak öngörülmesi, kişilerin mahremiyetinin korunmasını sağlayan en önemli ilkelerdendir. Hesap verilebilirlik, yürürlükteki veri koruması kanun ve kurallarının şirketçe uygulanmasını ve bunların uygulandığının her an için ispat edilebilir olmasını ifade etmektedir.[14] Hesap verilebilirliği sağlamak adına Tüzük'te idari ve teknik önlemler, risk analizleri vb. pek çok yükümlülük öngörülmüştür.[15] *Binding Corporate Rules ('BCR')* alınacak bu idari ve teknik önlemleri açıkça düzenlemekte ve taahhüt etmektedir. Dolayısıyla hesap verilebilirliği de arttırmaktadır.

Binding Corporate Rules'un esas düzenlenme amacı, bu metni hazırlayıp taahhüt eden global grup şirket bünyesinde serbest veri aktarımını sağlamasıdır. Dolayısıyla *Binding Corporate Rules* Tüzük içerisinde, üçüncü ülkelere veri aktarımı için öngörülen uygun güvenlik önlemleri altında düzenlenmiştir. Ancak çalışmamızda inceleneceği üzere *Binding Corporate Rules* pek çok başka avantaja da sahiptir. Öyle ki, grup şirket bünyesinde yürütülecek veri koruması hukuku uyumunun temelini oluşturabilecek, yükümlülüklerin yerine getirilmesini ve ispatı sağlayabilecektir.[16]

Veri işleme faaliyetleri günümüzde ülke ve kıta sınırlarını aşmaktadır. Hızlı ve pratik biçimde verileri üçüncü ülkelere taşıyabilmek hem bilgi toplumu hem de ticaret hayatı için önem taşımaktadır.[17] Dolayısıyla çok uluslu bir grup şirket topluluğunca verilecek benzer bir taahhüdün, Türk veri koruması hukukuna sağlayabileceği yarar da tespit edilmiş ve Kişisel Verileri Koruma Kurumu ('Kurum') tarafından 10.04.2020 tarihinde, Türkiye'de yerleşik veri sorumlularınca Bağlayıcı Şirket Kuralları ('BŞK') düzenlenebileceği öngörülmüştür. Uygulamada taşıyacağı önem nedeniyle çalışmamızda, Türk hukuku açısından geçerli Bağlayıcı Şirket Kurallarında hangi hususların taahhüt edileceği ve bu taahhütlerin uluslararası etkisi de araştırılmıştır.

---

[14] Centre for Information Policy Leadership, 'The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society', 23.07.2018 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf Erişim Tarihi: 07.06.2020.

[15] Age.

[16] United Nations Conference On Trade And Development, 'Data Protection Regulations And International Data Flows: Implications For Trade And Development' New York and Geneva 2016 https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf Erişim Tarihi: 07.06.2020.

[17] *Kühling ve Raab'a ait kısım,* KÜHLING Jürgen, BUCHNER Benedikt, Datenschutz-Grundverordnung Kommentar, 2. Auflage, C.H. Beck, München 2018, s.5.

Belirtmek gerekir ki çalışmamızda ayırt edici olması açısından, Tüzüğe göre düzenlenmiş *Binding Corporate Rules* İngilizce orijinal adı ile anılmıştır. Bağlayıcı Şirket Kuralları ise, 6698 sayılı Kişisel Verilerin Korunması Kanunu ('KVKK')[18] uyarınca Kurum tarafından oluşturulan alternatif uygun güvenlik önlemini ifade etmektedir. Tüzüğün düzenlediği, ancak Türk kanunlarında karşılığı bulunmayan diğer taahhütler, yöntemler yahut kavramlar, benzer bir karışıklığa sebep vermeyeceği için, doktrinde ve uygulamada benimsenmiş tercüme Türkçe terimler ile anılacaktır.

Binding Corporate Rules çok uluslu grup şirket üyelerinin, Tüzüğün öngördüğü yükümlülükleri yerine getireceklerini taahhüt etmektedir. Bunun yanında somut çok uluslu şirketin kendi ihtiyaçları, yapısı ve işleyişi gözetilerek düzenlenen hükümler de içermektedir. Bunun haricinde *Binding Corporate Rules* hazırlanırken grup şirket üyelerinin tâbi oldukları yerel mevzuat da araştırılmaktadır. Bundandır ki doğru uygulandıkları hallerde düzenleyenlerin veri koruması kanunlarına tam uyumunu sağlamakta ve ispat aracı olarak kullanılabilmektedir. Çalışmamızda *Binding Corporate Rules'un* tüm amaç ve avantajları ayrıntısıyla incelenecek, uygulamada sağladığı yararlar belirlenecektir.

GVKT md. 32 uyarınca, veri sorumlusu ve işleyenin riski belirleyerek, orantılı güvenlik önlemleri almaları beklenmektedir.[19] Böylece sorumluluk, şirketlere kaydırılarak işledikleri verilerin niteliklerini belirlemeleri ve veri sahipleri için meydana gelebilecek riskleri değerlendirmeleri öngörülmektedir. Şöyle ki, veri sorumlularınca yükümlülüklerin yerine getirilmesi ve veri koruma otoritelerince gerekli kontrollerin yapılması kaydıyla daha işlevsel bir veri koruma sisteminin yerleştirilmesi amaçlanmıştır.[20] *Binding Corporate Rules* veri sorumlularına belli bir serbesti tanıdığından bu amaca da hizmet eden bir sistemdir.

Birlik hukukunda *Binding Corporate Rules* terimi, Direktif döneminde aktif olan Md. 29 Çalışma Grubu[21] kararlarında, doktrinde ve uygulamada kullanılmaktaydı. Ancak ilk defa Tüzük ile mevzuat içerisinde düzenlenmiştir. *Binding Corporate Rules* Tüzüğün öngördüğü bütün yükümlülükleri taahhüt ederek Tüzüğe uyumu sağladığından,

[18] 24 Mart 2016 Kabul Tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu.
[19] KREMPELMEIER Sebastian, STAUDINGER Isabel, WEISER Katharina, Datenschutzrecht nach der DSGVO – zentrale Fragenstellungen, Jan Sramek Verlag, Salzburg, Avusturya 2018, s.108.
[20] QUELLE Claudia (2018), '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.
[21] 95/46 sayılı Direktif'in 29. Maddesi uyarınca kurulmuş Veri Koruma Çalışma Grubudur.

çalışmamızda ilk olarak Tüzüğün genel hatları çizilecektir. Öyle ki, *Binding Corporate Rules'u* düzenleyen maddeler, Tüzüğün genel mantığına, benimsediği ilkelere ve veri güvenliği prensiplerine atıf yapmaktadır.

Tam da bu nedenle, çalışmamızın ilk bölümünde, Tüzük ile sağlanmaya çalışan veri güvenliği standartları, genel ilkeler ve amaçlar saptanacaktır. Birinci bölümün devamında, Tüzüğün uygulama alanı belirlenerek uluslararası uygulanma halleri ortaya konulmaya çalışılacaktır. İlk bölümün son kısmında ise, Tüzüğün Birlik dışına veri aktarımı için getirdiği güvenli ülke listesi ve uygun güvenlik önlemleri incelenecektir. Bu önlemler altında *Binding Corporate Rules* dahil öngörülen tüm yöntemler karşılaştırılacak ve avantajları belirlenecektir.

Çalışmamızın ikinci kısmı ise *Binding Corporate Rules'un* Birlik hukukundaki gelişimi ile başlayacaktır. Tüzüğün öngördüğü şekliyle *Binding Corporate Rules* içeriğinde dair taahhüt edilmesi gereken hususlar belirlenecektir. Bu taahhüdü veren çok uluslu şirketlerin sorumlulukları ortaya konulacaktır. Grup şirketin üçüncü ülkelerdeki üyelerinin tâbi oldukları yerel hukuk ile taahhüt ettikleri *Binding Corporate Rules* arasındaki ilişki belirlenecektir.

İkinci bölümün son kısmında ise, Birlik dışından seçilen üç farklı örnek ülke ve hukuk düzenindeki *Binding Corporate Rules'a* benzer taahhütlere de değinilecektir. Bu başlık altında Birlik'ten yakın zamanda ayrılan Birleşik Krallık örneği incelenecek ve halihazırda onaylanmış *Binding Corporate Rules'un* akıbeti belirlenecektir. İnceleme için seçilen bir başka ülke de Birliğe üye olmayan ancak Avrupa Serbest Ticaret Birliği içerisindeki İsviçre'dir. Son olarak Asya-Pasifik Ekonomik İş Birliği'nin hazırladığı Sınırötesi Mahremiyet Kuralları *(ing. Cross Border Privacy Rules)* değerlendirilecektir. Benzer bir alanı hesap verilebilirlik üzerinden düzenleyen bu kurallar da çalışmamızda incelenecek ve *Binding Corporate Rules* ile karşılaştırılacaktır.

Çalışmanın üçüncü ve son bölümü ise Türk hukukuna odaklanacak ve *Binding Corporate Rules'u* çift yönlü bir biçimde ele alacaktır. İlk olarak, çok uluslu bir grup şirketin Türkiye'deki üyesinin verdiği *Binding Corporate Rules'dan* doğan taahhütler ve yükümlülükler belirlenecektir. Bu yükümlülüklerin Türk hukuku ile ilişkisi değerlendirilecektir. Böylece gerek ana şirketin gerekse Türkiye'deki üyenin sorumluluk halleri ortaya konulacaktır. İkinci olarak ise, Türk hukuku kapsamında geçerli olarak düzenlenebilecek Bağlayıcı Şirket Kuralları incelenecektir. Kuralların hangi şirket

yapılarınca ne hallerde düzenlenebilecekleri, avantajları ve içeriğinde taahhüt edilmesi gereken hususlar açıklanacaktır. Böylece üçüncü bölüm altında hem *Binding Corporate Rules* hem de Bağlayıcı Şirket Kurallarının uygulamasının somut olarak belirlenmesi hedeflenmektedir.

BÖLÜM 1. AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ

Birlik hukukunda Tüzük öncesi dönemde yürürlükte olan Direktif, üye devletler için çerçeve düzenleme niteliğindeydi. Bu nedenle her ülke kendi veri koruma yasasını uygulamaktaydı. Bu durum hem Birlik içindeki hem de üye devletlerle ile iş yapan diğer ülkelerdeki sorumlular için zorluk yaratmaktaydı. Zira, verilerin toplandığı, işlendiği, aktarıldığı ve/veya depolandığı her bir Birlik üyesi devletin yerel mevzuatlarına uyum gerekiyordu.

Uyulması gereken birçok farklı mevzuatın varlığı hem Birlik içerisindeki hem de üçüncü ülkelere veri akışını uzun ve karışık bir hale getirmekteydi. Bunun yanında şeffaflık Birlik içerisinde aynı esaslarda belirlenmediğinden, veri işleme sürecinin ilgili kişilerce erişilmesi ve öngörülmesi daha zordu. Bu durum kişilik haklarının bir parçası olan kişisel veriler için self-determinasyon hakkının, tam anlamıyla kullanılamamasına yol açmaktaydı.

Bu nedenlerle yıllar içerisinde ilerleyen veri koruması hukuku, Birlik'teki veri işleme süreçlerinde standartlaşmayı gerektirmiştir. Öyle ki yeknesak ve doğrudan uygulanabilir bir düzenlemeye ihtiyaç duyulmuştur. 27 Nisan 2016'da yayınlanan Tüzüğün amacı, Birlik içerisinde kişisel verilerin korunmasına ilişkin doğrudan uygulanabilen tek bir mevzuat getirmektir. Böylece üye devletlerin her birinde kişisel veri işleyen bir veri sorumlusunun, 27 farklı yerel mevzuata uyum sağlaması gerekmeyecektir. Birlik içerisinde serbest veri dolaşımı; daha hızlı ve güvenilir bir ticari hayatı sağlanacaktır.

Tüm üye devletlere aynı veri koruması kurallarının uygulanması, Avrupa iç piyasasında eşdeğer rekabeti de güçlendirmektedir. Diğer bir önemli amaç Birlik içindeki gerçek kişilerin, Avrupa Birliği Temel Haklar Bildirgesinde kişisel verilere ilişkin belirlenen kişilik haklarının[22] hem Birlik içinde hem de verilerin aktarıldığı üçüncü ülkelerde korunmasıdır.

[22] Tüzüğün düzenlenme gerekçelerinden biri olarak ABTHB md. 8 ve ABIHA md. 16 ile koruma altına alınan kişisel verilerin korunması hakkına dair ayrıntılı bilgi için bkz. *Buchner'e ait kısım,* KÜHLING, BUCHNER, age, s. 94.

Birlik içerisinde kişisel verilerin işlenmesine dair kabul edilen anlayış, veri işleme ilkelerinin daima korunmasını öngörmektedir. Bunun yanında, eğer kanunda öngörülen gerekçelerden biri yoksa, kişisel veri işlemek yasaktır. Veri işleme ilkelerine, verilerin aktarılması, silinmesi dahil işleme faaliyetinin tamamı boyunca uyulması gerekmektedir. Elbette ki söz konusu ilkeler, *Binding Corporate Rules* içerisinde de önem taşımaktadır. Hazırlanacak metinler, ilkeleri taahhüt etmekte ve hatta bu ilkeler üzerinden inşa edilmektedir. Çalışmanın ileri kısımlarında *Binding Corporate Rules* için verilecek taahhütlerde atıf yapılacak veri işleme ilkeleri, Tüzüğün genel işleyişini de ortaya koymaktadır. Dolayısıyla veri işleme ilkeleri çalışmamız için başlangıç noktası olacaktır.

1.1. GENEL VERİ İŞLEME İLKELERİ

Tüzüğe uygun bir veri işleme faaliyeti için genel veri işleme ilkelerine uyulması ve 6. maddede düzenlenen hukuka uygunluk sebeplerinden en az birinin varlığı gerekmektedir. GVKT md. 5 altında öngörülen genel veri işleme ilkeleri esasında, Avrupa Birliğinin İşleyişi Hakkında Antlaşma ('ABİHA') md. 16/1 ve ABTHB md. 8/2'nin somut bir görünümüdür. Şöyle ki ABTHB md. 8/2 kişisel verilerin korunmasını düzenlerken, ABİHA md. 16/1 Avrupa Konseyi'nin Antlaşmalarda öngörülen koşulların uygulanması için politika belirleyeceğini öngörmektedir.

Genel veri işleme ilkeleri Tüzük içerisinde, mülga Direktifteki karşılıklarının[23] aksine doğrudan uygulanabilir yükümlülükler olarak düzenlenmiştir. Veri işleme ilkeleri öncelikli olarak veri sorumlusunu bağlamaktadır. Dolayısıyla veri işleme sürecinde GVKT md. 28 uyarınca bir veri işleyen mevcut olsa dahi ilkelerin korunduğuna dair ispat yükü GVKT md. 5/2 uyarınca veri sorumlusunun üstündedir.[24]

1.1.1. Hukuka Uygun ve Adil İşleme ile Şeffaflık İlkesi

Hukuka uygun ve adil işleme ile şeffaflık ilkesi *(ing. lawfulness, fairness and transparency)* GVKT md. 5/1/a'da düzenlenmektedir. Her ne kadar bu üç ilke birbirileriyle ilişkili olsa da uygulanma açısından birbirilerine bağlı değildirler. Öyle ki,

[23] İlkelerin bazıları Direktif md. 6'da düzenlenirken, bazıları da Direktif'in farklı maddelerinden ve içtihattan çıkarılabilmektedir. Şeffaflık ilkesi ise, bir yenilik olup ilk düzenlemesini Tüzük'te bulmuştur.
[24] *Herbst'e ait kısım,* KÜHLING, BUCHNER, age, s. 212.

bu ilkelerin her birine riayet etmek için farklı yükümlülükleri yerine getirmek gerekmektedir.

Kanun lafzında geçen ilk ilke olan hukuka uygun veri işleme prensibi, iki şekilde anlaşılabilir. Dar anlamı, hukuka uygun veri işleme için özellikle md. 6/1'de öngörülen şekillerden birinin[25] sağlanmasıdır. İlkenin geniş anlamı ise, veri işleme süreçlerinde, Tüzük ve yerel mevzuatta öngörülen bütün yükümlülüklerinin yerine getirilmesidir. Hukuka uygunluk ilkesi Türk hukukundaki karşılığını KVKK md. 4/2/a'da bulmaktadır. Tüzük ile paralel biçimde Kişisel Verilerin Korunması Kanunu da kural olarak kişisel verileri işlemenin yasak olduğunu belirtmekte ve ancak Kanun'da açıkça izin verilen hallerde meşru olacağını düzenlemektedir.[26]

Adil işleme ilkesi ise, verisi işlenen kişinin işleme faaliyeti sonucunda dezavantaj yaşadığı her hal için, genel hüküm niteliğindedir. Bu ilke, yazılı bir kuralı ihlal etmemek koşuluyla Tüzüğün amacı dahilinde, kişisel verisi işlenen ilgili kişi ile veri sorumlusu arasındaki güç dengesini korumak için kullanılmaktadır. Şöyle ki adil veri işleme ilkesi, pazarlık gücü daha az olan ilgili gerçek kişi lehine yorum aracı işlevi görmektedir.[27] Alman doktrinindeki bir görüşe göre, adil işleme ilkesini *(alm. Treu und Glauben)* özel hukukun genel ilkelerinden olan ve BGB md. 242'de[28] düzenleme bulan dürüstlük kuralının bir görünümü olarak algılamak mümkündür.[29] Güncel görüş ise bu ilkenin, özellikle veri sorumlularının kanundan doğan haklarını kullanırken ilgili kişilere karşı adil davranma yükümlülüğünü düzenlediğini belirtmektedir.[30]

Tüzükteki adil veri işleme, KVKK md. 4/2/a'da dürüstlük kurallarına uygunluk ilkesi ile karşılık bulmaktadır. Ancak burada belirtmek gerekir ki bu ilke, TMK md. 2/2'de düzenlenen ve yukarıda açıklanmış BGB md. 242'nin karşılığı olan dürüstlük kuralıyla eş anlamlı değildir.[31] Kişisel Verilerin Korunması Kanunu daha ziyade adil bir kullanımdan bahsetmektedir. Türk doktrininde bu ilkenin özellikle tarafların çatışan

[25] Hukuka uygun veri işlenmesi için, kişinin rızası yoksa GVKT md. 6/1b-f bentlerinde öngörülen hallerden birinin varlığı gerekmektedir.
[26] ÇEKİN S. Mesut, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 3. Baskı, Onikilevha Yayınları, İstanbul, Türkiye 2020, s. 69, dn. 141.
[27] *Herbst'e ait kısım,* KÜHLING, BUCHNER, age, s. 217.
[28] BGB md. 242 *'Borçlu ifayı, işlem teamülü çerçevesinde doğruluk ve dürüstlük nasıl gerektiriyorsa o şekilde gerçekleştirmekle yükümlüdür'.*
[29] *Brühmann'a ait kısım*, GRABITZ Eberhard, HILF Meinhard, das Recht der Europäischen Union, 40. Auflage, C.H. Beck, München 2009, Art 6, RL 95/46/EG Rn. 5.
[30] ÇEKİN 2020, age, s. 70, dn. 142.
[31] Age.

menfaatlerini dengelemeyi amaçlayan hükümler çerçevesinde önem kazanacağı, rızanın özgür iradeye dayalı olup olmadığının ve gerekli tedbirlerin alınıp alınmadığının değerlendirmesinde gündeme geleceği belirtilmektedir.[32]

Direktif döneminde hukuka uygun ve adil veri işleme ilkeleri özellikle, gizli tutulan veri işleme faaliyetlerini kapsam dışı bırakmayı sağlamaktaydı.[33] Veri işleme faaliyetlerinde gösterilmesi gereken şeffaflık ise ayrıca düzenlenmeyip bu ilke içerisinde değerlendirilmekteydi.[34] Tüzük, şeffaflık ilkesini ayrıca düzenleyerek bu ilkenin gereklerinin yerine getirilmesi için ayrı yükümlülükler düzenlemiştir. Böylece hukuka uygun ve adil veri işleme ile şeffaflığın sağlanması ilkeleri birbirinden ayrılmış, her birinin yerine getirilmesi için gereken yükümlülükler açık bir şekilde belirlenmiştir.

Şeffaflık Türk hukukunda ise, KVKK md. 4/2/a hukuka ve dürüstlük kurallarına uygun olma ilkesi içerisinde yer almaktadır. KVKK md. 10 ve 11'de ilgili kişilere yapılacak açıklamalar düzenlenirken, yapılacak bilgilendirmenin şekli Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ[35] içerisinde belirlenmiştir.

Şeffaflığın, kişisel veriler için self determinasyon hakkının kullanılabilmesi için önemli olduğu söylenmektedir.[36] Öyle ki maddi ve şekli boyutundan bahsedilebilecek şeffaflık ilkesi, ilgili kişilere hangi bilgilerin ne şekilde iletileceğini düzenlemektedir.[37] GVKT md. 13 ve 14 veri sorumlusunun kimliği, işleme faaliyetinin kapsamı ve riskleri, ilgili kişi haklarının ve bu hakların nasıl kullanılacağı gibi ilgili kişilere açıklanması zorunlu bilgileri ayrıntısıyla düzenlemektedir.

GVKT md. 12/1 ise açıklanacak bilgilerin sade bir dille yazılmasını ve ilgili kişilere kısa ve öz, anlaşılır ve kolay erişilebilir biçimde iletilmesini öngörmektedir. Maddenin devamında bu bilgilerin ilgili kişilere yazılı biçimde yahut uygun görüldüğü takdirde elektronik şekilde iletilmesi düzenlenmiştir. GVKT gerekçe md. 39'da

---

[32] Age.
[33] DAMMAN Ulrich, SIMITIS Spiros, Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlag, Baden-Baden 2011, s. 297 vd.
[34] ÇEKİN 2020, s. 70, kn. 142.
[35] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ https://kvkk.gov.tr/Icerik/5443/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESINDE-UYULACAK-USUL-VE-ESASLAR-HAKKINDA-TEBLIG Erişim Tarihi: 04.06.2020.
[36] von LEWINSKI Kai, die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, Mohr Siebek Verlag, Tübingen, Almanya 2014, s.50.
[37] ÇEKİN 2020, s. 79, kn. 166 vd.

belirtildiği üzere, veri işleme faaliyetine dair yapılacak bilgilendirmenin kolay erişilebilir ve anlaşılabilir olması gerekmektedir. Benzer şekilde GVKT gerekçe md. 58 de şeffaflık ilkesine atıf yapmakta ve iletilecek bilgilerin kolay anlaşılması için görseller kullanılabileceğini, bu bilgilerin elektronik yollarla iletilebileceğini veya web sitelerinde ilan edilebileceklerini örnek vermektedir.

GVKT gerekçe md. 78'de şeffaflık sağlanırken ilgili kişilerin haklarının korunması için idari ve teknik önlemler alınması öngörülmektedir. Bu önlemler *inter alia* örnek verildiği şekliyle, kişisel veri işlenmesinin en aza indirilmesi, kişisel verilerin mümkünse psödönim kullanarak işlenmesi, kişisel verileri işleme sürecinde tam bir şeffaflık sağlanması, ilgili kişinin veri işleme süreçlerine erişebilmesi, veri sorumlusunun güvenlik önlemleri yaratıp geliştirmesidir.

GVKT gerekçe md. 78'de idari ve teknik önlemlerin alındığını göstermesi için, verilerin tasarım itibariyle ve varsayılan olarak korunmasını *(ing. data protection by design and default)* benimseyen politikalar hazırlanması öngörülmüştür. Karmaşık çok uluslu şirket yapılarına ait tüm bu bilgileri, kolay erişilebilir şekilde, tek bir yerde, açık olarak düzenleyen *Binding Corporate Rules* benzeri taahhütler, şüphesiz ki bu açıdan önemlidir. Dolayısıyla *Binding Corporate Rules'un* bu ilkeye hizmet ettiğini söylemek mümkün olacaktır.

Verilerin tasarım itibariyle korunması GVKT md. 25/1'de düzenlenmektedir. Bu ilke, yetkili kişiler (ör. uygulama geliştiriciler) tarafından, veri işleme faaliyetinin yürütüleceği sistemin (ör. bilgisayar programı, uygulama) geliştirilmeye başlanmasından itibaren, veri işleme faaliyeti devam ettiği sürece devam edecek şekilde, veri koruması kurallarının dikkate alınmasını gerektirmektedir. Öyle ki, söz konusu geliştiriciler tarafından uygulama, servis ve ürün geliştirme sürecinde, veri sorumlularının ve işleyenlerinin tüm yükümlülüklerini kolayca yerine getirebilecekleri teknolojiler benimsenmelidir. Geliştirilen bu teknolojiler, uygulama, süreç ve ürünlerin içerisine dahil edilmelidir. İlkenin veri sorumluları açısından veri işleme faaliyetindeki somut uygulaması ise, verilerin simetrik ya da asimetrik biçimde şifrelenmesi, ayrıştırılması gibi örneklerle sağlanabilir. Bunun yanında kişisel verilerle temas eden çalışanlar arasında bir

emir komuta zinciri oluşturulması, eğitimler verilmesi ve çalışanların testlere tâbi tutulmaları benzeri idari tedbirler de alınmalıdır.[38]

Verilerin varsayılan olarak korunması *(ing. data protection by default)* ise GVKT md. 25/2'de düzenlenmektedir. İlke ilgili kişilerin kendilerine dair yapılan veri işleme faaliyetleri için belirlenen önlemleri, kendi haklarını engelleyecek yahut hakların kullanımını zorlaştıracak biçimde değiştirememelerini belirtmektedir. Öyle ki veri sorumlusu aldığı önlemlerin değiştirilmemesi için, önlemlerin veri işleme amaç ve kapsamlarının tümünde geçerli olmasını sağlamalıdır.[39]

1.1.2. Amaçla Sınırlılık İlkesi

Amaçla sınırlılık ilkesi *(ing. purpose limitation)* GVKT md. 1/b'de düzenlenmektedir. Veri koruma hukukunun temellerinden biri olarak nitelendirilen amaçla sınırlılık ilkesi, veri işleme faaliyeti başlamadan evvel, hangi verilerin toplanıp ne süreyle işleneceğinin belirlenmesini gerektirmektedir.[40]

Belirlenecek amaçların hukuka uygun şekilde öngörülmesi gerekmektedir. Md. 29 Çalışma Grubu'nun yayınladığı bir görüşte, *'kişilerin deneyimini iyileştirmek, pazarlama amacı, IT-güvenlik amacı'* gibi geniş ifadelerin geçerli amaçlar olmadığı belirtilmektedir.[41] Tüzüğün lafzından da anlaşıldığı üzere, kişisel verileri işleme amaçlarının açık ve belirli şekilde yazılması gerekmektedir. Bunun yanında, belirlenen amaçlarla ilişkili, uyumlu sayılabilecek diğer amaçlar için de işleme mümkün kılınmıştır.[42] Veri sorumluları, diğer amacın belirlenen ile uyumlu olup olmadığına ilişkin değerlendirmeyi GVKT md. 6/4'de yer alan kriterlere göre yapacaktır.

Belirlenen amaçlarla ilişkilendirilemeyecek yeni amaçlarda, Tüzük terminolojik bir ayrıma gitmekte ve ilave veri işleme faaliyetinden bahsetmektedir *(ing. further processing, alm. Weiterverarbeitung).* Eğer ilave veri işleme faaliyeti söz konusuysa Md. 29 Çalışma Grubu görüşünce, hukuka uygun veri işleme faaliyeti için öngörülen yükümlülüklerin yeni baştan yerine getirilmesi gerekmektedir.[43] GVKT md. 6'da

---

[38] *Mantz ve Marosi'ye ait kısım*, SPECHT Louisa, MANTZ Reto, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, C.H: Beck, München, Almanya 2019, s. 77.
[39] Age.
[40] *Herbst'e ait kısım*, KÜHLING, BUCHNER, age, s. 218.
[41] Art. 29 Working Party Opinion 03/2013 on purpose limitation WP 203, 02.04.2013.
[42] *Herbst'e ait kısım*, KÜHLING, BUCHNER, age, s. 224.
[43] Art. 29 Working Party Opinion 03/2013 on purpose limitation WP 203, 02.04.2013.

düzenlenen bu sebeplerden örneğin rıza seçildiyse, rızanın yeni baştan alınması gerekecektir.

Amaçla sınırlılık ilkesi Türk hukukunda KVKK md. 4/2/ç'de işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ifadesiyle mevcuttur. Bu ilkenin tüzüğe paralel bir düzenleme içerdiği söylenebilecektir. Kişisel veriler ancak belirli, açık ve hukuka uygun amaçlar için işlenebilmektedir. Birlik hukukuna paralel bir şekilde Türk hukukunda da amaçların baştan, somut bir şekilde belirlenmesi gerekmektedir. Somutluk derecesi işlenen verilerin niteliğine ve verilerin nasıl toplandığına göre belirlenecektir.[44] Bu anlamda karmaşık veri işleme faaliyetleri için daha detaylı açıklamalar gerekmektedir.[45]

İleri veri işleme faaliyetlerine dair açıklama ise Kişisel Verilerin Korunması Kanunu gerekçesinde yer almaktadır. Öyle ki yeni bir amaç için veri işleme halinde yeniden rıza alınması gerektiği belirtilmektedir. Bu noktada yukarıda açıklandığı şekliyle Tüzüğün yaptığı ayrımın, Türk hukuku açısından da geçerli olacağı savunulmaktadır.[46] Nitekim, verilerin ilk amaçla bağlantılı diğer amaçlar için de yeniden açık rıza alınmadan işlenmesi ilgili kişinin haklarını olumsuz etkilemeyecektir. Hangi amaçların ilk amaçla bağlantılı sayılacağına ilişkin değerlendirme için GVKT md. 6/4'de belirlenene benzer kriterler kullanılabilecektir.

1.1.3. Asgari Düzeyde Veri İşleme İlkesi

Asgari düzeyde veri işleme ilkesi *(ing. data minimisation)* GVKT md. 5/1/c'de düzenlenmektedir. Bu ilke işlendikleri amaca erişmek adına gereken asgari düzeyde verinin, asgari süreyle işlenmesini ifade etmektedir. Tüzüğe göre veri işleme faaliyetiyle hedeflenen amaca, anonim verilerle de ulaşılabilecekse, kişisel veri olarak işlenmeleri asgari düzeyde veri işleme ilkesine aykırıdır.[47] Bunun yanında Tüzük bir güvenlik önlemi olarak verilerin psödönimler kullanılarak işlenmesini de teşvik etmektedir. Öyle ki, GVKT md. 25'de psödönim kullanmanın asgari düzeyde veri işleme ilkesine hizmet ettiği ve ilgili kişiler için riski azalttığı belirtilmektedir.

---

[44] ÇEKİN 2020, sge, s.73, kn.147
[45] Age.
[46] Age, s. 79, kn. 163; KÜZECİ Elif, Kişisel Verilerin Korunması, 3. Baskı, Turhan Kitabevi, Ankara 2019, Türkiye. s. 206, 207.
[47] *Herbst'e ait kısım,* KÜHLING, BUCHNER, age, s. 228.

Türk hukukunda bu ilkeyi somutlaştıran ayrıca bir hüküm bulunmamaktadır. Ancak KVKK md. 4/2/ç'de düzenlenen işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, belirtilen amaca kişisel verinin işlenmesinden başka araçlarla ulaşılabiliyor ve bu araçlar korunması amaçlanan temel hak ve özgürlüklere daha az müdahale ediyorsa, bu araçların tercih edilmesini sağlamaktadır.[48] Dolayısıyla Kişisel Verilerin Korunması Kanunu'ndaki ölçülülük ile asgari düzeyde veri işleme ilkesinin karşılanmaya çalışıldığı söylenebilecektir.

1.1.4. Doğruluk İlkesi

Doğruluk ilkesi *(ing. accuracy),* GVKT md. 5/1/d'de yer almakta ve kişisel veri içeriğinin doğru ve güncel olmasını gerektirmektedir. Madde doğruluk kriterini, veri işleme faaliyetinin kapsamına bağlamaktadır. Dolayısıyla kişisel veriler ancak veri işleme amacı için önem taşıdıkları ölçüde doğru olmalıdırlar. Örneğin veriler yıllarına göre düzenlenip bir havuzda işleniyorsa, alınacak kişisel veriye dair ay ve günün belirli olup olmaması sonuca etki etmeyecektir. Benzer şekilde kişilerin kilosu 5'er kiloluk aralıklarda işleniyorsa, kişisel verinin gramına kadar doğru olması gerekmemektedir.[49] Belirtmek gerekir ki doğruluk ilkesi beraberinde, doğru olmayan verilerin silinmesi yükümlülüğünü de getirmektedir.[50]

Tüzük ile benzer şekilde, KVKK md. 4/2/b doğru ve gerektiğinde güncel olma ilkesini düzenlemektedir. Nitekim KVKK md. 11/1/d ilgili kişilere, kendileri hakkındaki yanlış bilgilerin düzeltilmesini talep hakkı vermektedir.

1.1.5. Sınırlı Muhafaza İlkesi

Sınırlı muhafaza ilkesi *(ing. storage limitation)* GVKT md. 5/1/e'de düzenlenmektedir. Bu ilke kişisel verilerin, veri işleme amacı için gereklilikleri sona erdiği anda, muhafazasına son verilmesini ifade etmektedir. İlkenin yerine getirilmesi için öngörülen yöntemlerden biri verilerin silinmesidir. Tüzüğe göre veriler ilgili kişinin kimliğini tespite imkân verecek şekilde kaydedilmediği takdirde silinmiş sayılmaktadır.[51] Dolayısıyla, verilerin ilgili kişiyle ilişkilendirilmesinin önüne geçilmelidir. Örneğin

[48] ÇEKİN 2020, age, s.81, kn.171.
[49] *Herbst'e ait kısım,* KÜHLING, BUCHNER, age, s. 229.
[50] GVKT md. 17/2 bu hususu açıkça düzenlemektedir.
[51] *Herbst'e ait kısım,* KÜHLING, BUCHNER, age, s. 230.

veriler işlenirken psödönim[52] kullanıldıysa, kişilerin belirlenmesine elverişli ek bilgilerin yer aldığı liste yok edilmelidir. Bir başka ifadeyle sınırlı muhafaza ilkesi uyarınca verilerin işleme amaçları için gerekliliği sona erdiği anda, kişisel veri niteliğine son verilmesi gerekmektedir.

Bu ilke Türk hukukunda, KVKK md. 4/2/d'de mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ile yer almaktadır. İlkenin somut görünümü kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğüdür. Tüzüğe paralel şekilde KVKK md. 7 uyarınca, verilerin işlenmesini gerektiren sebepler ortadan kalktığında, kişisel veriler resen veya ilgili kişinin talebi üzerine silinecektir.

1.1.6. Bütünlük ve Gizlilik (Güvenlik) İlkesi

Bütünlük ve gizliliği düzenleyen *(ing. integrity and confidentiality (security))* GVKT md. 5/1/f verilerin genel güvenliğinin korunmasını ifade etmektedir. Bu ilke mahremiyeti korumakta ve veri akışı için belirlenen etik kurallara uyulmasını taahhüt etmektedir. Veri işleme faaliyeti için saptanan risklerden korunmak için bazı teknik ve idari önlemler öngörülmelidir.[53] Öyle ki alınacak bu önlemler, *Binding Corporate Rules* hazırlanırken dikkate alınacak ve bu taahhüt metinlerinde açıkça belirtilecektir. Dolayısıyla söz konusu taahhütlerin ilke amacına hizmet ettiğini söylemek isabetlidir.

Hangi risklere karşı önlem alınması gerektiği sorusunu cevaplarken, riskleri iki ana grupta toplamak mümkün olacaktır. İlk risk grubu yetkisiz ve hukuka aykırı veri işleme faaliyetleridir. Kişisel veriler ancak GVKT md. 4/10 kapsamında yetkilendirilmiş kişilerce işlenmelidir. Bu kişiler haricinde işlendikleri takdirde yetkisiz veri işlemeden bahsedilir. Hukuka aykırı veri işleme ise, GVKT md. 6/1 uyarınca bir hukuka uygunluk nedenine dayanılmadan yapılan veri işleme faaliyetlerini ifade etmektedir.

Önlem alınması gereken ikinci risk grubu ise, kişisel verilerde yaşanabilecek öngörülemeyen kayıp, zarar ve ziyandır. Şöyle ki, burada kapsama alınmak istenen

[52] GVKT md. 4/3/b uyarınca psödonimleştirilmiş veri, ek bir bilgi olmadan gerçek kişiyle ilişkilendirilemeyen veridir. Bu ek bilgiler ayrı bir yerde ve gerçek kişiyle ilişkilendirilmelerinin önüne geçen ek idari ve teknik tedbirlerle korunarak depolanmalıdır. Anonimleştirilmiş veri aksine psödonimleştirilmiş veriler, kişisel veri sayılmaktadır.

[53] Alınacak teknik ve idari önlemler GVKT md. 32'de somutlaştırılmıştır. Tüzükte ek bir önlem olarak, gerekçenin 39. maddesinde, yetkisiz kişilerin, verilerin işlendiği aletlere erişiminin engellenmesinin yanında, bu aletleri kullanmalarının da önüne geçilmesinden bahsetmektedir.

hususlardan biri de veri sorumlusu yahut çalışanları tarafından veri işleme için yetkilendirilmiş kişilerin, veri sorumlusunun haberi olmaksızın, işleme amaçlarından başka amaçlar için yapacakları işleme faaliyetleridir. Elbet böyle bir durumda sorumluluk değerlendirilirken, veri sorumlusunun bu riski engellemek adına aldığı önlemler dikkate alınacaktır.

Türk hukukunda bütünlük ve gizlilik (güvenlik) başlı başına bir ilke olarak düzenlenmemiştir. Ancak KVKK md. 12/1/c uyarınca veri sorumlusu, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idari tedbiri almakla yükümlüdür. Belirtilmelidir ki Bağlayıcı Şirket Kuralları, kanundaki bu yükümlülüğün yerine getirilmesi ve alınacak önlemlerin somutlaştırılması açısından önem taşımaktadır.

1.1.7. Hesap Verilebilirlik İlkesi

GVKT md. 5/2'de düzenlenen ve md. 24 ile somutlaştırılan hesap verilebilirlik ilkesi *(ing. accountability)* iki noktadan oluşmaktadır. Buna göre veri sorumlusu hem 5. maddenin 1. fıkrasında öngörülen ilkelere uymakla, hem de uyduğunu ispatla yükümlüdür. Veri sorumlusunun yükümlülükleri olarak adlandırılan 24. madde, GVKT md. 5/2 ile birlikte hesap verilebilirlik yükümlülüklerini uygulamaya koymaktadır.

Hesap verilebilirlik Tüzüğün merkezindeki kavramlardan biridir.[54] Tüzük'te düzenlenen şekliyle hızlı çözüm oluşturmayı, şeffaflığı ve yaptırımları içerdiği söylenebilecektir.[55] Veri sorumlusunun *ex ante* bir yaklaşımla *compliance* sağlamasını ve *compliance* sağladığını her zaman için gösterebilmesini yükümlülük altına almaktadır.[56] Böylece veri işleme sürecinin tamamının, henüz hukuka aykırılık meydana gelmeden Tüzüğün öngördüğü yükümlülüklere uyumlu hale getirilmesi hedeflenmektedir. Bu nedenle doktrinde hesap verilebilirlik ilkesinin, bütünüyle bir *compliance* sağlanmasına işaret ettiği söylenmektedir.[57]

[54] *Docksey'e ait kısım*, KUNER, Christopher, BYGRAVE, Lee, DOCKSEY, Christopher, The EU General Data Protection Regulation: A Commentary, Oxford University Press, Oxford, Birleşik Krallık 2020, s. 557.
[55] Age, s. 561.
[56] Age, s. 557.
[57] *Mantz ve Marosi'ye ait kısım*, SPECHT, MANTZ, age, s. 71.

Hesap verilebilirliğin ispatı için ilgili her evrak kullanılabilmektedir.[58] *Binding Corporate Rules* ispat için kullanılabilecek bir evraktır.[59] Nitekim Binding Corporate Rules *compliance* sağlanması için birçok yöntemi ve *compliance* sağlandığına ilişkin denetimleri taahhüt altına almaktadır.[60] Buna ek olarak GVKT md. 30 uyarınca tutulacak veri işleme faaliyeti kayıtları ve md. 35 uyarınca veri koruması etki değerlendirmeleri de hesap verilebilirlik için önemli araçlardır.[61]

Tüzüğün 24. maddesi altında, risk için uygun görülen teknik ve idari önlemlerin kurulması ve güncellenmesi öngörülmüştür. Hesap verilebilirliğin sağlanması için veri sorumlusunun alacağı önlemler yapılacak risk analizine göre belirlenecektir. Veri işleme faaliyetleri ilgili kişilerin hak ve özgürlükleri üstünde yüksek bir risk oluşturuyorsa, md. 35 uyarınca veri koruması etki değerlendirmesi yapılması gerekmektedir. Görüldüğü üzere veri sorumlularının bu yükümlülüğü, hesap verilebilirlik ile ilişkili risk kavramı üzerinden düzenlenmiştir. Tüzük, veri sorumlularının risk değerlendirmesi yaparken kullanacakları kriteri düzenlememiş, ancak yüksek risk oluşturan faaliyetleri örneklemiştir.[62] Risk değerlendirmesi yapılırken veri işleme faaliyetinin türü, kapsamı ve amaçlarının dikkate alınması söylenmiştir.[63]

Hesap verilebilirlik ilkesi uygulamada Yetkili Veri Koruma Otoriteleri'ni de ilgilendirmektedir.[64] Zira veri sorumlusu tarafından uyum ispat edilemediği takdirde Tüzük'te yüksek idari para cezaları öngörülmüştür. Mülga Direktif yaptırımları, meydana gelen hukuka aykırılıklar için düzenleyen bir mevzuattır. Direktif'teki *ex post* düzenlemeler uygulamada yetersiz kalmış ve hukuka aykırılıkların meydana gelmesine yol açmıştır.[65] Dolayısıyla Tüzük ile hukuka aykırılık henüz meydana gelmeden, hukuka aykırılığın önüne geçmeyi hedefleyen bir bakış açısı benimsenmiştir. Yukarıda bahsedildiği üzere veri koruması etki değerlendirmesi gibi hesap verilebilirliğin somut

[58] Age.
[59] Çalışmanın 2.3.1.8. ve 2.3.1.10. başlığına bakınız.
[60] *Docksey'e ait kısım*, KUNER, BYGRAVE, DOCKSEY, age, s. 562.
[61] *Mantz ve Marosi'ye ait kısım*, SPECHT, MANTZ, age, s. 71.
[62] GVKT gerekçe md. 75.
[63] GVKT gerekçe md 76.
[64] Yetkili Veri Koruma Otoriteleri GVKT md. 58/1 uyarınca veri sorumlularından bilgi ve belge isteme hakkına sahiptirler. Hesap verilebilirlik neticesinde riski yüklenmiş veri sorumlusu, istenen belgeleri sağlamakla yükümlüdür.
[65] DEMETZOU Katerina (2019), 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of high risk in the General Data Protection Regulation', Computer Law & Security Review, C. 35, S. 6, (Article 105342), s. 3.

örnekleri, Tüzük altında *ex ante* olarak tasarlanmışlardır.[66] Bu husus, Tüzüğün hukuka aykırılık meydana gelmeden aykırılığın önüne geçmeyi hedefleyen risk odaklı bakış açısına da uygun bir yaklaşımdır.[67]

Bu noktada hesap verilebilirlik için öngörülen yaptırımlar incelenmelidir. Tüzük'te hesap verilebilirlik için *ex ante* tasarlanan araçların işletilmemesi (ör. veri koruması etki değerlendirmesinin yapılmaması) halinde, herhangi bir hukuka aykırılık meydana gelmese de veri sorumlusuna bir yaptırım uygulanıp uygulanmayacağı tartışılmaktadır.[68] Fikrimizce veri sorumlusuna yalnızca veri koruması etki analizinin yapılmaması dolayısıyla, bir hukuka aykırılık meydana gelmese de yaptırım uygulanması Tüzüğün amacına uygundur.

Hesap verilebilirlik Direktif döneminde de var olan bir ilke olup Tüzük ile uygulamasını güçlendirmek adına araçlar benimsenmiştir.[69] Veri koruması etki analizleri de bu araçlardan biridir. Hesap verilebilirliğin etkin uygulamasını sağlamayı hedeflemektedir. Dolayısıyla Tüzük ile hedeflenen etkin hesap verilebilirlik için *ex ante* bir uygulama gerekmektedir. Nitekim GVKT md. 83/4/a maddesi uyarınca, veri sorumlularının/işleyenlerinin GVKT md. 25-39 maddeler arasındaki yükümlülüklerine aykırılık halinde 10 milyon EUR, şayet bir ticari teşebbüs söz konusu ise global cironun 2 %'sine kadar idari para cezası düzenlenmiştir. Sayılan bu yükümlülüklerin arasında verilerin, tasarım itibariyle ve varsayılan olarak korunması, veri işleme kayıtları, veri koruması etki değerlendirmeleri, veri koruması görevlisi ve veri ihlallerine hazırlık gibi hesap verilebilirlik araçları da mevcuttur.

Ancak doktrinde Tüzüğün gelecek teknolojilere uygulanabilirliğini sağlamak adına, özellikle geniş düzenlenen hesap verilebilirlik kavramının[70], yukarıda açıklanan yaptırımlarda sorun yaratabileceği söylenmektedir.[71] Öyle ki hesap verilebilirlik için öngörülen veri koruması etki değerlendirmesi yükümlülüğü, veri sorumlusunun yapacağı

---

[66] Age.
[67] Age.
[68] *Docksey'e ait kısım*, KUNER, BYGRAVE, DOCKSEY, age, s. 566.
[69] Age, s. 565, taslak GVKT md. 22/2 altında hesap verilebilirlik için özellikle beş araç sayılmıştır. Bunlar dokümantasyon, güvenlik, veri koruması etki değerlendirmeleri, önceden bir yetkilendirme veya danışma ve veri koruma görevlileridir ('DPO'). Tüzüğün son halinde hesap verilebilirlik odaklı araçlar olarak md. 24/3 altında davranış kuralları ve sertifikalar, md. 25 verilerin tasarım itibariyle ve varsayılan olarak korunması, md. 30 veri isleme kayıtları, md. 35 veri koruması etki değerlendirmeleri, md. 37-39 veri koruma görevlisi ve md. 47 *Binding Corporate Rules* benimsenmiştir.
[70] Md. 29 Çalışma Grubu, Opinion on Accountability 3/2010, kn. 49.
[71] DEMETZOU, age, s. 7.

risk değerlendirmesine göre meydana gelmektedir. Ancak kanunda bu değerlendirme için yeknesak kriterler öngörülmediğinden veri sorumlularının haksız ve değişken yaptırımlara tâbi tutulması mümkündür.[72]

Kişisel Verilerin Korunması Kanunu ise ayrı bir ilke olarak hesap verilebilirliği düzenlememiştir. Ancak Kişisel Verileri Koruma Kurulu'nun ('Kurul') yapacağı incelemenin usul ve esaslarını düzenleyen KVKK md. 15/3 uyarınca veri sorumluları, inceleme konusuyla ilgili istenmiş bilgi ve belgeleri on beş gün içinde Kurul'a göndermek ve gerektiğinde Kurul'un yerinde inceleme yapılmasına imkân sağlamak zorundadır. Bu anlamda Bağlayıcı Şirket Kurallarının Türk hukuku açısından bir ispat kolaylığı sağlayacağı açıktır.

1.2. UYGULAMA ALANI

Tüzüğün yeniliklerinden biri bölgesel uygulama alanının genişletilmesidir. Şöyle ki Tüzükte üçüncü ülkedeki bazı veri sorumluları için sınırötesi *(ing. extraterritorial application)* uygulama getirilmiştir. Böylece Tüzük belli durumlarda, üçüncü ülkelerdeki veri sorumlularını da yükümlülük altına almaktadır. Bu nedenle çok uluslu veya Birlik ülkeleri ile ticaret yapan şirketler için uyum sağlanması gereken bir mevzuattır. Çoğu zaman Tüzüğün uygulama alanına giren üçüncü ülkelerdeki şirketler, hem tâbi oldukları yerel mevzuat hem de Tüzük için uyum projeleri yürütmektedirler. Dolayısıyla *Binding Corporate Rules* gibi çok uluslu şirketlerin veri uyum süreçlerini yeknesak hale getiren taahhüt metinleri daha da önem kazanmıştır.

Tüzüğün direkt uygulanması için ikili bir ilke benimsenmiştir. Bunlardan ilki Direktif ile getirilmiş ve esasları Avrupa Adalet Divanı ('Divan' 'AAD') kararlarıyla da somutlaştırılmış olan kuruluş ilkesidir *(ing. establishment principle).* İkinci ise Tüzük ile benimsenen pazaryeri ilkesidir *(ing. marketplace principle).* Pazaryeri ilkesi ile Tüzüğün uygulama alanı Birlik dışındaki veri sorumlularını ve/veya işleyenleri de kapsayabilecek şekilde genişlemiştir. Bu başlık altında her iki ilke incelenecek ve Tüzüğün hangi şirketler için doğrudan uygulanabilir olduğu belirlenecektir.

[72] Age., s. 8.

1.2.1. Kuruluş İlkesi *(ing. Establishment Principle)*

Kuruluş ilkesi Tüzüğün bölgesel uygulama alanına ilişkindir. GVKT md. 3/1 uyarınca bir veri işleyen veya sorumlusunun, Birlik içerisindeki kuruluşunun faaliyetleri bağlamında işlenen tüm veriler Tüzük kapsamındadır. Bir başka ifadeyle kuruluş ilkesi uyarınca veri işleme faaliyetinin Birlik içerisinde gerçekleştirilmesi aranmamaktadır.

Bu ilkenin usul ve esasları, Tüzük öncesi Direktif döneminde alınan Divan kararlarıyla belirlenmiştir. Bu anlamda ilk olarak 'kuruluş' kavramının içeriği belirlenmelidir. Tüzükte herhangi sabit bir oluşum üzerinden yapılacak etkili ve gerçek bir faaliyetin bu madde kapsamında olacağı düzenlenmiştir.[73] Söz konusu oluşum, bir bayi veya şube olarak kurulabilmektedir ve hukuki bir kişiliğe sahip olması aranmamaktadır.

Söz konusu ilke Direktif döneminin önemli kararlarından *Google Spain*[74] içerisinde tartışılmıştır. Karar bir İspanya vatandaşının unutulma hakkını kullanarak silinmesini istediği, google aramasında çıkan 12 yıl öncesine ait iflas haberleri hakkındadır. Google'ın şirket yapılanmasına göre, Amerika'da yerleşik Google Inc. şirketinin İspanya'da bir bağlı kuruluşu bulunmaktadır. İspanya'daki bağlı Google kuruluşu yalnızca reklam alanı satmakta ve pazarlama işleri yürütmektedir. Bundan hareketle Google, söz konusu bağlı kuruluşun veri işleme faaliyeti gerçekleştirmediğini iddia etmiştir. Google'ın iddiasına göre veri işleme faaliyetini yürüten şirket Google Inc. Amerika Birleşik Devletleri'nde yerleşiktir. Dolayısıyla veri işleme faaliyeti de Amerika Birleşik Devletleri'nde yürütülmektedir. Google Inc. bu açıklaması doğrultusunda, İspanya'nın yargı alanı dışında olduğunu iddia etmiştir.

Divan ilk olarak, Google arama motorunda çıkan arama sonuçları elbette 'veri işleme' faaliyeti olarak adlandırmıştır. Bu hizmetin Amerika Birleşik Devletleri'ndeki Google Inc. tarafından sağlandığını; bu şirketin veri sorumlusu olduğunu söylemiştir. İspanya'daki bağlı şirkete ilişkin değerlendirmesinde ise, faaliyetlerinin yalnızca pazarlama ve reklam yeri satmak olsa da bunların ekonomik bir faaliyet olduğunu belirlemiştir. Dolayısıyla İspanya'daki bağlı şirketin faaliyetleri dolayısıyla ana şirketin ekonomik çıkar sağladığı tespit etmiştir. Divan böylece, İspanya'daki kuruluşun faaliyetlerinin Google Inc. ana şirketine bağlı olduğuna ve ayrı değerlendirilemeyeceğine

[73] GVKT gerekçe md. 22
[74] AAD C – 131/12

hükmetmiştir. Öyle ki Divan karar verirken, verilerin nerede işlendiğinin değil[75], kuruluşun faaliyetleri bağlamında işlendiğini dikkate almıştır.[76] Buradan hareketle veri sorumlusunun İspanya'nın yargı alanında olduğuna hükmetmiştir.[77]

Kuruluş ilkesinin sınırları Divan'ın Direktif döneminde verdiği Weltimmo[78] kararıyla çizilmeye devam etmiştir. Karar bir Slovak şirketinin Macaristan'daki kuruluşunun ihlali nedeniyle, Macar veri koruma otoritelerinin kestiği cezaya ilişkindir. Slovak şirket, Macaristan'da herhangi bir şirket merkezi, şube veya bayi bulunmadığını belirtmiştir. Bundan hareketle, Macaristan veri koruma otoritelerinin yetki alanında olmadığını iddia etmiştir. Kararda Divan *Google Spain* kararına atıf yaparak; bir ülkedeki kuruluşun sabit bir oluşum olması için herhangi bir hukuki kişiliğe gerek olmadığını belirtmiştir. Somut olayda, Slovak şirketin Macaristan'da bir temsilci kişisi bulunduğunu, Macarca bir internet sitesi kullandığını, Macar banka hesapları olduğunu belirtmiş ve bu hususları, sabit bir oluşum için yeterli görmüştür.[79] Böylece Macaristan'da herhangi bir hukuki kişiliği bulunmadan faaliyet gösteren Slovak şirketinin, Macar veri koruma otoritelerinin yetkisinde olduğuna hükmedilmiştir.

Yukarıdaki kararlarda belirlenen esaslar, Avrupa Birliği Veri Koruma Kurulu'nun ('Birlik Kurulu') Tüzüğün bölgesel uygulama alanına dair yayınladığı 3/2018 sayılı kılavuzda[80] örneklendirilmiş ve somutlaştırılmıştır. Belirtilmelidir ki bir oluşumun Tüzüğün bölgesel uygulama alanına ilişkin GVKT md. 3/1 veya md. 3/2 kapsamına girip girmediği, her bir somut olayda ayrı değerlendirilmelidir. Kılavuz, kuruluş ilkesi bağlamında iki ana olgunun dikkate alınmasını tavsiye etmiştir. İlk olarak Birlik dışındaki veri sorumlusu veya işleyen ile Birlik içerisindeki kuruluş arasındaki ilişki incelenmelidir. İkinci olarak ise Birlik içerisindeki kuruluşun sağladığı ekonomik gelir değerlendirilmelidir. Eğer bu ekonomik gelir, Birlik dışındaki veri işleme faaliyetlerinden ayrı değerlendirilemiyorsa, kuruluş ilkesi gereğince Tüzüğün uygulanacağı söylenebilecektir. Kılavuz bu değerlendirme kriterlerini örneklerle somutlaştırmıştır.

---

[75] TREACY Bridget, SIMPSON Aaron, An Introduction Do Data Protection Law, Lexis Nexis, London, Birleşik Krallık 2019, s.78.
[76] AAD, C-131/12 (Google Spain), 52, 13.05.2014 K.
[77] AAD, C-131/12 (Google Spain), 20, 23, 32, 33, 51, 52, 57, 13.05.2014 K.
[78] AAD, C-230/14 (Weltimmo)
[79] AAD, C-230/14 (Weltimmo), 11, 13, 16, 29, 32, 01.10.2015 K.
[80] European Data Protection Board-Guidelines 3/2018 on the territorial scope of the GDPR.

Bu örneklerden biri, Çin menşeili bir e-ticaret sitesine ilişkindir. Şirketin kişisel veri işleme faaliyetlerinin tamamı Çin'de yürütülmektedir. Çinli şirket, Avrupa pazarı hakkında araştırma yapmak, Avrupa'da pazarlama ve reklam kampanyaları yürütmek amacı ile Berlin'de bir ofis açmıştır. O kadar ki Berlin ofisinin kurulma amacı Çinli şirketin sunduğu hizmetin kârını arttırmaktır. Bu nedenle Çin'deki şirketin Avrupa satışları dolayısıyla işlediği kişisel veriler, Berlin'deki ofisin faaliyetleriyle ayrılmaz biçimde bağlı sayılacaktır. Bundandır ki ancak bu kişisel verilere ilişkin işleme faaliyetleri GVKT md. 3/1'e tâbidir.

Kılavuzda verilen bir diğer örnek Güney Afrika'daki bir otel zinciridir. Birlik içerisinde herhangi bir yerleşik düzeni veya ofisi bulunmayan otel, web sitesi üzerinden İngilizce, Almanca, Fransızca ve İspanyolca paket programlar sunmaktadır. Bu durum otelin GVKT md. 3/1 uyarınca Tüzük kapsamına girmesi için yeterli değildir. Ancak dikkat edilmelidir ki bu otel örneği, bir sonraki başlık altında incelenecek pazaryeri ilkesi uyarınca Tüzüğün uygulama alanına girebilecektir.

Verilen bir diğer ilginç örnek Meksikalı bir perakende şirketine ilişkindir. Şirket, Meksikalı müşterilerinin kişisel verilerinin işlenmesi amacıyla İspanyalı bir veri işleyenle veri işleme sözleşmesi imzalamıştır. Meksikalı şirket, yalnızca Meksika pazarına hizmet sunmaktadır ve işlenen kişisel veriler de Birlik vatandaşlarına ait değildir. Bu durumda Meksikalı şirket GVKT md. 3/1 uyarınca Tüzüğün kapsamında olmayacaktır. Ancak İspanyalı veri işleyen şirket, İspanya'da kurulu olduğu için niteliği itibariyle GVKT md. 3/1'in uygulama alanındadır. Bu nedenle veri işleyen, faaliyetleri dolayısıyla Tüzükte öngörülen tüm yükümlülüklere uymak zorundadır.

1.2.2. Pazaryeri İlkesi *(ing. Marketplace Principle)*

Pazaryeri ilkesi Tüzük ile getirilen bir yenliktir. Bu ilke sayesinde Tüzük, Birlik'te yerleşik olmayan veya Birlik'te herhangi bir temsilciği bulunmayan veri sorumlularına veya işleyenlere de doğrudan uygulanabilmektedir. İlke dolayısıyla Tüzüğün doğrudan uygulanabilmesi için Birlik dışındaki bu veri sorumluları/işleyenlerinin Birlik'teki gerçek kişilere mal ve/veya hizmet sunması yahut bu gerçek kişilerin internetteki aktivitelerini izlemesi gerekmektedir.

Pazaryeri ilkesi olarak adlandırılan düzenleme, GVKT md. 3/2'de aşağıdaki gibi yer almaktadır;

> *Bu tüzük, Avrupa Birliği içerisindeki veri sahiplerinin (ilgili kişilerin) kişisel verilerinin işlenmesi halinde, işleme aktivitesi aşağıdaki durumlarla ilişkili olduğu takdirde, Avrupa Birliği içerisinde kurulu olmayan veri sorumluları veya işleyenleri için de uygulanır;*
>
> *(a) İlgili kişinin karşılığında bir bedel ödeyip ödemediğine bakılmaksızın, Avrupa Birliği içerisindeki ilgili kişiye mal veya hizmet sunulması; veya*
>
> *(b) Avrupa Birliği içerisinde gerçekleşen hareketlerinin izlenmesi.*

İlk olarak belirtmek gerekir ki, Tüzük ilgili kişiler için 'Avrupa Birliği içerisindeki veri sahipleri' ifadesini kullanarak vatandaşlık bağı aranmadığına işaret etmektedir. Bu anlamda hizmetin sunulduğu ilgili kişinin Birlik'teki bir ülkede yerleşik bir hayatının olması (ör. işyeri, okulu) yeterlidir. Benzer şekilde yerleşik hayatlarını Birlik dışında sürdüren Birlik vatandaşlarının (ör. Türkiye'deki bir lisede çalışan Alman öğretmen) bu ilkede bahsedilen ilgili kişi olmadıkları söylenebilecektir.

Bir önceki başlıkta 'Birlik'te kurulu olmak' ifadesinin Tüzük'teki hukuki anlamı ayrıntısıyla açıklanmıştır. Dolayısıyla bu başlıkta GVKT md. 3/2 değerlendirilirken, a bendinde yer alan 'mal veya hizmet sunumu' kavramıyla başlanacaktır. Birlik hukuku açısından 'mal', ticari bir işleme konu olabilecek, para değeri olan ürünü ifade etmektedir. 'Hizmet sunumu' ise mal kavramını sınırlandıran, kural olarak maddi karşılığı ölçülebilen hizmet için kullanılmaktadır.[81] Ancak maddenin lafzında belirtildiği üzere, veri sorumlusu veya işleyenin bu maddeye tâbi olup olmadığı değerlendirilirken, sunulan mal veya hizmet karşılığı bir bedel ödenip ödenmediği dikkate alınmamaktadır.

Önemli bir diğer husus da mal veya hizmet sunumunun hangi hallerde Birlik'teki kişilere yöneltilmiş sayılacağıdır. Tüzüğe göre hizmetin belirli ve açık olarak Birlik'teki ilgili kişiye yöneltilmesi gerekmektedir. Örneğin bir internet sitesinin Birlik'teki bir ilgili kişinin erişimine açık olması, mal veya hizmet sunumunun ona yönlendirildiğini belirlemeye tek başına yetmeyecektir.[82]

---

[81] *Meyerdierks'e ait kısım,* MOOS Flemming, SCHEFZIG Jens, ARNING Marian, Die Neue Datenschutz-Grundverordnung, De Gruyter Yayınevi, Berlin, Almanya 2018, s. 47.
[82] GVKT gerekçe md. 23

Sunulan hizmetin Birlik içerisindeki kişiye yöneltilmesi kavramı Birlik Kurulu'nun 3/2018 sayılı kılavuzunda örneklendirilmiştir. Verilen örneklerden biri Avustralyalı bir şirkete ilişkinidir. Bu şirket kullanıcılarının tercihleri yönünde kişiselleştirilen bir mobil haber servisi sunmaktadır. Servis, yalnızca Avustralyalı kişilere sunulmakta ve servise Avustralya uzantılı bir cep numarası ile kayıt olunmaktadır. Servisi kullanan bir Avustralya vatandaşı, tatil için Almanya'ya gidip bu servisi kullanmaya devam etse dahi, Avustralyalı şirket Tüzüğün doğrudan uygulama alanında olmayacaktır. Öyle ki Avustralyalı şirketin sunduğu servis, Birlik içerisindeki kişileri hedef almamaktadır.

Hizmetin yöneltilip yöneltilmediğine ilişkin değerlendirme somut olayda pek çok farklı kriter ile yapılmaktadır. Şöyle ki, internet sitesinin Birlik'teki ilgili kişinin kendi dilinde de mevcut olması, sunulan mal veya hizmet bedelinin ilgili ülkenin para birimiyle gösterilmesi, alan adı uzantısı olarak ilgili ülke uzantısının (ör. Almanya için .de veya Fransa için .fr) mevcut olması, iletişim bilgisi olarak ilgili Birlik ülkesi alan kodlu telefon numarası belirtilmesi gibi hususlar dikkate alınmaktadır.[83]

Türkiye'deki bir otel zinciri üzerinden örneklemek gerekirse, otelin İngilizce web sitesi üzerinden uluslararası rezervasyon kabul etmesi, GVKT md. 3/2 dolayısıyla doğrudan uygulanabilirlik için yeterli değildir. Ancak aynı otel zinciri, Almanca bir site kurarak, Almanya'da yaşayan Türkler için özel bir fiyatla paket program sunuyorsa GVKT md. 3/2'den bahsedilecektir. Ancak belirtmek gerekir ki, burada aktif bir reklam faaliyeti dahi aranmamaktadır.[84]

Nitekim 3/2018 sayılı kılavuzda verilen örneklerden biri de Orta Doğu'ya İngilizce, Fransızca ve İspanyolca konuşan rehberler eşliğinde paket tur sunan bir Türk seyahat şirketine ilişkindir. Turlar Türk şirketin aynı üç dilde erişilebilen web sitesi üzerinden pazarlanmakta ve Euro ve İngiliz Sterlini[85] ile online rezervasyon kabul edilmektedir. Türk şirket pazarlama faaliyeti yürütmek ve ticari geliri arttırmak amacıyla Tunuslu bir müşteri hizmetleri firmasıyla (veri işleyen) anlaşmıştır. Bu müşteri hizmetleri firması Türk şirketin yönlendirmesi altında İrlanda, Fransa, Belçika ve İspanya'daki eski müşterileri arayarak, geçmiş seyahatleri hakkında bilgi almakta ve yeni tur programları

[83] *Meyerdierks'e ait kısım,* MOOS, SCHEFZIG, ARNING, age, s. 48.
[84] ÇEKİN 2020, age, s. 39.
[85] Bu noktada Birlik Kurulu'nun 2/2018 sayılı ilgili kılavuzunun yayınlandığı 12 Kasım 2019 tarihinde henüz İngiltere'nin Birlik'ten çıkışına ilişkin Brexit tamamlanmadığı belirtilmelidir.

hakkında bilgilendirmektedir. Bu durumda veri sorumlusu Türk seyahat şirketi de veri işleyen Tunuslu müşteri hizmetleri de Tüzüğün doğrudan uygulama alanına girecektir. Zira hizmetin Birlik'teki kişilere yöneltilmesi söz konusudur.

GVKT md.3/2/b ise Birlik'teki ilgili kişilerin, Birlik içerisindeki hareketlerinin izlenmesi düzenlenmektedir. İlgili kişilerin hareketlerinin izlenmesi kavramı temelde gerçek kişilere ilişkin yapılan profillemeyi *(ing. profiling)* içermektedir. Bu bentte, izlenen gerçek kişiye dair alınacak kararları etkilemek üzere, gerçek kişiyi ve/veya kişisel tercihlerini, davranış biçimlerini, tavırlarını analiz ve tahmin yöntemleriyle verilerinin işlenmesinden bahsedilmektedir.[86]

Birlik Kurulu'nun kılavuzunda bu bent de örneklendirilmiştir. Örnekte Amerikan bir danışmanlık şirketi konu alınmaktadır. Amerikan şirketi Fransız bir alışveriş merkezine, satışı arttırmak amacıyla dükkanların en uygun nasıl sıralanacağına ilişkin danışmanlık hizmeti vermektedir. Bu hizmeti sağlarken, Amerikan şirketi alışveriş merkezini ziyaret eden müşterilerin hareketlerini Wi-Fi ağı üzerinden takip etmektedir. Amerikan şirketinin hizmeti Fransız alışveriş merkezine yöneltilmemiş olsa bile, Fransız müşterilerin hareketleri izlendiğinden GVKT md. 3/2/b uyarınca doğrudan uygulanabilirlik söz konusudur.

Yukarıda açıklandığı üzere GVKT md. 3/2 dolayısıyla Tüzüğün doğrudan uygulama alanına giren üçüncü ülkelerdeki kuruluşlar, Tüzük'teki yükümlülükleri yerine getirmelidirler. Bu anlamda akla gelen ilk yükümlülüklerden biri, GVKT md. 27 uyarınca Birlik içerisinde bir temsilci atamak olacaktır. Bir sonraki başlıkta üçüncü ülkelerdeki şirketler ile Birlik üyesi şirketler arasında yapılan veri aktarımları incelenecektir. Üçüncü ülkelerdeki bu şirketlere Tüzük doğrudan uygulanmıyor olsa dahi yapılan veri aktarımları neticesinde gündeme gelebilecek yükümlülükler değerlendirilecektir. Tüzüğün üçüncü ülkelerdeki bu veri sorumlularına/işleyenlere veri aktarılması için *Binding Corporate Rules* dahil öngördüğü tüm yöntemler karşılaştırılacaktır.

1.3. BİRLİK İÇERİSİNDEN ÜÇÜNCÜ ÜLKELERE VERİ AKTARIMI

Uluslararası ticaretin gelişmesi ve büyümesi için elbette uluslararası veri aktarımı gerekmektedir. Dijitalleşmenin hız kazandığı 2005 ila 2014 yılları arasında uluslararası

[86] GVKT gerekçe md. 24

veri aktarımları da kırk beş kat artmıştır.[87] Dolayısıyla, hızlı büyüyen bu alanı düzenleyen mevzuatlar önem arz etmektedir.

1970'lerden bu yana 70'ten fazla ülke ve kuruluş, uluslararası veri akışını düzenleyen veri koruma ve gizlilik kanunları getirmiştir. Ancak konu hakkında kapsamlı hukuki çalışmalar, ancak internetin yaygınlaştığı 1990'lı yıllarda yapılmaya başlamıştır.[88] Uluslararası veri akışı kuralları milletlerarası özel hukuk, insan hakları hukuku, internet düzenlemeleri gibi pek çok farklı alanlara etkisi olan, önemli ve geniş bir başlıktır.[89]

Veri temelli ekonomideki gelişmelerle Birlik vatandaşlarına ait kişisel veriler de Birlik dışarısına aktarılmaya başlanmıştır. Bu aktarımlar kanunen düzenlenmediği takdirde Birlik vatandaşlarının temel haklarını ve Birliğin benimsediği veri koruma kurallarını tehdit edecektir. Divan uluslararası veri aktarımlarına dair verdiği *Weltimmo*[90]*, Schrems I*[91]*, Schrems II*[92] gibi kararlar ile Birlik vatandaşlarının temel haklarını uluslararası boyutta korumayı hedeflemektedir. Bahsi geçen kararlar Birlik pazarında yer almak isteyen uluslararası aktörlere bir uyarı olarak dahi nitelendirilebilir.[93] *Schrems I ve Schrems II* kararları Birlik ile Amerika Birleşik Devletleri arasındaki aktarımı direkt ilgilendirmektedir.[94]

Divan'ın bu kararlarıyla Birlik'te benimsenen veri koruma standartlarının pek çok farklı yargı alanına sirayet etmesi söz konusudur. Nitekim kişisel verinin en çok ve sık şekilde işlendiği alanlardan biri olan bulut bilişimdeki gelişmeler de buna işaret etmektedir. Birlik pazarına girmek isteyen bulut servis sağlayıcılarının hemen hepsi Birliğin veri koruma kurallarını benimsemiştir.[95]

---

[87] MATTOO Aaditya, MELTZER Joshua (2019), 'International Data Flows and Privacy: The Conflict and Its Resolution', Journal of International Economic Law, C. 21, S. 4, s. 769-789.
[88] WAGNER Julian (2018), 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide Adequate Protection?', International Data Privacy Law, C.8, S. 4, s. 318-337.
[89] KUNER Christopher, Transborder Data Flows and Data Privacy Law, 1st Edition, Oxford University Press, Birleşik Krallık 2013, s. 3.
[90] AAD C-230/14
[91] AAD C-362/14
[92] AAD C-311/18
[93] WEAVER Russel, FRIEDLAND Steven, GILLES William, BOUHADANA Irene, Privacy in a Digital Age Perspective from Two Continents Volume IV, Carolina Academic Press, North Carolina, Amerika Birleşik Devletleri 2017, s. 39.
[94] AAD E. C-362/14 K. 06.10.2015, Schrems v. Data Protection Commissioner, 82ff.
[95] KUNER Christopher (2014), 'The European Union and the Search for an International Data Protection Framework', Groningen Journal of International Law, C. 2, S. 2, s. 55-71.

Tüzüğün beşinci bölümü, Birlik içerisinde taahhüt edilen kişisel veri korumasının üçüncü ülkelerde de uygulanmasını ilgilendirmektedir. Söz konusu bölüm altında, Birlik dışarısındaki üçüncü bir ülkeye yahut uluslararası bir örgüte yapılacak veri aktarımlarının tâbi olduğu yükümlülükler düzenlenmektedir. Kişisel verilerin üçüncü ülkelere aktarılması Birlik'teki ilgili kişilerin hakları açısından bir risk teşkil etmektedir. Bu riski azaltmak adına GVKT md. 44 önleyici tedbir niteliğinde düzenlenmiştir. GVKT md. 44 üçüncü ülkelere veri aktarımının ancak 5. bölümde öngörülen yükümlülüklerin yerine getirilmesiyle mümkün olduğunu düzenlemektedir.[96] Birlik dışarısına yapılacak aktarımlar için düzenlenen 44. maddede dört temel husus yer almaktadır;

a. Kişisel verilerin, Birlik dışındaki üçüncü ülkelere aktarımı için, GVKT 5. bölüm dışında öngörülen, özellikle de GVKT 2. bölümde düzenlenen veri koruma ilkelerinin gereklilikleri yerine getirilmelidir.
b. Birlik dışındaki ülkelere veya uluslararası örgütlere veri aktarımı, ancak GVKT 5. bölümdeki izin usullerinin en az birini yerine getirmek koşuluyla yapılabilir.
c. Tüzüğün koruması, verinin aktarıldığı üçüncü ülkeden diğer ülkelere yapılacak ileri aktarımlarda *(ing. onward transfer)*[97] da devam etmelidir.
d. GVKT 5. bölümde belirlenen kurallar, Tüzük'te belirlenen standartların altına düşmemek amacıyla kullanılmalıdır.

GVKT 5. bölüm altında, Birlik'ten üçüncü ülkelere veri aktarımını somutlaştırmak adına, belirli usuller öngörülmüştür. İlk olarak verinin aktarılacağı üçüncü ülkede, Birlik düzenlemelerine denk veri koruması esaslarının bulunup bulunmadığı değerlendirilmektedir. Üçüncü ülkede yeterli bir koruma olduğuna karar verildiyse, bu ülke 'güvenli ülke' ilan edilmektedir. Güvenli ülkelerde yer alan veri sorumluları/işleyenlere, Birlik'ten serbestçe veri aktarılabilmektedir. Aşağıda yeterli korumanın bulunduğuna dair kararın nasıl verildiği ve bu kararın etkisi incelenecektir. Hakkında yeterli korumanın bulunduğuna dair karar olmayan üçüncü ülkeler için ise, korumanın başka yöntemlerle taahhüt edilmesi aranmaktadır. *Binding Corporate*

[96] *Paal'e ait kısım*, PAAL Boris, PAULY Daniel, Datenschutz-Grundverordnung, 2. Auflage, C.H. Beck, München, Almanya 2018, s. 537.
[97] Tüzüğe göre bir veri sorumlusu/işleyenin kendisine aktarılan kişisel veriyi bir başka veri sorumlusu/işleyene aktarmasına 'ileri aktarım' adı verilmektedir *(ing. onward transfer)*.

Rules'un da arasında bulunduğu bu diğer 'uygun güvenlik önlemleri' çalışmamızın 1.3.3. maddesinde alt başlıklar halinde açıklanacak ve karşılaştırılacaktır.

1.3.1. Yeterli Korumanın Bulunduğuna Dair Karar

ABTHB md. 8/1 kişisel verilerin üçüncü ülkelere aktarılması halinde, Birlik'te öngörülen ile aynı oranda bir korumanın devam ettirilmesini öngörmüştür. Dolayısıyla Tüzüğün uluslararası veri aktarımına dair hedefi, Tüzük'te ilgili kişilere sağlanan koruma standartlarının verilerin aktarıldığı ülkede de korunmasıdır. Bundadır ki ilk olarak, aktarımın yapılacağı üçüncü ülkede Tüzük açısından karşılıklı/yeterli bir korumanın varlığı değerlendirilmektedir.

GVKT md. 45 uyarınca, Avrupa Birliği Komisyonu bazı ülkelerde Tüzüğe denk bir korumanın bulunduğuna dair karar verebilmektedir. Söz konusu madde, mülga Direktif'in 25. maddesinden geliştirilmiştir ve Komisyon'un hedef ülkede yeterli koruma incelemesini yaparken, değerlendirmeye alacağı kıstasları içermektedir. Bu karar üçüncü ülkeler açısından çoğu kez 'Birlik ile uyum göstergesi' olarak algılanmaktadır. Aynı zamanda Birlik dışından alınacak müşteri hizmetleri benzeri veri işleme hizmetleri için tercih edilmelerini sağlamaktadır.[98]

Üçüncü ülkede yeterli korumanın bulunduğuna dair karar verilebilmesi için mutlaka dikkate alınması gereken kriterler 45. maddenin 2. paragrafında sayılmıştır. Bu kıstaslar tüketici biçimde belirlenmemiştir ve Avrupa Birliği Komisyonu somut incelemede ek olarak başkaca hususları da değerlendirebilmektedir.[99] GVKT md. 45/2'de sayılan değerlendirme kıstasları üç başlık altında toplanmıştır. İlk olarak, üçüncü ülke veya uluslararası örgütün iç hukukundaki veri koruma mevzuatı incelenmektedir. İkinci başlık ise, bağımsız bir yetkili veri koruma otoritesinin *(ing. data protection authority)* bulunup bulunmadığının ve uygulamada verdiği kararların değerlendirilmesidir. Son olarak üçüncü ülkenin veri koruması alanında uluslararası yükümlülüklere uyumuna

[98] *Selmayr'a ait kısım,* EHMANN Eugen, SELMAYR Martin, Datenschutz-Grundverordnung Kommentar, 2. Auflage C.H. Beck, München, Almanya 2018, s. 783.
[99] *Paal'e ait kısım,* PAAL, PAULY, age, s. 544.

bakılmaktadır.[100] Hakkında karşılıklı koruma bulunduğu kararı verilerek serbest veri dolaşımına sokulan ülkeler arasında Türkiye bulunmamaktadır.[101]

Bu karar Tüzük uyarınca yalnız belirli bir bölgeyle veya üçüncü ülkedeki belirli bir sektörle sınırlanabilmektedir. Avrupa Birliği Komisyonu'nun şu ana kadarki uygulamasından, her ne kadar artık geçerli olmasa da böyle bir imkânın bir noktada tanınmış olduğu bilinmektedir. Öyle ki, bir sonraki başlıkta inceleneceği üzere Birlik ile Amerika Birleşik Devletleri arasındaki mülga *Safe Harbor* ve *Privacy Shield* düzenlemeleri, bu anlamda önemli örneklerdir.

1.3.2. Amerika Birleşik Devletleri, *Safe Harbor ve Privacy Shield*

Avrupa'nın yakın tarihindeki faşizmde kişisel verilerin taşıdığı önem görülmüş ve bu dönemlerden sonra, kişilik hakları kapsamında korunmasına azami önem verilmiştir. Nitekim doktrinde bazı hukukçulara göre, Tüzük korumasındaki yüksek standart da bu tarihi durumun bir yansımasıdır. Dolayısıyla Avrupa dışındaki devletlerin çoğu zaman bu kadar ayrıntılı bir koruma düzeni benimsememelerinin sebeplerinden biri, tarihlerindeki bu fark olarak değerlendirilebilir.[102]

Birlik hukukundaki veri koruması düzenlemeleri, üye devletler için doğrudan uygulanmakta ve tüm veri işleme alanlarını kapsamaktadır. Amerika Birleşik Devletleri'nde ise kişisel verilerin korunmasına ilişkin federal ve tüm veri sorumlularına uygulanan bir düzenleme bulunmamaktadır. Veri koruması hukukunda sektörel bir yaklaşım benimseyen Amerika Birleşik Devletleri, Birlik ile veri aktarımı konusunda incelenmesi gereken önemli bir örnektir. Amerika Birleşik Devletleri ise hem federal hem de eyalet boyutunda uyulması gereken birçok kanun bulunmaktadır. Doktrinde niteliği itibariyle sektörel düzenlenen bu eyalet ve federal kanunların, işletmeler için zorluk yarattığı söylenmektedir.[103]

Bu iki kıta, kişisel veriler ve mahremiyet konusuna da sistematik olarak farklı yaklaşmaktadır. Birlik ülkelerinin pek çoğunda mahremiyetin, temel bir hak olarak

---

[100] Bu anlamda değerlendirilmeye alınan temel kriter olarak bkz. European Treaty Series No: 108 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'

[101] Birlik Komisyonu üçüncü ülkelere veri aktarımında yeterlilik kararı https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en Erişim Tarihi: 30.01.2020

[102] MATTOO, MELTZER, age, s. 774.

[103] WEBER H. Rolf, STEIGER N. Dominic, Transatlantic Data Protection in Practice, Springer, Berlin-Heidelberg, Almanya 2017, s. 39.

korunduğu bilinmektedir. Aynı zamanda Avrupa İnsan Hakları Sözleşmesi ('AİHS') md. 8, mahremiyeti temel hak olarak korumaktadır.[104] Amerika Birleşik Devletleri'nde mahremiyet hakkı daha ziyade mülkiyet ile ilişkilendirilirken, özellikle son otuz beş yılda bütüncül bir mahremiyet anlayışı geliştirmeye başlanmıştır.[105] Öyle ki mahremiyet düzenlemelerinin giderek tüm sektörlere yayılması da söz konusudur.[106]

Amerika Birleşik Devletleri'ndeki sektörel düzenlemelerin yansıması olarak, Birlik ile arasındaki veri aktarımları da *Safe Harbor ve Privacy Shield* anlaşmalarıyla sektörel biçimde düzenlenmiştir. Birlik ile Amerika Birleşik Devletleri arasındaki karşılıklılığı sektörel olarak sağlayan *Safe Harbor ve Privacy Shield* veri aktarımı yapan şirketler için önem taşıyan yöntemler belirlemiştir. O kadar ki, *Safe Harbor* ve sonrasında da *Privacy Shield'in* ortaya koyduğu prensiplerden kilit bir gereklilik olarak söz edilmiştir.[107]

Uygulamaya ilk olarak konulan antlaşma *Safe Harbor* olmuştur.[108] Bu antlaşma Avrupa Birliği Komisyon'u ve Amerika Birleşik Devletleri Ticaret Bakanlığı ortak çalışmasıyla geliştirilmiştir. Antlaşmada kişisel verilerin korunması için güvenli bir liman *(ing. safe haven)* yaratmak amacıyla, yedi adet ilke benimsenmiştir. Söz konusu yedi prensip, *Safe Harbor'ı* taahhüt eden şirketler için bağlayıcı nitelik kazanmıştır. Öyle ki, bu yedi prensip; aydınlatma yükümlülüğü *(ing. notice)*, veri sahiplerinin seçim hakkı *(ing. choice),* kurallara ileri aktarımlarda da uyulması (*ing. onward transfer)*, veri güvenliği *(ing. security)*, verilerin doğru ve güncel olması *(ing. data integrity)*, erişim hakkı *(ing. access)* ve son olarak da bağlayıcılık *(ing. enforcement)* olarak belirlenmiştir.[109]

Her ne kadar söz konusu ilkeler *Safe Harbor* taahhütlerini veren şirketler için bağlayıcı olarak düzenlense de yapılan bir araştırmada, şirketlere tanınan bu otonominin ters teptiği belirlenmiştir. 2010 tarihli bu araştırmaya göre Safe Harbor taahhütlerini veren Amerikan şirketlerinin ancak 21%'inin bu taahhütlere uyduğu tespit edilmiştir.[110] Neticede kişisel veriler gelir getiren bir pazardır ve şirketler kişisel verileri kullanarak

---

[104] Age, s. 20.
[105] Age, s. 27.
[106] Age, s. 28.
[107] KLECHA Robert, Datenübermittlungen in die USA nach dem Safe Harbor Urteil des EuGH, Verlag Dr. Kovac, Hamburg, Almanya 2018, s. 65.
[108] Direktif döneminde Komisyon'un 2000/520 kararıyla *Safe Harbor* kriterleri belirlenmiştir.
[109] *Safe Harbor* prensiplerinin ayrıntılı değerlendirmesi için bkz. KLECHA, age, s. 70.
[110] VOSKAMP Frederike, Transnationaler Datenschutz, 1. Auflage, Nomos Verlag, Frankfurt, Almanya 2015, s. 118.

pek çok şekilde kar elde etmektedirler.[111] Bu kullanım alanları hedeflenen müşteri kitlelerine reklam sunabilmek, başarılı pazarlama kampanyaları yürütmek, ürün geliştirmek ve hatta fiyat belirlemek olarak örneklenebilir.[112]

Safe Harbor iptal edilip *Privacy Shield* benimsenirken, kişisel verilerden ekonomik çıkar sağlayan bu şirketlerin *Privacy Shield* uyumunun, nitelik itibariyle arttırılması gerektiği söylenmiştir.[113] Paralel şekilde *Privacy Shield* benimsendikten sonra, şirketlerin uyumunu arttırmak adına Federal Ticaret Komisyonu'nun yüksek cezalar uyguladığı bilinmektedir.[114] Dolayısıyla *Safe Harbor'a* uyum problemlerinin, Tüzük'te böylesine yüksek cezaların öngörülmesine katkı sağladığı yönünde bir yorum da yapılabilecektir.

Safe Harbor antlaşması Tüzüğün düzenlenmesiyle hemen hemen paralel bir şekilde, Divan'ın C-362/14 kararıyla geçersiz kılınmıştır. Söz konusu karar, Birlik'ten üçüncü ülkelere yapılacak tüm veri aktarımlarına ilişkin ilkeler ortaya koymakta ve birçok açıdan *Binding Corporate Rules'u* da ilgilendirmektedir.[115] Dolayısıyla her ne kadar hâlihazırda onaylanmış *Binding Corporate Rules'un* geçerliliğini direkt olarak etkilemese de karar sonrasında pek çok üye devlet *Binding Corporate Rules* onay süreçlerini durdurmuştur.[116]

1.3.2.1. AAD C-362/14 Schrems v. Data Protection Commissioner Kararı (Schrems I) ve Üçüncü Ülkelere Veri Aktarımına Etkisi

Safe Harbor antlaşmasının iptali, Avusturyalı bir hukuk öğrencisi Maximillian Schrems'in *Facebook Ireland Ltd.* şirketine karşı, İrlanda Yetkili Veri Koruma Otoritesi nezdinde yaptığı başvuru ile gündeme gelmiştir. Schrems'in 25.06.2013 tarihli bu başvurusu Amerikan şirketi *Facebook Inc.*'in İrlanda'daki iştiraki *Facebook Ireland Ltd.*'nin kişisel verileri Amerika Birleşik Devletleri'ne aktararak, oradaki sunucularda depolamasına ilişkindir. Edward Snowden tarafından sızdırılan evrakta açık edildiği

[111] 2013 yılı itibariyle Bulut bilişim bazlı big data şirketi BlueKai'ın, kişisel veriler için her gün 75 milyon online müzayede yürüttüğü bilinmektedir. OECD, Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, Paris, Fransa 2013.
[112] SPIEKERMANN Sarah, BÖHME Rainer, ACQUISTI Alessandro, HUI Kai-Lung (2015), 'Personal Data Markets', Electron Markets, C. 25, s. 91–93.
[113] SCHNEIDER Jochen, Datenschutzrecht nach der EU-DSGVO, S. 325, 2. Auflage, C.H. Beck, München, Almanya 2019, s. 327.
[114] Age.
[115] KLECHA, age, s. 67.
[116] DSK Positionspaper v. 21.10.2015

üzere Amerika Birleşik Devletleri gizli servisi, Facebook tarafından aktarılan bu kişisel verilere erişmektedir.[117]

İrlanda yetkili veri koruma otoritesi Maximillian Schrems'in başvurusunu değerlendirirken, Amerika Birleşik Devletleri'nin müdahalesinin ABTHB md. 7 ve md. 8 yükümlülüklerine de *Safe Harbor* ilkelerine de aykırı olduğunu tespit ederek kararı askıya almıştır.[118] İrlanda Yüksek Mahkemesi de müdahaleyi ölçüsüz ve aşırı bularak mahremiyetin ihlal edildiğine kanaat getirmiştir. Bu noktada gündeme gelen soru ulusal veri koruma otoritelerinin Avrupa Birliği Komisyonu'nun *Safe Harbor* kararına müdahale yetkisine ilişkindir. Bir başka ifadeyle *Safe Harbor* taahhüdünde 'yeterli bir koruma' bulunup bulunmadığına ilişkin kararın, İrlanda yetkili veri koruma otoritesince verilip verilemeyeceği tartışılmıştır.

Bu soruya cevap vermek ve Amerika Birleşik Devletleri'nin kişisel verilere erişimini değerlendirmek için karar, Divan incelemesine sevk edilmiştir.[119] Divan yaptığı incelemede, üçüncü ülkelerde 'yeterli veri koruması' olup olmadığına dair kararı ancak Avrupa Birliği Komisyonu'nun verebileceğini belirtmiştir.[120] Üye devletler ise Komisyon'un üçüncü ülkelerdeki 'yeterli veri korumasına' ilişkin kararına uymakla yükümlüdür.[121]

Divan, kararın *Safe Harbor'a* ilişkin kısmında, antlaşmadan yalnızca sertifikalanmış şirketlerin yararlanabileceğini ve bu antlaşmanın Amerika Birleşik Devletleri'nin kurumları için geçerli olmadığını belirtmiştir. Dahası, Amerika Birleşik Devletleri'nin 'yeterli veri koruması' kriterlerini sağlamadığını, kişisel verilerin korunması için yeterli somut önlemler alınmadığını tespit etmiştir. Kararın devamında *Safe Harbor* Ek 1/4'deki 'ulusal güvenlik, kamu yararı veya çatışma halinde Amerikan kanunlarının üstün olacağına' dair istisna düzenlemeleri eleştirmiş, son derece geniş ve belirsiz bulmuştur.[122] İrlanda Yüksek Mahkemesi'nin başvurusunu değerlendiren Divan,

---

[117]Edward Snowden'ın sızdırdığı evraklardan anlaşıldığı şekilde Amerikan Güvenlik Ajansının siviller üzerinde yaptığı gözetime ilişkin bkz: 'Edward Snowden: the Whistleblower Behind NSA Surveillance Revelations' https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance Erişim Tarihi: 18.11.2020.

[118] MMR 2015, 753.

[119] MMR 2015, 753, 754.

[120] Divan kararda 'yeterli korumanın bulunduğuna ilişkin' değerlendirmeyi yaparken dikkate alınacak kıstasların altını bir daha çizmiştir ve bu kriterler, Tüzük düzenlenirken md. 45/2'ye de olduğu gibi alınmıştır.

[121] MMR 2015, 753.

[122] Age, kn. 83.

kararı sonucunda *Safe Harbor* antlaşmasını geçersiz kılmıştır.[123] Maximillian Schrems'in başvurusuyla başlayan bu süreç, Divan'ın yalnızca Birlik ile Amerika arasındaki kişisel veri aktarımını değil tüm ticaret hayatını da etkileyen bir karar vermesiyle sonlanmıştır.[124]

Divan kararında belirlediği 'yeterli korumanın bulunduğuna' ilişkin değerlendirme kıstasları, yalnızca Amerika için değil, tüm diğer üçüncü ülkeler için geçerlidir. Kararda şekli bir gereklilik olarak, ABTHB md. 7 ve 8 ayrımının yapılması ve taahhüt altına alınması gerektiği belirtilmiştir.[125] Esasa ilişkin belirlenen noktalardan biri, üçüncü ülkede 'yeterli veri koruması' için birebir paralelliğin aranmadığı ancak 'içerik itibariyle eşitlik'[126] gerektiğidir.[127] Kararda belirtilen önemli bir diğer husus da istisna hükümlerinin muğlak tutulmaması gerektiğidir. Öyle ki Amerika Birleşik Devleti kurumları, aktarılan kişisel verilere ancak son derece istisnai durumlarda erişebilmelidir. Dolayısıyla Amerikan kanunları ancak sınırlı uygulama alanı bulabilmelidir. Bunun yanında, kişisel verisi aktarılan Birlik vatandaşının kişisel verilerine erişim, verilerin silinmesi ve değiştirilmesi talep hakkı uygulanmalıdır. Bu hakların uygulanabilmesi için elverişli yöntemlerin belirlenmesi gerekmektedir.[128]

Yukarıda bahsi geçen kararda önem atfedilen tüm bu hususlar, Tüzük döneminde de korunmuştur. Görüldüğü üzere Tüzük'te belirlenen pek çok esas, Birlik hukukunda yıllar içerisinde meydana gelen ihtiyaçlara göre geliştirilmiştir. *Schrems I* kararından çıkarılacak temel nokta, kişisel verilerin aktarıldığı ülkede Birlik ile benzer bir korumanın somut örneklerle ispat edilmesinin gerektiğidir.

Yukarıda açıklandığı üzere *Safe Harbor* antlaşmasının iptalinden sonra, Birlik ile Amerika Birleşik Devletleri arasındaki kişisel veri aktarımını düzenlemek için *Privacy Shield* getirilmiştir. Avrupa Birliği Komisyonu'nun 2016/1250/EU kararıyla benimsenen *Privacy Shield,* Divan'ın yukarıdaki kararında belirlenen esaslar gözetilerek düzenlemiştir. Günümüzde iptal edilmiş olan *Privacy Shield'e* ve bu iptal kararına ilişkin ayrıntılı açıklama bir sonraki başlıkta yer almaktadır.

---

[123] Age, kn 67.
[124] KUNER Christopher (2017), 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', German Law Journal, C. 18, S. 4, s. 864.
[125] MMR 2015, 753, kn. 88.
[126] Age, kn. 73.
[127] Doktrinde, Divan'ın söz konusu ifadeye dair detaylı ve somut bir açıklama yapmaması eleştirilmektedir. Bkz. KLECHA, age, s. 84.
[128] MMR 2015,753 kn. 95.

1.3.2.2. AAD C-311/18 Data Protection Commissioner v. Facebook Ireland Limited, Schrems Kararı (Schrems II) ve Üçüncü Ülkelere Veri Aktarımına Etkisi

Divan yukarıda açıklanan *Schrems I* kararını takiben, 16 Temmuz 2020 tarihinde *Schrems II* adıyla anılan ikinci bir önemli karar vermiştir. Söz konusu karar temel olarak Birlik ile Amerika Birleşik Devletleri arasındaki kişisel veri aktarımı için uygulanan *Privacy Shield'e* ilişkindir. Ancak karar, Birlik'ten üçüncü ülkelere veri aktarımı için uygun bir güvenlik önlemi olan standart veri koruma maddelerine dair de önemli hususlar içermektedir. Kararın amacı ve uygun güvenlik önlemleri için belirlenen kıstasların genel niteliği düşünüldüğünde, bir diğer güvenlik önlemi olan *Binding Corporate Rules* için de geçerli sayılacaklarını söylemek mümkündür. Uygun güvenlik önlemlerinin tamamı çalışmamızın 1.3.3. başlığı altında incelenecektir.

Schrems II kararında Divan, 'verilerin aktarıldığı ülkede yeterli bir veri koruma güvenlik düzeyinin olması' kavramını, Birlik vatandaşlarının Birlik içinde sahip oldukları hak ve imkânlardan, verilerin aktarıldığı üçüncü ülkede de aynı kolaylıkta yararlanabilmeleri olarak belirlemiştir.[129] Bu kriter Divan'ın uluslararası veri aktarımına ilişkin önceki kararlarıyla da tutarlı bir görüştür.[130] Dolayısıyla yeterli bir güvenlik düzeyinin tespiti, alınan uygun güvenlik önlemleri, sahip olunan ve ilgili kişilerin kullanabilecekleri haklar ile hukuki imkânlara göre yapılmaktadır. Değerlendirmeye alınan iki diğer önemli kriter ise, verilerin aktarıldığı ülkedeki devlet otoritesinin, aktarılan verilere erişimini sağlayan iç hukuk kuralları ve genel hukuk sistemidir.[131]

Privacy Shield belirlenen bu kıstaslar üzerinden değerlendirilmiş ve Tüzük ile Avrupa Birliği Temel Haklar Bildirgesi'nde sağlanana eşdeğer bir veri korumasını taahhüt etmediğine kanaat getirilmiştir.[132] *Privacy Shield'de* Amerika Birleşik Devletleri kanunlarının uygulanacağı istisna haller olarak belirlenen ulusal güvenlik, kamu yararı veya kolluk kuvvetleri gerekçeleri geniş bulunmuştur.[133] Bunun yanında Amerikan Dış

[129] AAD C-311/18, 96, 97, 98.
[130] BOTTA Jonas (2020), 'Eine Frage des Niveaus: Angemessenheit drittstaatlicher Datenschutzregime im Lichte der Schlussanträge in „Schrems II" - Der Prüfungsmaßstab der Gleichwertigkeit und seine Reichweite im Bereich der nationalen Sicherheit', Computer und Recht, C. 36, S. 2, s. 82-89.
[131] AAD C-311/18, 103, 104, 105.
[132] 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: 20.08.2020.
[133] AAD C-311/18, 164, 165.

İstihbarat İzleme Kanunu'nda (*Foreign Intelligence Surveillance Act*), Birlik'teki kişilerin verilerine erişime dair şeffaflığın olmadığı tespit edilmiştir. Bu kanundaki pek çok hükmün, Tüzüğün amaçla sınırlılık, ölçülülük, gereklilik gibi temel ilkelerine aykırı olduğu belirlenmiştir.[134] Ayrıca bu kanuna dayanarak, Birlik'teki sivillere ait verilerin hedeflenip izlenmesi halinde ilgili kişilerin kullanabilecekleri yeterli hukuki imkân da mevcut değildir. Dolayısıyla Birlik'te sağlanan haklara eşdeğer bir korumanın var olmadığına karar verilmiş ve *Privacy Shield* iptal edilmiştir.[135]

Kararın devamında Divan standart veri koruma maddelerine dair inceleme yapmış ve geçerliliğinin devamına karar vermiştir. Bu uygun güvenlik önlemi, niteliği itibariyle kişisel veriyi Birlik'ten aktaran sorumlu ile verinin aktarıldığı üçüncü ülkedeki sorumlu/işleyen arasında sözleşmesel yükümlülük öngörmektedir. Dolayısıyla Divan kararında bu hususu belirtmiş ve üçüncü ülkedeki devlet otoritesi nezdinde bir bağlayıcılıklarının olmadığını da ortaya koymuştur.[136] Dolayısıyla standart veri koruma maddelerinin geçerliliği için bazı ek yükümlülükler belirlenmiştir.

İlk olarak verileri Birlik'ten aktaran kişinin, verilerin aktarıldığı üçüncü ülkedeki devlet otoritelerinin denetleme yetkisine dair bir iç hukuk araştırması yapması gerekmektedir.[137] Bu noktada üçüncü ülkedeki kişi, tâbi olduğu iç hukuk dolayısıyla standart veri koruma maddelerine uyamayacağını bildirebilmektedir. Araştırma sonucunda, tarafların standart veri koruma maddelerinin gereklerini yerine getiremeyecekleri belirlenirse, Birlik'teki veri sorumlusunun aktarımı durdurması ve/veya sözleşmeyi feshetmesi gerekmektedir.[138]

Divan sözleşme tarafları için öngörülen bu yükümlülüklerin yanında, verinin aktarıldığı Birlik ülkesindeki veri koruma otoritesi için de yükümlülükler öngörmektedir. Öyle ki, bu veri koruma otoritelerinin denetim yükümlülüğü mevcuttur.[139] Söz konusu veri aktarımını denetlerken üçüncü ülkede gerek devlet kurumlarının erişimi gerekse başka bir sebeple, standart veri koruma maddelerinin korunamadığını tespit ederlerse, veri aktarımını askıya alma veya yasaklama görevleri vardır.[140] Görüldüğü üzere Divan

[134] AAD C-311/18, 178, 179, 180
[135] AAD C-311/18, 185.
[136] AAD C-311/18, 125, 126, 130.
[137] AAD C-311/18, 134, 135.
[138] AAD C-311/18, 140.
[139] AAD C-311/18, 107, 108.
[140] AAD C-311/18, 113, 114.

kararında önceki kararlarla paralel şekilde, Birlik'teki veri koruma otoritelerinin sürece dahli güçlendirilmiştir.[141] Öyle ki uygun güvenlik önlemi uyarınca verilen taahhütlerle yerel mevzuatın çatıştığı durumların çoğunluğunda, Birlik hukukuna üstünlük verilmelidir.[142]

Standart veri koruma maddelerine dair ortaya konulan bu hususların, bir diğer uygun güvenlik yöntemi olan *Binding Corporate Rules* için de geçerli olduğunu söylenebilecektir. Nitekim üçüncü ülkede *Binding Corporate Rules* taahhüdü vermiş grup şirket üyelerinin iç hukuk araştırması yapmaları gerekmektedir. Araştırmayı takiben yükümlülüklerin yerine getirilip getirilemeyeceğine dair bilgilendirme yapılması gerekmektedir. Yükümlülüklerin yerine getirilemeyeceğinin tespit edilmesi halinde ise, veri aktarımının durdurulması söz konusu olacaktır. Aşağıdaki başlıkta, Tüzüğün veri aktarımı için öngördüğü tüm diğer uygun güvenlik önlemleri karşılaştırılmıştır.

1.3.3. Veri Aktarımı İçin Öngörülen Uygun Güvenlik Önlemleri

Verilerin aktarılacağı üçüncü ülkede, yeterli korumanın bulunduğuna karar verilmemişse, tarafların uygun güvenlik önlemlerinden *(ing. appropriate safeguards, alm. geeignete Garantien)* birini sağlamaları gerekmektedir. GVKT md. 46'da yer alan bu önlemler temelde, Birlik içerisindeki hak ve yükümlülüklerin verilerin aktarıldığı ülkede de korunacağını taahhüt etmektedir. Bu önlemler aynı zamanda, sürecin Birlik ülkelerindeki yetkili veri koruma otoritelerince izlenmesi ve denetlenmesini de sağlamaktadır.[143]

Tüzük'te öngörülen yedi uygun güvenlik önlemi, iki temel başlık altında toplanabilmektedir. Şöyle ki ilk grupta, Birlik'teki yetkili veri koruma otoritelerinin ek iznine tâbi olan önlemler yer almaktadır. Bu önlemler, verinin aktarıldığı üçüncü ülkedeki veri sorumlusu/işleyenle imzalanacak sözleşme maddeleri (GVKT md. 46/3/a) ve kamu makamlarınca veri sahiplerinin haklarını içerir düzenlemelerdir (GVKT md. 46/3/b). İlk grupta yer alan bu önlemler, daha masraflı ve yavaş kaldığından, uygulamada pek tercih edilmemektedirler ve bu çalışma içerisinde de incelenmeyecektir.

---

[141] BOTTA, age, s. 82-29.
[142] BCR taahhütleriyle yerel mevzuatın çatıştığı durumlarda izlenmesi öngörülmüş yollara için çalışmanın 2.3.1.13. başlığına bakınız.
[143] *Paal'e ait kısım*, PAAL, PAULY, age, s. 557.

Yetkili veri koruma otoritelerinin ek iznine tâbi olmayan, ikinci gruptaki önlemler ise kırk altıncı maddenin ikinci fıkrasında aşağıdaki gibi sıralanmaktadır.[144]

- Kamu makamları arasında hukuki bağlayıcılığı olan bir araç;
- Md. 47 uyarınca *Binding Corporate Rules;*
- Avrupa Birliği Komisyonu tarafından belirlenen yahut yerel veri koruma otoritelerince belirlenip Komisyonca onaylanan standart veri koruma maddeleri;
- Md. 40 uyarınca onaylanmış davranış kuralları;
- Md. 42 uyarınca onaylanmış sertifikalar.

1.3.3.1. Binding Corporate Rules

GVKT md. 46/2/b *Binding Corporate Rules'u* üçüncü ülkelere veri aktarımı için uygun güvenlik önlemlerinden biri olarak saymıştır. İçeriğine ve onay sürecine dair açıklamalar ise GVKT md. 47'de yer almaktadır. Çalışmamızda *Binding Corporate Rules'u*n içeriğine ve onay süreçlerine dair ayrıntılı açıklamalar ikinci bölüme bırakılmıştır. Bu başlık altında ise uygun güvenlik önlemi niteliğine dair genel bir değerlendirme yapılacaktır.

Tüzük'te grup şirket yahut ekonomik iş birliği halindeki teşebbüslerin *Binding Corporate Rules* hazırlayabilecekleri öngörülmüştür.[145] Tüzük'te öngörülen yükümlülükleri taahhüt eden bu kurallar, grup şirketin ihtiyaçlarına göre ve şirket bünyesindeki tüm kuruluşlar için bağlayıcı olarak hazırlanmaktadır. Yetkili veri koruma otoritesince onaylanıp yürürlüğe giren *Binding Corporate Rules,* grup şirket içerisinde yapılacak tüm veri aktarımları için uygun bir güvenlik önlemi teşkil etmektedir. Bu anlamda global bir şirket yapısının *Binding Corporate Rules* düzenlemesi avantajlı olacaktır. Öyle ki, grup şirketin veri koruma politikası dünya çapında yeknesak şekilde ve Tüzüğün öngördüğü standartlarda belirlenecektir. Grup şirket ağında, ek bir izne gerek olmaksızın serbest veri dolaşımı yapılabilecektir.[146]

---

[144] SCHNEIDER, age, s. 325.

[145] Hangi şirket yapılanmalarının BCR düzenleyebileceğine ilişkin ayrıntılı açıklama çalışmamızın 2.3. başlığında yer almaktadır.

[146] BOWMAN John, GUFFLET Myriam (2017), 'Meeting the Challenge of a Global GDPR and BCR Programme', European Data Protection Law Review, C. 3, S. 2, s. 257-261.

Binding Corporate Rules ancak grup şirket yapısına dahil kuruluşlar arasındaki aktarımlarda uygun güvenlik önlemi teşkil etmektedir. Öyle ki şirket yapısı içerisindeki herhangi bir kuruluş, yeterli korumanın bulunmadığı üçüncü bir ülkedeki başka bir sorumluya veri aktarırken, GVKT md. 46 uyarınca belirlenen diğer uygun güvenlik önlemlerinden birini almalıdır.[147]

Binding Corporate Rules belirli hallerde daha zorlu bir yöntem sayılabilecek standart veri koruma maddelerine alternatif oluşturabilmektedir.[148] Öyle ki global bir grup şirketin üyeleri arasındaki, pek çok farklı kategorideki kişisel verileri aktarımlarının standart veri koruma maddeleriyle düzenlenmesi daha zorlu bir süreç yaratabilmektedir. Bu önlemlerin her ikisi de sözleşmesel taahhüt niteliğindedir. Ancak *Binding Corporate Rules* ile aktarılacak verilerin çeşidinde bir sınırlamaya gidilmemektedir. Bu önlem, olası tüm veri aktarımları dahil olacak şekilde tüm veri işleme faaliyetlerine *ex post* uygulanabilir biçimde tasarlanmaktadır.[149] Standart veri koruma maddeleri ise aktarılacak verinin niteliğine göre, verinin aktarılacağı karşılıklı iki taraf arasında düzenlenmektedir. Bu anlamda grup şirket üyelerinin zincir şeklinde yapacakları aktarımlarda, her aktarım öncesinde baştan düzenlenmeleri gündeme gelebilecektir. Dolayısıyla söz konusu grup şirket *Binding Corporate Rules* düzenleyebilecek bir yapılanmaya sahipse, grup içi aktarımlar için bu önlemin alınması daha avantajlı olacaktır.

1.3.3.2. Standart Veri Koruma Maddeleri

Standart veri koruma maddeleri *(ing. standard data protection clauses)* GVKT md. 46/2/c'de üçüncü ülkelerdeki kişilere veri aktarımı için uygun bir güvenlik önlemi sayılmaktadır. Bu maddeler, istisnai şekilde diğer sözleşme yükümlülüklerinin önüne geçmekte ve üçüncü ülkelerde de Tüzük korumasını sağlamaktadır. Bu önlem için Avrupa Birliği Komisyonu'nca geliştirilmiş sözleşmeler yahut üçüncü kişilerce önerilip Komisyon tarafından onaylanan sözleşmeler kullanılabilmektedir.[150] Çalışmamızın tarihi itibariyle, Komisyon tarafından 'standart sözleşme maddeleri *(ing. standard contractual clauses)*' adıyla düzenlenmiş üç adet sözleşme mevcuttur. Bu üç matbu sözleşme, farklı

[147] WAGNER, age, s. 318-337.
[148] BOWMAN, GUFFLET, age, s. 257-261.
[149] MATTOO, MELTZER, age, s. 769-789.
[150] *Paal'e ait kısım,* PAAL, PAULY, age, s. 562.

veri işleme amaçları için öngörülmüştür ve GVKT md. 46/2/c uyarınca uygun güvenlik önlemi sayılmaktadır.[151]

Direktif döneminde de mevcut olan sözleşmeler, veri aktarımının hukuka uygunluğunun hâlihazırda yetkili mercilerce teyit edildiğini göstermektedir. Şüphesiz ki, uygun güvenlik önleminin hızlı uygulanabilirliği, sözleşme tarafları için bir avantajdır. Bunun yanında, idari süreçlerin belirsizliğini de ortadan kaldıran standart veri koruma maddeleri, taraflara yüksek bir koruma sağlamaktadır.[152]

Komisyon tarafından hazırlanan standart sözleşme maddeleri güncel hallerinde, geliştirilmiş ve uygulamada sorun yaratan kısımları giderilmeye çalışılmıştır.[153] Şöyle ki bu sözleşmeler taraflar için son derece kati ve somut yükümlülükler öngörmekte ve yoruma yer bırakmamaktadır.[154] Bu anlamda esas faaliyeti veri işlemek olmayan, küçük orta çaplı veri sorumluları için uygun bir önlemdir.[155] Ancak hâlihazırda yerleşik veri aktarımı mekanizmaları ve gizlilik politikaları mevcut olan, büyük çaplı global organizasyonların ihtiyaçlarını karşılayamamaktadır.

Nitekim Avrupa Birliği Komisyonu tarafından hazırlanmış bu sözleşmeler, tarihleri itibariyle dijital çağın getirdiği teknolojik yenilikler yönünden eksiktir. Göze çarpan hususlardan ilki, pek çok şirket için vazgeçilmez hale gelmiş bulut bilişim *(ing. cloud)* sistemlerinin bu sözleşmelerde eksik oluşudur.

Bu husus haricinde matbu sözleşmelerin tek bir amaca yönelik yazılması dolayısıyla, farklı amaçlar için yapılan veri aktarımlarında birden fazla sözleşme imzalanmaktadır.[156] Öyle ki, bu durum hukuki olarak gerekli olandan daha fazla taahhüt verilmesini de beraberinde getirmektedir. Bu durumlarda, şirketlerin kendi politikalarına göre hazırlanabilen ve her tür veri aktarımı sürecini taahhüt eden diğer alternatifler daha avantajlıdır.

---

[151] SET I; ABI. EG 2001 L 181,19;
SET II; ABI. EG 2004 L 385, 74;
ADV; ABI. EU 2010 L 39,5.
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en Erişim Tarihi: 07.03.2020.

[152] Age.

[153] *Schantz'a ait kısım* SIMITIS Spiros, HORNUNG Gerrit, SPIECKER Indra, Datenschutzrecht DSGVO mit BDSG, 1. Auflage, Nomos Verlag, Baden-Baden, Almanya 2019, s. 998 vd.

[154] Age.

[155] Data Protection and Brexit https://ico.org.uk/for-organisations/data-protection-and-brexit/keep-data-flowing-from-the-eea-to-the-uk-interactive-tool/ Erişim Tarihi: 07.03.2020.

[156] Örnek olarak uluslararası ticaret odası görüşleriyle, ticarete elverişli olarak geliştirilen SET II sözleşme, işçi verilerinin aktarılmasına izin vermemektedir. Şayet isçi verileri de aktarılacaksa, ek olarak SET I sözleşmesinin de imzalanması gerekmektedir. *Paal'e ait kısım*, PAAL, PAULY, age, s. 564.

Bu noktada belirtilmesi gereken bir husus da Divan'ın 16 Temmuz 2020 tarihli *Schrems II* kararıdır. Çalışmamızın 1.3.2.2. başlığında ayrıntısıyla incelenen bu karar, standart sözleşme maddelerinin uygulamasına dair de önemli hususlar içermektedir. Karardan sonra standart sözleşme maddelerini imzalayan taraflara, üçüncü ülkedeki veri koruması kurallarına dair araştırma yükümlülüğü getirilmiştir. Taraflar üçüncü ülkedeki devlet otoritelerinin aktarılan kişisel veriler üzerindeki denetim yetkisini de araştırmakla yükümlüdür. Araştırma sonucunda standart sözleşme maddeleri gereklerinin yerine getirilemeyeceği belirlenirse, sözleşme feshedilmeli ve/veya aktarım durdurulmalıdır.[157] Karar aynı zamanda Birlik'teki veri koruma otoritelerinin de denetim yetkisi ve görevini güçlendirmektedir. Birlik veri koruma otoriteleri üçüncü ülkede standart sözleşme maddelerinin korunmadığını tespit ederlerse aktarımı durdurabilecek veya yasaklayabileceklerdir.[158]

1.3.3.3. Davranış Kuralları

Çalışmamızın 1.3.2.1. ve 1.3.2.2. başlıklarında ortaya konulduğu üzere Amerikan hukukunda, sektörel veri koruması kuralları mevcuttur. Benzer şekilde sektörel bir düzenleme olan davranış kuralları *(ing. codes of conduct)* Birlik hukukunda GVKT md. 40 ile düzenlenmiştir.[159] Davranış kuralları, veri sorumlusu/işleyen üyelerini temsile yetkili bir sektör veya ticari birliklerinin, sektörün özel ihtiyaçlarını gözeterek hazırladıkları önceden onaylanmış araçlardır. Hazırlayan birliğe üye veri sorumluları/işleyenler istedikleri takdirde, davranış kurallarına uymayı taahhüt ederek, bu kurallara kendileri için hukuki bağlayıcılık kazandırabilmektedirler. Bundandır ki davranış kuralları esasında, hesap verilebilirliği arttıran ihtiyari uyum araçlarıdır.

Davranış kuralları, aktarma dahil tüm veri işleme süreçlerini içerir şekilde hazırlandıklarından, GVKT md. 46/2/e'de üçüncü ülkelere veri aktarımında uygun bir güvenlik önlemi olarak sayılmaktadırlar. Şöyle ki, bir davranış kuralının Tüzüğe göre uygun güvenlik önlemi teşkil edebilmesi için üç yükümlülüğü yerine getirmesi gerekmektedir. Buna göre; GVKT md. 40'da sayıldığı şekilde belirlenen veri koruma

[157] AAD C-311/18, 140.
[158] AAD C-311/18, 113, 114.
[159] Age, s. 566.

ilkelerini taahhüt etmelidir; GVKT md. 55 uyarınca yetkili veri koruma otoritesi veya Avrupa Birliği Komisyonunca onaylanmalıdır; hukuki bağlayıcılığı olmalıdır.

Davranış Kuralları, meslek odaları veya birlikler gibi kurumlarca sektör bazında hazırlandığından, söz konusu sektörün belirli ihtiyaçlarına göre geliştirilmektedirler. Bunun yanında hazırlandıkları ticari birliğin üyeleri veri sorumluları/işleyenler için hızlı ve görece hesaplı bir uyum yöntemidirler. Ek olarak yetkili veri koruma otoritesince onaylandıklarından, davranış kurallarına uymayı taahhüt eden veri sorumluları/işleyenlerinin yetkili otorite nezdinde güvenilirliklerini arttırmaktadırlar.[160] Bu anlamda davranış kuralları şeffaflık ve hesap verilebilirlik ilkelerine hizmet etmektedir.

Dolayısıyla veri sorumlusunun/işleyenin üyesi olduğu meslek birliği davranış kuralı hazırlamışsa, bunun veri sorumlusu şirketçe taahhüt edilmesi pek çok açıdan avantajlıdır. Ancak veri sorumlusu/işleyenin özellikle devamını talep ettiği yerleşik bir politikası veya özel bir yapılanması mevcutsa, veri aktarımı için başka uygun güvenlik önlemleri düşünülebilir.

1.3.3.4. Sertifikalar

Sertifikalar *(ing. certification)* veri sorumlusu veya işleyenin Tüzüğe uyumluluğunu gösterir damga/mühürlerdir. GVKT md. 42/5 uyarınca üye devletlerin yetkili veri koruma otoriteleri veya GVKT md. 43. uyarınca yetkili sertifika kuruluşları tarafından verilmektedirler.[161] Üçüncü ülkelerdeki veri sorumlusu/işleyenlerin sertifika alması halinde, bu sertifika Birlik'ten kendisine yapılacak veri aktarımlarında GVKT md. 46/2/f uyarınca uygun güvenlik önlemi niteliğindedir.

Sertifika almak isteyen üçüncü ülkelerdeki veri sorumlularının/işleyenlerinin kümülatif olarak dört yükümlülüğü yerine getirmeleri gerekmektedir.[162] Sertifika kriterleri, Avrupa Birliği Komisyonunca onaylandığı şekliyle belirlenen veri koruma ilkelerini içermelidir. Sertifika, Tüzüğün yetkili addettiği akredite bir kuruluş veya Birlik Kurulu tarafından verilmelidir. Üçüncü ülkedeki veri sorumlusu/işleyen, Tüzüğün

[160] Guide to Codes of Conduct https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/ Erişim Tarihi: 08.03.2020

[161] Tüzüğün 63. maddesi uyarınca Birlik Kurulu tarafından verilen yaygın bir sertifika olarak bkz. European Data Protection Seal.

[162] *Paal'e ait kısım,* PAAL, PAULY, age, s. 567.

öngördüğü yükümlülükleri taahhüt etmelidir. Son olarak sertifika kriterlerinin, üçüncü ülkedeki veri sorumlusu/işleyen için hukuki bağlayıcılığı aranmaktadır.

Birlik'te yerleşik bir veri sorumlusu/işleyen için sertifikanın sağladığı en büyük avantaj, potansiyel denetim masraflarının azalmasıdır. Bunun yanında veri sahipleri nezdinde yaratılan güven, bir pazarlama avantajı da taşıyabilir.[163] Üçüncü ülkelerdeki veri sorumluları/işleyenleri için ise elbette ki, taşıdığı avantaj daha büyüktür. Birlik'ten yapılacak veri aktarımları için hâlihazırda uygun bir güvenlik önleminin varlığı, üçüncü ülkedeki sorumluları olumlu bir seçenek haline getirecektir. Öyle ki, veri işleme süreçlerinin maliyet uygunluğu amacıyla *outsource* edildiği durumlarda, üçüncü ülkelerdeki sorumlular için sertifikaların ticari önemini vurgulamak gerekir.

Sertifika süreçlerinin Birlik hukukunda, Tüzük öncesi dönemde de yaygın biçimde kullanıldığı belirtilmelidir. Nitekim Birlik içerisinde 2013 yılı itibariyle verilmiş veri koruma sertifikalarına bakıldığında[164], altı farklı ülke tarafından çeşitli uyumlulukları gösteren farklı isimlerle verilmiş neredeyse toplam beş yüz sertifika olduğu görülmektedir. Bunlardan en yaygın olanı, sertifika yöntemini benimseyen ilk ülke olan Almanya'nın verdiği gizlilik mührü *(ing. Privacy Seal, alm. Gültesiegel)* sertifikasıdır. Belirtmek gerekir ki, yerleşik bu yöntemin Tüzük içerisinde yeknesak biçimde düzenlemesi, pratik uygulanabilirlik açısından doktrinde tartışılmaktadır.[165]

Görüldüğü üzere Tüzük, üçüncü ülkelere veri aktarımı için pek ihtiyaca göre değişen çeşitli uygun güvenlik önlemleri belirlemiştir. Bunlar şirket özelinde değerlendirilerek, ihtiyaca cevap vereni seçilmelidir. Uygun güvenlik önlemlerinin Türkiye'deki şirketler için anlamına bakıldığında, çalışmamızın konusunu oluşturan *Binding Corporate Rules*, pek çok açıdan önem arz etmektedir. İlk senaryoda, global bir yapının Türkiye'deki üyesi veri sorumlusu/işleyene uygun güvenlik önlemi niteliğindeki *Binding Corporate Rules* iletilip, buna uyması beklenecektir. Bu halde Türkiye'deki şirket için bağlayıcı olacak *Binding Corporate Rules'a* bir uyum süreci yönetilecektir. Öyle ki hem tâbi olunan Türk iç hukukuna hem de Binding Corporate Rules yükümlülüklerine uyulmalıdır.

---

[163] GDPR Certification https://www.eugdpr.institute/gdpr-certification/ Erişim Tarihi: 09.03.2020
[164] Data Protection Schemes Active in Europe https://www.researchgate.net/figure/Data-protection-certification-schemes-active-in-Europe-in-2016_tbl1_305821630 Erişim Tarihi: 29.04.2020.
[165] LACHAUD Eric (2016), 'Why the Certification Process Defined in the GDPR Cannot Be Successful', Computer Law & Security Review, C. 32, s. 814–826.

Bundan başka, Türkiye'de kurulu ancak Birlik'te üyeleri olan global bir grup şirketin kendi Bağlayıcı Şirket Kurallarını düzenlemesi gündeme gelebilir. Bu halde düzenlenecek Bağlayıcı Şirket Kuralları Türk hukuku açısından global şirket bünyesinde serbest veri akışını sağlayacaktır. Düzenlenen Bağlayıcı Şirket Kurallarının, Birlik'te akredite bir kuruluştan GVKT md. 46/2/f uyarınca sertifikalanması da düşünebilir. Öyle ki bu durumda Türkiye'de hazırlanan Bağlayıcı Şirket Kuralları, Birlik'ten yapılacak veri aktarımları için de Tüzüğe göre uygun güvenlik önlemi niteliği kazanacaktır. Tüm bu ihtimaller çalışmamızın devamında ayrıntısıyla incelenecektir.

BÖLÜM 2. BINDING CORPORATE RULES

Binding Corporate Rules global grup şirketlerin kendi içerisindeki veri yönetimlerini, yeterli ve aynı koruma düzeyinde taahhüt eden metinlerdir. Bu metinler grup şirketin tüm üyeleri için bağlayıcıdır ve her birinin tüm veri işleme faaliyetlerine uygulanmaktadır. *Binding Corporate Rules* düzenleyen grup şirketin veri işleme sürecini gözeterek, ihtiyaçlarına göre hazırlanmakta ve yetkili veri otoritesince onaylanmaktadır. Dolayısıyla grup şirket bünyesinde eşit ve Tüzüğe uygun veri korumasını taahhüt eden bu metinler, grup şirket içerisinde serbest veri dolaşımını sağlamaktadır.[166]

Veri korumasını şirket düzeyinde taahhüt eden bu uygulamalar yalnızca Birlik hukukunda değil, pek çok farklı hukuk sisteminde de mevcuttur.[167] Çalışmamız Birlik hukukuna odaklandığından, temel incelememiz Tüzük içerisindeki *Binding Corporate Rules'a* yönelecektir. Birlik hukukundaki uygulamadan bahsedildiğini ayırt etmek adına, *Binding Corporate Rules* terimi İngilizce bırakılmıştır. Karşılaştırmanın yararlı olacağı noktalarda üçüncü ülkeler ve hukuk sistemlerindeki farklı isimli benzer düzenlemeler incelenecektir. Çalışmamızın üçüncü bölümü altında ise Türkiye'deki paralel Bağlayıcı Şirket Kuralları değerlendirilecektir.

Birlik hukukunda *Binding Corporate Rules,* Direktif döneminde Md. 29 Çalışma Grubu kararlarıyla benimsenmiştir. Direktif içerisinde yazılı olarak düzenlenmeyen *Binding Corporate Rules,* davranış kurallarından geliştirilmiştir ve ilk defa Tüzük içerisinde kanuni düzenleme bulmuştur. Tüzük'te grup şirketlerin yahut ekonomik iş birliği halindeki teşebbüslerin *Binding Corporate Rules* düzenlemelerinden yararlanabileceği yazılmış ve md. 47 ile geçerlilik koşul ve şartları belirlenmiştir.

Çalışmamızın bu bölümü altında, *Binding Corporate Rules'un* düzenlenme amaç ve avantajları belirlenecek ve Birlik hukuku içerisindeki tarihi gelişimi incelenecektir. Bundan sonra *Binding Corporate Rules* süreçleri Tüzük özelinde değerlendirilecek ve

[166] MASOCH Daniela (2019), 'Why Should Companies Invest in Binding Corporate Rules?' ICLG.com online journal, publishing date 03.07.2019.
[167] SULLIVAN Claire (2019), '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. 35, s. 380-397.

geçerlilik koşul ve şartları, içeriği ile onay prosedürü ele alınacaktır. Son olarak, *Binding Corporate Rules* benzeri taahhütler karşılaştırmalı hukukta ele alınacak ve Birlik dışından seçilen örnek ülke ve hukuk sistemleri incelenecektir.

2.1. BINDING CORPORATE RULES AMAÇ VE AVANTAJLARI

Binding Corporate Rules, grup şirket tarafından kendi ihtiyaçları gözetilerek *(ing. tailor made)* hazırlanmaktadır. Global grup şirketin bünyesinde yer alan tüm kuruluşlar için bağlayıcı şekilde düzenlenen metin, üyelerin her birinin Tüzüğe uyumunu göstermektedir. Tüzüğün öngördüğü şekilde hazırlanıp onaylatılmış *Binding Corporate Rules*, grup şirket içerisindeki veri aktarımlarında uygun bir güvenlik önlemi sayılmaktadır. Dolayısıyla şirket bünyesinde yer alan tüm kuruluşlar arasında kişisel verilerin serbest akışını sağlamaktadır. Grup şirket bünyesinde dünya çapında, Tüzük ile uyumlu aynı veri koruma standardının belirlenmesi, çok daha kolay ve işler bir süreç yaratmaktadır. Öyle ki, uyum süreci çalışanlarca daha kolay yönetilebilir ve ilgili kişilerce de daha rahat anlaşılabilir hale gelmektedir.[168]

Taşıdığı bu avantajlarla *Binding Corporate Rules*, uluslararası veri aktarımı için uygun bir güvenlik önleminden daha fazlasıdır. Şirkete özel düzenlenip dünya çapında aynı korumayı taahhüt eden *Binding Corporate Rules*, grup şirketin tamamında şeffaf bir veri işleme uyum sürecinin temelini oluşturabilecektir.[169] O kadar ki, eğer grup şirket yapısının tek amacı, şirket içerisinde serbest veri akışı yaratmaksa, *Intra Group Data Transfer Agreement* gibi sözleşme yöntemleriyle görece küçük çaplı, daha ucuz alternatifler düşünülebilir.[170] Bu alternatif, çalışmamızın 1.3.3.2. başlığında incelenen standart veri koruma maddeleri altında hukuka uygun veri aktarımı sağlamaktadır. Bilindiği üzere *Binding Corporate Rules*, grup şirket bünyesindeki tüm üyelerin tüm veri işleme faaliyetlerini düzenleyen geniş çaplı bir uyum projesini gerektirmektedir. Bu anlamda *Intra Group Data Transfer Agreements*, grup şirket üyelerinin sadece kendi aralarındaki küçük çaplı veri aktarımı için uygun bir alternatiftir (ör. iki üye şirketin insan kaynakları bölümleri arasındaki veri aktarımları).

[168] *Zerdick'e ait kısım,* EHMANN, SELMAYR, age, s. 694.
[169] BOWMAN, GUFFLET, age, s. 257-261.
[170] MASOCH, age.

GVKT md. 5/2 uyarınca veri sorumluları, veri işleme ilkelerine uyulduğuna dair hesap verilebilirliği sağlamakla yükümlüdürler. *Binding Corporate Rules'un* önemli amaçlarından biri, grup şirket bünyesinde hesap verilebilirliği sağlamak ve ispat edebilmektir. Bu anlamda sağladıkları en büyük avantajlardan biri de kanun ile uyumu *(ing. compliance)* göstermektir. O kadar ki, hukuk muhakemesi kuralları uyarınca yahut idari yargılamalarda *Binding Corporate Rules,* geçerli bir ispat aracı sayılmaktadır.[171]

Bu düzenlemelerin, mahremiyet ve veri koruması gerekliliklerine dair şirket içi bilinç, anlayış ve hassasiyeti de arttırdığı bilinmektedir. Zira *Binding Corporate Rules* şirket içerisinde veri korumasıyla ilgilenecek ayrı bir bölümün yapılandırılmasını ve mahremiyetin şirket kültürüne daimî olarak dahil edilmesini gerektirmektedir. Dolayısıyla potansiyel hukuka aykırılıklar sonucunda, veri sorumlusu hakkında verilecek idari para cezaları da azalmaktadır.[172] *Binding Corporate Rules*, kapsamlı ve işler bir veri koruma kültürünün yerleştirilmesi için, şirket içinde aşağıda sayılanlar dahil ancak bunlarla sınırlı olmayacak şekilde ayrıntılı yöntemler öngörmektedir:

a. Hazırlanan veri koruması uyum projesinin gözlem ve denetimi için bir yönetim biriminin kurulması;
b. Kişisel verinin adil ve hukuka uygun işlenmesini sağlamak için politikalar (şirket iç yönergeleri) hazırlanması;
c. Şeffaflık adına veri sahiplerine yeterli bilgi ve bildirimlerin yapılması;
d. Veri koruması uyum projesi dahilinde ve işleme süreçlerinde risk değerlendirmesinin yapılması ve riskin yönetimi;
e. Kişisel verileri işleyen çalışanlara, periyodik bilgilendirme yapılması ve eğitimler verilmesi;
f. İç ve dış denetimlerle veri koruması kurallarına uyulduğunun (compliance) denetlenmesi;
g. İlgili kişilerin soru ve taleplerine hızlı ve yeterli şekilde cevap verilebilmesi için uygun yönetim bölümlerinin kurulması.

[171] *Wieczorek'e ait kısım,* SPECHT, MANTZ, age, s. 176.
[172] MASOCH, age.

Bu anlamda bakıldığında *Binding Corporate Rules,* grup şirketin veri yönetimi politikalarının resmîleştirilip yayınlanmasıdır. Bu kurallar kanun koyucu, iş ortakları ve müşteriler nezdinde hesap verilebilirliği sağlamaktadır. Dolayısıyla *Binding Corporate Rules* düzenlememiş rakip şirketler üstünde ciddi bir ticari rekabet avantajı da taşımaktadır.[173]

Binding Corporate Rules taahhütleri şirket özelinde hazırlanıp onaylandıklarından ve yeni yapılanmalar gerektirdiğinden görece masraflı ve uzun bir süreçtir. Ancak yukarıda gösterildiği şekilde, süreç sonunda şirkete büyük avantajlar sağlayabilmektedir. Getirebileceği avantajlar, grup şirketin ihtiyaçları doğrultusunda değerlendirilmeli ve *Binding Corporate Rules* düzenlemesine değip değmeyeceği belirlenmelidir.[174]

2.2. BINDING CORPORATE RULES TARİHÇESİ

Dijitalleşmenin getirdiği önemli gelişmelerden biri olarak veri aktarımları artık eskisi gibi bir noktadan diğerine (sabit hatlarla) yapılmamaktadır. Günümüzde veriler, birçok bilgisayarın özel bir ağ yahut internet üzerinden iletişimiyle aktarılmaktadır.[175] Bu gelişme elbette ki global şirketlerin veri yönetimi süreçlerine de yansımıştır. Çok uluslu şirketler günümüzde, yapılandıkları farklı konumlarının her birinde yerel bilgi işlem sistemleri kurmamaktadırlar. Hem maliyetten tasarruf hem de pratik getirileri açısından müşteri ve çalışan verileri, çoğunlukla kurulan merkez bilgi işlem sisteminde saklanmaktadır. Bu gelişmeler dolayısıyla, grup şirket arasında özel bir ağ yahut internet üzerinden daimî bir veri akışı söz konusudur.

Yukarıdaki hususların yanında veri aktarımı konusundaki sorunlar, *dynamic routing*[176] (tr. dinamik yönlendirme) ve *cloud computing* (tr. bulut bilişim) sistemlerinin yaygınlaşmasıyla artmıştır. Bulut bilişimin niteliği itibariyle veriler bir 'bulutta' işlenmektedir ve statik şekilde belirli bir yerde tutulmamaktadır. Bu sistemler dolayısıyla verilerin internet üzerinden hangi ülkelere yönlendirilip aktarıldığı; hangi ülkelerde

[173] MASOCH, age.
[174] KULEZSA, Joanna (2014), 'Transboundary data protection and international business compliance', International Data Privacy Law, C. 4, S. 4, s. 298 – 306.
[175] MOEREL Lokke, Binding Corporate Rules: Corporate Self Regulation of Global Data Transfers, Oxford University Press, Birleşik Krallık 2012.
[176] Dinamik yönlendirme sistemi, verilerin belirlenmiş bir yörünge üzerinde kalan ağ içerisinde işlendiği statik yönlendirmenin zıttı niteliğindedir. Dinamik yönlendirmeyle verilerin internet üzerinden nereye yönlendirildiği öngörülememektedir.

depolandığı öngörülememektedir. Bundandır ki farklı yerel mevzuatlara tâbi olan global şirketlerin veri aktarımının şeffaf ve yeknesak şekilde düzenlenmesi son derece önemlidir. *Binding Corporate Rules'un* Birlik hukuku içerisindeki gelişimi, çok uluslu grup şirketlerin veri aktarımlarındaki sorunları çözmek amacıyla, Direktif döneminde başlamıştır.

Md. 29 Çalışma Grubu kararlarıyla Direktif'in 26. ve 29. maddelerince geliştirilen *Binding Corporate Rules*, Direktif'te ismen yer almamaktadır. Ancak Tüzük öncesindeki dönemde dahi, doktrin ve uygulama tarafından *Binding Corporate Rules* ismiyle anılmıştır.[177] Bu taahhütler Tüzük'te de, Md. 29 Çalışma Grubu kararlarıyla belirlenen esaslar geliştirilerek *Binding Corporate Rules* ismiyle düzenlenmiştir.[178] Bu nedenle aşağıda ilk olarak, Direktif döneminde Md. 29 Çalışma Grubu tarafından yayınlanan kataloglar ve kılavuzlar incelenecektir. Sonrasında onaylanan ilk *Binding Corporate Rules* olan Daimler Crysler şirketinin taahhütleri ve süreç değerlendirilecektir.

2.2.1. 95/46 Direktif Dönemi ve Md. 29 Çalışma Grubu Karar Kataloğu

Direktifin yürürlükte olduğu dönemde geliştirilen *Binding Corporate Rules'a* dair pek çok Md. 29 Çalışma Grubu kararı, tavsiyesi ve görüşü mevcuttur. Tüzüğün yürürlüğe girmesiyle Md. 29 Çalışma Grubu ortadan kaldırılmış ve yerine Birlik Kurulu getirilmiştir. Ancak Md. 29 Çalışma Grubu tarafından hazırlanan evrak günümüzde de önem taşımaktadır. Öyle ki *Binding Corporate Rules* Tüzük içerisinde düzenlenirken bu dokümanlardan yararlanılmıştır. Ek olarak Direktif döneminde onaylanmış *Binding Corporate Rules*[179], hukuk güvenliği açısından Tüzüğün yürürlüğe girmesinden sonra da hukuka uygun sayılmaktadır.[180] Yukarıdaki hususların yanında belirtilmelidir ki Md. 29 Çalışma Grubu tarafından yayınlanan evrakın bir kısmı, Birlik Kurulu'nca desteklenmekte ve halen kullanılmaktadır.

---

[177] Direktif döneminde, Md. 29 Çalışma Grubu kararları bugün *Binding Corporate Rules* olarak bildiğimiz taahhütler için farklı çeviriler kullanabilmekteydi. Tüzüğün Almanca çevirisinde *verbindliche interne Datenschutzvorschriften* olarak adlandırılan taahhütler, Md. 29 Çalışma Grubu kararlarında *verbindliche Unternehmensregelungen* olarak adlandırılmaktaydı.

[178] *Schröder'e ait kısım,* KÜHLING. BUCHNER, age, s. 864.

[179] Tüzüğün yürürlüğe girmesinden önce Direktif döneminde hazırlanıp onay süreçleri biten BCR listesi için bkz. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841 Erişim Tarihi: 19.03.2020.

[180] Tüzük yürürlüğe girmeden hazırlanıp onaylanmış BCR, yetkili veri koruma otoritelerince iptal edilmediği sürece hukuka uygun sayılmaktadır. Nitekim onay süreçlerini Tüzüğün yürürlüğe girmesinden önce tamamlayan pek çok şirket, hala bu taahhüt metinlerini kullanmaktadır.

Direktif döneminde *Binding Corporate Rules'a* dair hazırlanan tüm evrak *(Working Paper ('WP')),* Md. 29 Çalışma Grubu arşivinde[181] aşağıdaki şekilde yer almaktadır;

- 2015 yılında WP 204 içerisinde yayınlanan *'Veri İşleyen Binding Corporate Rules'una dair açıklayıcı evrak';*
- 2014 yılında WP 212 içerisinde yayınlanan *'Birlik içerisindeki yetkili veri koruma otoritesine sunulacak Binding Corporate Rules ve Sınırötesi Mahremiyet Kuralları kapsamında Asya-Pasifik Ekonomik İş birliği hesap verilebilirlik görevlilerine (ing. accountability agents) sunulacak Binding Corporate Rules için atıflar'* hakkında 02/2014 sayılı görüş;
- 2013 yılında WP 204 içerisinde yayınlanan *'veri işleyen Binding Corporate Rules'una ilişkin açıklayıcı evrak'*;
- 2012 yılında WP 195 içerisinde yayınlanan *'veri işleyen Binding Corporate Rules'unda bulunması gereken ilkeler ve nitelikler'* tablosunu içerir 02/2012 sayılı bildiri çalışması;
- 2012 yılında WP 195a içerisinde yayınlanan *'veri işleme faaliyetleri için yapılacak veri aktarımlarına dair hazırlanan Binding Corporate Rules için standart başvuru formu'* konulu ve 01/2012 sayılı tavsiye;
- 2008 yılında WP 155 içerisinde yayınlanan *'Binding Corporate Rules'a dair sıkça sorulan sorular'* konulu bildiri çalışması;
- 2008 yılında WP 154 içerisinde yayınlanan *'Binding Corporate Rules yapısı için bir çerçeve oluşturulması'* konulu bildiri çalışması;
- 2008 yılında WP 153 içerisinde yayınlanan *'Binding Corporate Rules içerisinde bulunacak ilkeler ve nitelikleri içerir tablo'* konulu bildiri çalışması;
- 2007 yılında WP 133 içerisinde yayınlanan '*veri aktarımı faaliyetleri için hazırlanan Binding Corporate Rules standart başvuru formu*' konulu ve 1/2007 sayılı tavsiye;

[181] Md. 29 Çalışma Grubu görüşleri için arşiv https://ec.europa.eu/justice/article-29/documentation/opinion- recommendation/index_en.htm#maincontentSec21 Erişim Tarihi 19.03.2020.

- 2005 yılında WP 108 içerisinde yayınlanan *'Binding Corporate Rules onayı için başvurularda kullanılacak matbu bir kontrol listesi'* konulu bildiri çalışması;
- 2005 yılında WP 107 içerisinde yayınlanan *'Binding Corporate Rules'un yarattığı yeterli korumanın bulunmasına (ing. adequate safeguard) dair fikir birliğine varılması süreci'* konulu bildiri çalışması;
- 2004 yılında WP 102 içerisinde yayınlanan *'Binding Corporate Rules'un onaylanması için başvuru'* konulu matbu kontrol listesi;
- 2003 yılında WP 74 içerisinde yayınlanan *'Kişisel verilerin üçüncü ülkelere aktarımı: Direktif md. 26/2'yi uluslararası veri aktarımında kullanılacak Binding Corporate Rules düzenlemek için uygulamak'* konulu bildiri çalışması.

Yukarıdaki listenin bir kısmı günümüzde mülga hale gelip geçerliliğini yitirse de tarihçe açısından hâlâ bir önem taşımaktadır. Yukarıda belirtildiği şekilde, WP kararlarının bir kısmı, Birlik Kurulu tarafından hâlâ desteklenmektedir.[182] Aşağıda listesi verilen güncel nitelikli bu dokümanlara halen atıf yapılmaktadır;

- 2018 yılında WP 263 rev.01 içerisinde yayınlanan *'Tüzük altında veri sorumluları ve işleyenleri Binding Corporate Rules'u onayı için iş birliği süreci'* konulu bildiri çalışması;
- 2018 yılında WP 264 içerisinde yayınlanan *'veri sorumlusu Binding Corporate Rules'u onay başvuru formuna dair tavsiyeler'*;
- 2018 yılında WP 265 içerisinde yayınlanan *'veri işleyen Binding Corporate Rules'u onay başvuru formuna dair tavsiyeler'*;
- 2018 yılında WP 256 rev.01 içerisinde yayınlanan *'Binding Corporate Rules'da yer alacak ilke ve nitelikleri içerir tablo'* konulu bildiri çalışması.

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

- 2018 yılında WP 257 rev.01 içerisinde yayınlanan *'veri işleyen Binding Corporate Rules'unda yer alacak ilke ve nitelikleri içerir tablo'* konulu bildiri çalışması.

2.2.2. Onaylanan İlk Binding Corporate Rules: Daimler Chrysler AG

Birlik hukukunda onaylanan ilk *Binding Corporate Rules,* önde gelen Alman otomobil şirketlerinden biri olan Daimler Chrysler AG[183]'ye aittir. Bu dönemde henüz bütün üye devletler *Binding Corporate Rules'u* tanımadığı için, düzenlemenin yasal mahiyeti belirsiz kalmıştır.[184]

Bir önceki başlıktaki listeden anlaşılacağı üzere, *Binding Corporate Rules* konusunda Birlik hukukunda yapılan ilk çalışma WP 74 dokümanıdır. İlk eğilim, düzenlenen *Binding Corporate Rules'a* Direktif'in 26. maddesi içinde yasal dayanak bulmak yönünde olmuştur. Bunun üzerine Daimler Chrysler tarafından WP 74 dokümanını hakkında bir görüş yazılmış ve Md. 29 Çalışma Grubu'na iletilmiştir.[185] İletilen görüş içerisinde, *Binding Corporate Rules'a* dair henüz bağlayıcı olarak belirlenen bir karar verilmemesinin, çokuluslu şirketleri zor duruma soktuğu ve uyum süreçlerini tehlikeye attığı belirtilmiştir. Görüşün devamında Birlik'teki yetkili veri koruma mercilerinin, şirketlerce hazırlanan *Binding Corporate Rules'u* yalnızca WP 74 esaslarına uyulmadığı takdirde reddetme haklarının olması gerektiği belirtilmiştir. Görüşte aynı zamanda *Binding Corporate Rules'a* dair varılacak anlaşmanın, Birlik'teki tüm yetkili veri koruma mercileri için bağlayıcılığının önemi vurgulanmıştır.

Binding Corporate Rules'un Birlik hukukunda henüz yeni benimsenmeye başlandığı bu dönemde, Daimler Chrysler ve Birlik veri koruma otoriteleri temsilcileri arasında süreç açısından önemli bir toplantı yapılmıştır.[186] Bu toplantıda Birlik veri

[183] Daimler ve Chrysler şirketleri 2007 yılında ayrılmıştır ve şirketin adı Daimler AG olarak değiştirilmiştir. https://tr.wikipedia.org/wiki/Daimler_AG Erişim Tarihi: 20.03.2020.

[184] SCHRÖDER Christian, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, 1. Auflage, Nomos Verlag, Frankfurt, Almanya 2007, s. 214, 221.

[185] Birlik Komisyonu DaimlerChrysler BCR'a Dair Görüş https://ec.europa.eu/justice/article-29/press-material/public-consultation/bcr/2003_bcr/daimlerchrysler_en.pdf Erişim Tarihi: 20.03.2020.

[186] Berlin toplantısı adıyla anılan ve 27-28 Mayıs 2004 yılında yapılan bu oturuma, Avusturya, Almanya, Macaristan, Polonya, Birleşik Krallık, Hollanda ve Avrupa Birliği Komisyonu katılmıştır. Özel sektörden ise o dönemde BCR düzenlemelerinde en çok ilerlemiş şirketler olan GE, Philips ve Daimler Chrysler'in temsilcileri davet edilmiştir. BCR'a dair deneyimlerin ve ihtiyaçların değerlendirildiği bu toplantı, BCR tarihçesi açısından son derece önemlidir. Nitekim Md. 29 Çalışma Grubu'nun BCR hakkındaki tavsiyelerini içerir bildirileri toplantıyı takiben yayınlanmıştır.

koruma otoriteleri, koyulan kurallara uygun düzenlenecek *Binding Corporate Rules'u* karşılıklı şekilde tanıma kararı almıştır.[187] Böylece *Binding Corporate Rules,* günümüzde Tüzük'teki düzenlemesine yaklaşılmaya başlamıştır.

2.3. TÜZÜK İÇERİSİNDE BINDING CORPORATE RULES

GVKT md. 4/20'de yer alan tanıma göre *Binding Corporate Rules*, üye devletlerin yargı alanında kurulu veri işleyen veya sorumlularınca, üçüncü ülkelerde yer alan grup şirket yahut ekonomik iş birliği halindeki teşebbüslerine yapılacak kişisel veri aktarımları için hazırlanan ve tarafların uymayı taahhüt ettikleri kişisel veri koruma politikalarıdır. Paralel biçimde GVKT 110. gerekçe maddesi, bir grup şirketin yahut ekonomik iş birliği halindeki teşebbüslerin, Birlik'ten aynı yapı içerisinde yer alan diğer şirketlere yaptıkları uluslararası veri aktarımlarında onaylanmış bir *Binding Corporate Rules*'dan yararlanabileceklerini öngörmektedir. Maddenin devamında, söz konusu *Binding Corporate Rules'un* kişisel veri işleme ilkelerini ve ilgili kişilerin haklarını muhakkak taahhüt etmesi gerektiği de vurgulanmaktadır.

Tüzük'te *Binding Corporate Rules'un* grup şirket yahut ekonomik iş birliği halindeki teşebbüs yapısı içerisinde, veri işleyen ve/veya veri sorumlusu için düzenlenebileceği öngörülmüştür. Veri sorumlusu *Binding Corporate Rules'u* veri aktarımları dahil veri sorumlusu sıfatıyla yapılan (ör. insan kaynakları) tüm veri işleme faaliyetlerini düzenlemektedir. Veri işleyen *Binding Corporate Rules'u* ise, müşteriler adına hareket edilirken (ör. *outsource*) kullanılmaktadır. Md. 29 Çalışma Grubu tarafından yayınlanan ilk *Binding Corporate Rules* taslağı*,* veri sorumluları için düzenlenmiştir. *Binding Corporate Rules* hesap verilebilirlik açısından temel taş sayılmakta ve oluşturulduğundan beri Md. 29 Çalışma Grubu tarafından teşvik edilmektedir.[188]

Binding Corporate Rules'un içeriğine dair genel düzenleme GVKT md. 47'de yer almaktadır. Onay süreci ise GVKT md. 57, md. 63 ve md. 64'de düzenlenmektedir. Çalışmamızın bu başlığı altında Tüzük'te *Binding Corporate Rules'un* içeriği için

[187] MOEREL Lokke, Binding Corporate Rules: Fixing Regulatory Patchwork of Data Protection [n.n.] 2011, s. 23.
[188] BOWMAN, GUFFLET, age, 257-261.

öngörülen asgari hususlar, kişi ve konu bakımından uygulaması, hukuki bağlayıcılığı ve onay süreci incelenecektir.

2.3.1 Binding Corporate Rules İçerisinde Verilecek Taahhütler

Binding Corporate Rules'un henüz geliştirildiği dönemden itibaren şeffaflık ilkesine verilen önem vurgulanmaktadır. Nitekim Tüzük içerisinde *Binding Corporate Rules'da* bulunması gereken asgari unsurları içeren madde, şeffaflığı sağlamak adına 14 fıkra halinde yazılmıştır. Maddenin detaylı şekilde düzenlenmesi, uyumluluk sürecinin Birlik içerisinde tutarlılığını ve kolay yönetilmesini sağlamaktadır. Zira *Binding Corporate Rules'un* onay süreçleri düzenleyen şirketin bulunduğu üye devlete göre, farklı veri koruma otoritelerince yürütülmektedir.

Binding Corporate Rules aşağıda incelenecek on dört fıkranın yanında, grup şirketin Tüzük'ten doğan tüm yükümlülüklerini düzenlemek durumundadır.[189] Örnek olarak GVKT md. 47/2d'de öngörülen veri işleme ilkeleri, GVKT md. 5'deki genel düzenlemeden şaşmamalıdır. Bir başka örnek de md. 28 uyarınca grup şirket adına üçüncü ülkede tayin edilebilecek veri işleyenlerdir. *Binding Corporate Rules'un* içinde bu veri işleyenler öngörüldüyse, md. 28 yükümlülükleri de yerine getirilmeli; sözleşme üzerine veri işleme için gerekli kontratlar imzalanmalıdır.[190]

Tüzüğün genel yükümlülükler haricinde *Binding Corporate Rules'da* özellikle bulunmasını aradığı asgari unsurlar aşağıdaki gibidir.

2.3.1.1. Binding Corporate Rules'u Düzenleyen Şirketin Yapısı ve İletişim Bilgileri (GVKT md. 47/2/a)

Bu fıkra Tüzüğün büyük hassasiyet gösterdiği veri sahiplerine karşı şeffaflığı sağlamak adına düzenlenmiştir. Fıkra aynı zamanda Tüzüğün şirketler için düzenlediği yükümlülüklerin daha kolay bir şekilde uygulanabilmesini sağlamaktadır. Bu fıkra sayesinde örneğin şirket hakkında tazminatın gündeme gelmesi halinde, sorumlular daha kolay ayrılabilmekte ve belirlenebilmektedir. Bu nedenle *Binding Corporate Rules* düzenleyen grup şirket veya ekonomik iş birliği içerisindeki teşebbüsün yapısı

[189] WP 256.
[190] WP 257.

gösterilmeli, şirketlerin nasıl gruplandığı saptanmalıdır. Bunun yanında tüm üyelerin iletişim bilgileri ve üçüncü ülkelerdeki üyelerden sorumlu Birlik şirketleri belirtilmelidir.

2.3.1.2. Veri Aktarımları ve İşlenen Veriler (GVKT md. 47/2/b)

Direktif döneminde üçüncü ülkelere veri aktarımı, verilerin aktarıldığı Birlik ülkesindeki yetkili veri koruma otoritesinin onayına tâbiydi. Bu onay sürecinde verilerin aktarıldığı ülkeye dair gereken tüm bilgilerin alındığı varsayılmaktaydı. Dolayısıyla Direktif döneminde *Binding Corporate Rules* içerisinde verilerin aktarılacağı üçüncü ülkelere ilişkin detaylı bilgi aranmamaktaydı.[191] Tüzük döneminde düzenlenecek *Binding Corporate Rules* ile üçüncü ülkelere veri aktarımı için ayrı bir onay süreci gerekmemektedir. Bu nedenle veri aktarımına ve işlemesine dair sürecin *Binding Corporate Rules* içerisinde detaylı olarak yazılması öngörülmüştür.[192]

Buna göre verilerin işlenme yöntem ve şekilleri, toplanan verilerin kategorileri, veri işleme süreci şekli, amacı ve kapsamı, veri sahiplerinin kategorisi ve üçüncü ülkelerde verilerin aktarıldığı kişiler gibi bilgilerin belirtilmesi gerekmektedir.

2.3.1.3. İç ve Dış Bağlayıcılık (GVKT md. 47/2/c)

Tüzüğün lafzı, iç ve dış bağlayıcılık kavramını açıklamamaktadır. İç ve dış bağlayıcılığın kriterleri için Birlik Kurulu'nun görüşlerinden yararlanılmaktadır. Buna göre iç bağlayıcılık, *Binding Corporate Rules* düzenleyen grup şirket veya ekonomik iş birliği içerisindeki teşebbüslerin tüm üyelerine ve bunların çalışanlarına verilecek açık emir ve talimatlarla sağlanmaktadır. Bu zincir düzeninin nasıl kurulacağı konusunda ise şirket özgür bırakılmıştır.[193] İç bağlayıcılık için kurulan yapı *Binding Corporate Rules* içerisinde belirtilmelidir.

Dış bağlayıcılığın sağlanması için ise, tüm üçüncü kişilerin haklarının ve bu hakların nasıl kullanılacağının açık ve anlaşılır biçimde yazılması gerekmektedir.[194] Bu anlamda verisi işlenen ilgili kişiler de üçüncü kişi sayılmaktadır. Dış bağlayıcılığın getirdiği önemli yükümlülüklerden biri olarak, Birlik'te yerleşik bir üyenin, üçüncü ülkelerde meydana gelebilecek hukuka aykırılıklarda hukuki sorumluluğu üstlenmesi

[191] WP 204.rev01.
[192] WP 256.
[193] WP 256, WP 257.
[194] WP 152, WP 74, WP 108.

gerekmektedir. Üçüncü ülkelerin sorumluluğunu üstlenen bu üye şirket *Binding Corporate Rules* içerisinde belirtilmelidir.[195] Bu şekilde üçüncü kişilerin, yazılan haklarını pratik biçimde kullanabilmeleri sağlanmaktadır.

2.3.1.4. Veri İşleme İlkeleri (GVKT md. 47/2/d)

GVKT md. 47/2/d maddesinde, *Binding Corporate Rules* içerisinde taahhüt edilecek veri işleme ilkelerine dair tüketici olmayan bir liste öngörülmüştür. Çalışmamızın 1.1. başlığında ayrıntısıyla incelenen bu veri işleme ilkelerinin taahhüt edilmesi, başlı başına yeterli görülmemektedir. İlkelerin *Binding Corporate Rules* içerisinde, grup şirket veya ekonomik iş birliği içerisindeki teşebbüs yapısında nasıl kullanıldığı somut şekilde yazılmalı ve örneklendirilmelidir.[196]

2.3.1.5. İlgili Kişinin Hakları (GVKT md. 47/2/e)

Tüzüğün ilgili kişilere tanıdığı bütün haklar *Binding Corporate Rules* içerisinde de kapsamlı olarak taahhüt edilmelidir. Bu anlamda aşağıda sayılanlar dahil ancak bunlarla sınırlı olmayacak şekilde; veri işleme ilkeleri, md. 15'de düzenlendiği üzere ilgili kişinin hakları, md. 16 uyarınca verilerin düzeltilmesi ve değiştirilmesi hakkı, md. 17 uyarınca silinme *'unutulma'* hakkı, md. 18'de yer aldığı şekliyle veri işlenmesini kısıtlama hakkı, md. 21 itiraz ve md. 22 uyarınca verilerin profilleme *(ing. profiling)* dahil otomatik karar alma *(ing. automated decision making)* sürecine dahil edilmesine itiraz hakkı ve md. 82 uyarınca tazminat hakları taahhüt edilmelidir. Ayrıca eğer ilgili kişinin tâbi olduğu ulusal veri koruma kanunları, Tüzük'ten üstün bir koruma sağlıyorsa, bu haklar da *Binding Corporate Rules'a* dahil edilmelidir.

Binding Corporate Rules'da taahhüt edilen hakların kullanılabilmesi için yöntemler de gösterilmelidir. Öyle ki yetkili veri koruma otoriteleri nezdinde şikâyet yahut üye devletlerin yetkili ve görevli mahkemeleri önünde dava usulleri açıklanmalıdır. Buna göre tercih ilgili kişide olacak şekilde, verileri üçüncü ülkelere aktaran Birlik ülkesindeki mahkemeler ile grup şirket merkezinin yerleşik olduğu Birlik ülkesindeki

[195] *Zerdick'e ait kısım,* EHMANN, SELMAYR, age, s. 696.
[196] *Paal'e ait kısım,* PAAL, PAULY, age, s. 584.

mahkemeler yetkilidir.[197] Ek olarak GVKT md. 79/2 uyarınca ilgili kişinin ikamet yerindeki bir mahkemede de dava açılabilmektedir.

2.3.1.6. Birlik'teki Kuruluşların Sorumluluğu (GVKT md. 47/2/f)

Bilindiği üzere *Binding Corporate Rules'da* verilerin aktarıldığı üçüncü ülkedeki potansiyel hukuka aykırılıklar için Birlik'teki sorumlu üye şirket açıkça belirtilmelidir. Bu yükümlülük şeffaflığın sağlanmasına da hizmet etmektedir. *Binding Corporate Rules*'da grup şirketin üçüncü ülkelerde kurulu üyeleri için müşterek sorumluluk öngörülmelidir. Bu husus kanuni bir yükümlülük olmadığından, bağlayıcı olması için *Binding Corporate Rules* içerisine mutlaka yazılmalıdır. Birlik'teki müşterek sorumlu üye şirket, hukuka aykırılığın izinin kendisine hiçbir şekilde sürülemediğini ispat ederse sorumluluktan kurtulabilmektedir.[198]

Kullanılan bu ifadeyi bir kurtuluş beyyinesi olarak ele almak mümkündür.[199] Nitekim *Binding Corporate Rules'da* işbu başlık altında açıklandığı üzere, üçüncü ülkedeki üye şirketler için öngörülmüş yükümlülükler, gösterilecek özene işaret etmektedir. Üçüncü ülkedeki üye şirketin tâbi olduğu iç hukuk araştırması yapılmalı ve *Binding Corporate Rules* yükümlülüklerine aykırı hususlar belirlenmelidir. Gerekli hallerde Birlik'teki yetkili veri koruma otoritesine danışılmalıdır. *Binding Coprorate Rules* altında öngörülen teknik ve idari tedbirler, üçüncü ülkedeki üye şirket için de bağlayıcı şekilde uygulanmalıdır. Gerekli denetimler ve raporlamalar yapılmalıdır. Dolayısıyla Birlik'teki müşterek sorumlu şirketin gerekli özeni gösterdiğini ispat etmesi halinde kendisine kurtuluş imkânı tanınması, *Binding Corporate Rules'un* mantığı ve amaçlarıyla uyumludur. Bu noktada ispat yükü Birlik'teki üye şirket üstündedir.[200] Çalışmamızın devamında inceleneceği üzere *Binding Corporate Rules* taahhütlerine uyulmaması özen borcuna da aykırılığı göstermektedir.[201]

Üçüncü ülkedeki üye şirketin olası hukuka aykırılıkları için, Birlik'teki hangi üye şirketin müşterek sorumlu kılınacağı GVKT md. 47'de düzenlenmemiştir. Grup şirketler, *Binding Corporate Rules* düzenlerken kendi yapıları uyarınca, Birlik'teki herhangi bir

---

[197] WP 256.
[198] WP 257.
[199] Kurtuluş beyyinesi hakkında bkz. OĞUZMAN M. Kemal, ÖZ M. Turgut, Borçlar Hukuku Genel Hükümler Cilt – II, 10. Bası, Vedat Kitapçılık, İstanbul, Türkiye 2013, s. 148 vd.
[200] WP 257.
[201] Bkz. dn. 233.

üye şirketi müşterek sorumlu kılabilmektedirler. Bu tercih genel olarak, üçüncü ülkelere verilerin aktarıldığı şirket veya Birlik'teki ana merkezden yana kullanılmaktadır.

2.3.1.7. Bilgilerin İlgili Kişilere İletilmesi (GVKT md. 47/2/g)

GVKT'nin md. 13. ve md. 14'de ilgili kişilere iletilmesi gereken bilgiler düzenlenmiştir. *Binding Corporate Rules* içerisine bu bilgilerin hangi yöntemle verileceği de yazılmalıdır. Söz konusu yükümlülük, internet veya intranet üstünden yapılacak bilgilendirmeyle yerine getirilebilmektedir. Bu anlamda unutmamak gerekir ki, ilgili kişilerin tüm haklarını kolayca kullanabilmeleri için gereken bütün bilgiler açık ve anlaşılır şekilde iletilmelidir.[202]

2.3.1.8. Çalışanların Görevleri ve Compliance (GVKT md. 47/2/h)

Binding Corporate Rules uyarınca grup şirkette bir veri koruma görevlisi *(ing. Data Protection Officer)* atanmalıdır. Bunun yanında *compliance* (uyumluluk) sağlanması için şirket içerisinde ayrı bir bölümün yapılandırılması gereklidir. Grup şirket içerisindeki bütün çalışanlar *compliance* sürecinden haberdar edilmelidir. Öyle ki kurulacak bölümün yapısı, ödevleri ve yetkileri *Binding Corporate Rules* içerisinde düzenlenmelidir.[203] Bunun yanında grup şirket üyesi her bir kuruluşun ödevleri belirlenmeli ve bir kontrol (emir komuta) zincirine bağlanmalıdır.[204] Dolayısıyla *compliance* için her bölümün raporlama yapacağı üst bölüm belli olmalı ve bu üst bölümden gelecek talimatlara uyulmalıdır.

2.3.1.9. İtiraz ve Şikâyet Süreci (GVKT md. 47/2/i)

Bu fıkra uyarınca *Binding Corporate Rules'da* iç şikâyet süreçleri öngörülmelidir. İlgili kişiler şikayetlerini grup şirket içerisinde hangi bölüme ne yolla ileteceklerini bilmelidirler. Örneğin ilgili kişilerin şikâyet ve itiraz haklarını kendilerine iletilen formlar aracılığıyla kullanmaları düzenlenebilir. Formda şikâyetin araştırılabilmesi için istenen gerekli bilgileri de doldurmaları öngörülebilir. Yahut şikayetlerin bildirilmesi için şirketin web sitesi üzerinden bir özel bir pencere açılabilir. *Binding Corporate Rules'da*

[202] *Schröder'e ait kısım,* KÜHLING, BUCHNER, age, s. 876.
[203] WP 257.
[204] WP 256, WP 257, WP 74.

bu süreç açıkça belirtilmeli ve iç şikayet için kurulan yöntem açıklanmalıdır. Grup şirket nezdinde yapılan iç şikâyet, bir ila en fazla üç ay içerisinde araştırılarak tatmin edici biçimde cevaplanmalıdır.[205]

2.3.1.10. Compliance Devamı İçin Kontrol Süreçleri (GVKT md. 47/2/j)

Binding Corporate Rules'un amacı veri koruması ve mahremiyeti şirket kültürüne dahil etmektir. Bu anlamda daimî bir *compliance* yaratılması hedeflenmektedir. Dolayısıyla *Binding Corporate Rules* onaylandıktan sonra da *compliance* sürdürülmeli ve kontrol edilmelidir.[206] Şirkette kurulan *compliance* bölümü periyodik aralıklarla testler yürütmelidir. Veri koruma yükümlülüklerine ve *Binding Corporate Rules'a* uyumun denetlendiği bu testler, veri koruma görevlisi ve grup şirketin yönetim kurulu ile paylaşılmalıdır. Yapılan denetimlerin sonucu, talep üzerine yetkili veri koruma otoritelerine de iletilmelidir.

Söz konusu test ve denetimler, iç veya dış servis sağlayıcılar (ör. akredite denetim kuruluşları) aracılığıyla yürütülebilmektedir.[207] *Binding Corporate Rules* içerisinde grup şirket üyelerinin bu testleri hangi aralıklarla yürüteceği ve sonuçlarını kimlerle paylaşacağı belirtilmelidir. Yapılacak bu denetimlerin, herhangi bir hukuka aykırılık iddiasında ispat aracı olabileceklerinin altını çizmek gerekir.

2.3.1.11. Binding Corporate Rules'un Güncellenmesi ve Yetkili Veri Koruma Otoritesine Bildirilmesi (GVKT md. 47/2/k)

Grup şirket yapısı ve veri işleme süreçleri sürekli değişmektedir. Bu nedenle düzenlenen *Binding Corporate Rules'u* statik bir kurallar bütünü olarak düşünmek yanlıştır. Bu noktada meydana gelen değişikliğin boyutu değerlendirilmelidir. Elbette her yeni değişiklikte yeni bir *Binding Corporate Rules* düzenlenip onaylanması gerekmeyecektedir. Değişiklik ancak yürürlükteki *Binding Corporate Rules'u* temelden etkiliyorsa, *Binding Corporate Rules'un* baştan düzenlenip onaylanması gündeme gelecektir. Belirtmek gerekir ki yapılan değişikliğin *Binding Corporate Rules'u* temelden

[205] WP 256, WP 257, WP 74, WP 108, WP 204.rev01.
[206] WP 256, WP 257.
[207] Söz konusu denetimlerin niteliğine ve içeriğine dair ayrıntılı bilgi için bkz. WP 256, WP 257.

etkileyip etkilemediğine dair şüphe varsa, yetkili veri koruma otoritesine danışılmalı ve yeni bir onay sürecinin gerekliliğine dair görüş alınmalıdır.[208]

Md. 29 Çalışma Grubu veri işleme süreçlerindeki değişikliklere dair aşağıdaki esas hususları benimsenmiştir[209];

- Grup şirket içerisinde, veri işleme süreçlerindeki değişiklikler takip edilerek değerlendirilmeli ve *Binding Corporate Rules'da* değişikliğe gidilip gidilmemesi gerektiğini belirlenmelidir. Bu amaçla yetkili veri koruma otoriteleri ile koordinasyonu sağlayacak bir kişi/pozisyon yaratılmalıdır;
- Grup şirket yapısı içerisine yeni bir kuruluşun katılması halinde, kuruluş yürürlükteki *Binding Corporate Rules'u* taahhüt etmeli ve *compliance* sağlanmalıdır;
- Yıllık olarak yapılan değişiklikler, yetkili veri koruma otoritesi ile paylaşılmalı, eğer değişikliklerden biri temel nitelikli olarak değerlendirilirse izlenilecek yol yetkili veri koruma otoritesi ile birlikte kararlaştırılmalıdır;
- *Binding Corporate Rules'da* yapılan her değişiklik, grup şirket ile sözleşmeli veri işleyenlerle paylaşılmalı ve *compliance* sağlanmalıdır.

2.3.1.12. Yetkili Veri Koruma Otoritesi ile İş Birliği (GVKT md. 47/2/l)

Binding Corporate Rules düzenleyen grup şirket, yetkili veri koruma otoritesi ile birlikte çalışmakla yükümlüdür. Bu ortak çalışma süreci *Binding Corporate Rules'da* tasvir edilmelidir. Yükümlülüğün yerine getirilmesi için GVKT md. 47/2/f uyarınca yapılan *compliance* denetimlerinin sonuçları, GVKT md. 47/2/k uyarınca yapılacak güncellemeler yahut GVKT md. 47/2/m uyarınca verilen yerel taahhütler, yetkili veri koruma otoriteleriyle paylaşılmalıdır.

2.3.1.13. Üçüncü Ülkelerdeki Binding Corporate Rules'a Aykırı Kanuni Yükümlülüklere Dair Bildirim (GVKT md. 47/2/m)

Grup şirketin üçüncü ülkedeki üyeleri *Binding Corporate Rules'da* verilen taahhütleri değerlendirmeli ve tâbi oldukları yerel mevzuatla karşılaştırmalıdır. Üçüncü

[208] *Schröder'e ait kısım,* KÜHLING, BUCHNER, age, s. 879.
[209] WP 256, WP 257, WP 204.rev01.

ülkedeki veri koruma kanunlarına dair yapılan bu araştırma, grup şirketin *compliance* birimi ve veri koruma görevlisiyle paylaşılmalıdır. Yerel mevzuatla çatıştığı için uygulanamayacak *Binding Corporate Rules* yükümlülükleri varsa, bu husus Birlik'teki müşterek sorumlu üyeye veya genel merkezin *compliance* bölümüne bildirilmelidir. *Binding Corporate* Rules ile çatışan yerel mevzuat hükümleri yetkili veri koruma otoritesi ile de paylaşılmalıdır.

Yerel mevzuat hükümleri ile *Binding Corporate Rules'un* çatıştığı noktada, GVKT md. 23 uyarınca bir değerlendirme yapılmaktadır. Belirtmek gerekir ki, çalışmamızda ayrıntısıyla incelenen *Safe Harbor* kararı[210] bu değerlendirme için önem taşımaktadır. Söz konusu kararda, Birlik hukuku ile üçüncü ülkelerin mevzuatının çatıştığı hallerde benimsenecek prensipler ayrıntısıyla belirlenmiştir. Bu ilkeler *Binding Corporate Rules* ile üçüncü ülke kanunlarının çatıştığı noktada da uygulanabilir niteliktedir.

2.3.1.14. Çalışanlara Verilecek Eğitimler (GVKT md. 47/2/n)

Binding Corporate Rules'u düzenleyen grup şirket bünyesindeki bütün kuruluşlar, çalışanlarına periyodik aralıklarla eğitimler vermekle yükümlüdürler. Verilecek eğitimlerin niteliği[211] *Binding Corporate Rules'da* belirtilmelidir. Öyle ki eğitim programlarının örneklenmesi dahi öngörülmüştür.[212]

2.3.2. Binding Corporate Rules'un Konu Bakımından Uygulaması

Binding Corporate Rules niteliği itibariyle üçüncü ülkelere veri aktarımı için uygun güvenlik önlemlerini sıralayan 46. madde kapsamında değerlendirilmelidir. Bu madde Birlik'ten ve Avrupa Ekonomik Alanı'ndan üçüncü ülkelere aktarılan kişisel verileri düzenlemektedir.[213] Bu nedenle *Binding Corporate Rules* da temelde Birlik ve Avrupa Ekonomik Alanı'ndan üçüncü ülkelere aktarılan kişisel verilere uygulanmaktadır. Dolayısıyla şirketler düzenledikleri *Binding Corporate* Rules'un

[210] AAD C-362/14
[211] Bu konuda detaylı bilgi için bkz. WP WP 257, WP 257, WP 75, WP 108.
[212] WP 256, WP 153.
[213] ASTB üyesi ülkelerden üçü (İzlanda, Lihtenştayn ve Norveç) AEA antlaşması (Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI to the EEA Agreement, OJ L 296/41, of 23 November 2000) kapsamında 95/46 sayılı Direktif'i iç hukuklarında uygulamışlardır.

konusu kişisel verileri, yalnızca Birlik ve Avrupa Ekonomik Alanı'ndan aktarılan kişisel verilerle sınırlayabilmektedirler.[214]

Binding Corporate Rules yalnızca belirli bir kişisel veri grubuyla (ör. müşteri verileri) da sınırlanabilmektedir. Bu durumda diğer veri grupları için başka koruma/uygun güvenlik önlemleri (ör. standart veri koruma maddeleri) öngörülmelidir. Zira *Binding Corporate Rules* üçüncü ülkelere veri aktarımında kullanılacak uygun bir güvenlik önleminden çok daha fazlasıdır. Görüldüğü üzere geniş taahhütler içermekte ve uzun uyum projeleri gerektirmektedir. Öyle ki kişisel verilere karşı bütün tutum ve yaklaşım politikasını belirlemektedir.[215] Bu nedenle konu bakımından sınırlanması tercih edilebilmektedir.

2.3.3. Binding Corporate Rules'un Kişi Bakımından Uygulaması

Tüzüğün tanımları içeren 4. maddesi uyarınca grup şirketler yahut ekonomik iş birliği içindeki teşebbüsler *Binding Corporate Rules* düzenleyebilmektedir. GVKT md. 4/20'deki *Binding Corporate Rules* tanımında veri sorumlusu ve veri işleyen ayrımları yapılmamıştır. Nitekim her ikisi için de *Binding Corporate Rules* düzenlemek mümkündür ve bu husus şirketin kararına bırakılmıştır.[216]

Tüzüğün *Binding Corporate Rules* düzenleyebilecek yapılara ilişkin getirdiği sınırlamada 'grup şirketler' ile kast edilen oldukça açıktır. Ancak hangi yapıların 'ortak ekonomik faaliyet/iş birliği içerisindeki teşebbüsler' olarak değerlendirileceği incelenmelidir. Tüzüğün lafzından anlaşıldığı şekilde, *Binding Corporate Rules* düzenleyebilmek için hukuki anlamda bir grup şirket yapısı gerekmemektedir. Öyle ki, çıkar ve kâr adına ortak ekonomik faaliyet gösteren (ör. *joint venture, şubeler, bağlı kuruluşlar*) her tür yapı *Binding Corporate Rules* düzenleyebilmektedir.[217]

Buna ek olarak, kullanılan teşebbüs kavramı da yapının hukuki kişiliğine dair bir zorunluluk olmadığına işaret etmektedir.[218] Şöyle ki teşebbüs kavramının tercih edilmesi

[214] *Schröder'e ait kısım,* KÜHLING, BUCHNER, age, s. 869.
[215] FILIP Alexander (2013), 'BCR aus der Sicht einer Datenschutzaufsichtsbehörde – Praxiserfahrungen mit der europaweiten Anerkennung von BCR', ZD, C. 2, s. 51-60.
[216] *Wieczorek'e ait kısım,* SPECHT, MANTZ, age, s. 177.
[217] Age.
[218] *Zerdick'e ait kısım,* EHMANN, SELMAYR, age, s. 695.

aynı zamanda, Küçük Orta Büyüklükte İşletmelerin hedef alındığına dair bir gösterge olarak da yorumlanabilir.[219]

2.3.4. Onay Süreci

Binding Corporate Rules farklı ülkelerdeki farklı yerel hukuk düzenlemelerine tâbi şirketler için bağlayıcı olarak düzenlenmektedir. Bu nedenle yetkili veri koruma otoritelerinin iş birliğini ve karşılıklı taahhütlerini gerektirmektedir.[220] Nitekim GVKT md. 47'ye uygun olarak hazırlanmış bir *Binding Corporate Rules,* md. 63'de düzenlenen Birliğin tamamı için öngörülmüş tutarlılık mekanizmalarına da tâbidir.

Grup şirket merkezinin bulunduğu Birlik ülkesindeki yetkili veri koruma otoritesi, *Binding Corporate Rules* düzenlenirken bu tutarlılık mekanizmalarını izlemektedir. Öyle ki bu yetkili veri koruma otoritesi, md. 56 uyarınca *Binding Corporate Rules'u* baş yetkili otorite *(ing. lead supervisory authority)* olarak onaylamaktadır.[221] Ancak grup şirketin Birlik ülkelerinde kurulu diğer kuruluşlarının bulunduğu yerdeki yetkili veri koruma otoriteleri de onay sürecine katılmaktadırlar.[222]

Belirtmek gerekir ki, grup şirketin Birlik'te yalnızca bir adet kuruluşu olması halinde bu tutarlılık sürecine gerek kalmamaktadır.[223] Nitekim GVKT md. 57/1 ve md. 58/3/j'de düzenlendiği üzere her yetkili veri koruma otoritesinin kendi yargı alanında düzenlenen *Binding Corporate Rules'u* onaylama yetkisi bulunmaktadır.

2.4 BİRLİK'TEKİ ANA ŞİRKETİN SORUMLULUĞU

Tüzüğün sekizinci bölümü hukuki çareler, sorumluluk ve cezaları düzenlemektedir. Söz konusu bölüm altında 82. maddede maddi/manevi tazminat ve 84. maddede cezai sorumluluk halleri düzenlenmektedir. Bu maddeler önem teşkil etse de

[219] Bkz. Komisyon'un 6 Mayıs 2003 tarihli 2003/361/EC sayılı 'mikro küçük ve orta büyüklükte işletme tanımı'.
[220] Bu konuda tüzük öncesi dönemden beri gelişim için bkz. WP107 sayılı 'BCR için bir ortak çalışma oluşturulması' konulu bildiri çalışması.
[221] Tutarlılık mekanizmalarına dair ayrıntılı bilgi için bkz. KÜHLING Jürgen, MARTINI Mario (2016), DSGVO: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht*?,* EuZW, C.6, s. 448.
[222] *Schröder'e ait kısım,* KÜHLING, BUCHNER, age, s. 871.
[223] *Paal'e ait kısım,* PAAL, PAULY, age, s. 576.

üye devletlerin iç hukuku uyarınca şekillendirilip uygulanması beklenmektedir.[224] Dolayısıyla çalışmamızın bu başlığı altında, Birlik içerisinde yeknesak uygulanan idari para cezaları incelenecektir. Nitekim idari para cezaları düzenlenirken amaçlananlardan biri, Facebook ve Google gibi büyük veri aktörlerinin faaliyetleri için Birlik içerisinde tutarlı bir uygulama benimsenmesidir.[225]

Tüzük önemli bir yenilik olarak 83. maddede yüksek idari para cezaları öngörmüştür. Veri sorumlusu ve veri işleyenin GVKT md. 8, md. 11, md. 25-39, md. 42 ve md. 43'de düzenlenen yükümlülüklere aykırı davranmaları halinde, yetkili veri koruma otoritesince tayin edilmek üzere 10 000 000 EUR'ya kadar, şayet bir ticari teşebbüs söz konusu ise global cironun 2 %'sine kadar idari para cezası düzenlenmiştir.

Veri işleme ilkelerinin, hukuka uygunluk hallerinin, ilgili kişiden alınacak rızaya dair öngörülen yükümlülüklerin ve özel nitelikli kişisel verilere dair düzenlemelerin yer aldığı GVKT md. 5, md. 6, md. 7 ve md. 9'un ve ilgili kişilerin haklarının düzenlendiği GVKT md. 12 ila 22'nin ihlalinde ise, yine yetkili veri koruma otoritesince tayin edilmek üzere 20 000 000 EUR'ya kadar, şayet bir ticari teşebbüs söz konusu ise global cironun 4 %'üne kadar idari para cezası öngörülmüştür. Burada belirtilmelidir ki veri sorumlusu, rızanın Tüzüğe uygun şekilde alındığını ispatla yükümlüdür.[226]

GVKT md. 44 ila md. 49'da öngörüldüğü şekilde *Binding Corporate Rules* dahil ancak bununla sınırlı olmayacak şekilde, üçüncü ülkelere veri aktarımı için öngörülen yükümlülüklere aykırılık da 20 000 000 EUR'ya kadar, bir ticari teşebbüs söz konusu olduğunda ise global cironun 4 %'üne kadar idari para cezasını gerektirmektedir.

Görüldüğü üzere, *Binding Corporate Rules'u* taahhüt eden Türkiye'deki üye şirketin, onaylanan bu şirket kurallarına riayet etmesi gerekmektedir. Özellikle veri işleme ilkelerine[227], hukuka uygunluk sebeplerine[228] ve ilgili kişilerden alınacak rızalara[229] Tüzüğün öngördüğü ve *Binding Corporate Rules'da* yazıldığı şekilde

---

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

[225] Her ne kadar Tüzük'teki idari para cezalarında makas oldukça geniş tutulmuşsa da global ciro üzerinden tayin edilmesi ekonomik olarak hakkaniyetlidir. Böylece Birlik'te tutarlı bir uygulama benimsenmeye çalışılmıştır. Age, s. 723.

[226] KÜHLING Jürgen, KLAR Manuel, SACKMANN Florian, Datenschutzrecht, 4. Auflage, C.F. Müller, Heidelberg, Almanya 2018, s. 208.

[227] Ayrıntılı bilgi için çalışmamızın 1.1. başlığına bakınız.

[228] Ayrıntılı bilgi için bkz. *Kamp'a ait kısım*, von dem BUSSCHE Axel, VOIGT Paul, Konzerndatenschutz: Rechtshandbuch, 2. Auflage, C.H. Beck, München, Almanya 2019, s. 349.

[229] Ayrıntılı bilgi için çalışmamızın 3.1.2. başlığına bakınız.

uymalıdır. Türkiye'deki şirket aynı zamanda *Binding Corporate Rules* dahilinde kendisine aktarılan verileri, üçüncü bir kişiye aktarırken Tüzük'te düzenlenen veri aktarımı yükümlülüklerini de[230] yerine getirmelidir. Bu yükümlülüklere uyulmaması halinde Birlik'teki merkez yapı hakkında, *Binding Corporate Rules'u* taahhüt eden global grup şirketin son finansal yılı cirosunun 4 %'üne kadar idari para cezası uygulanabilmektedir.

Yukarıda Tüzük'te düzenlenen genel idari para cezaları incelenmiştir. Bunların yanında, özellikle üçüncü ülkedeki üye şirketin *Binding Corporate Rules'a* aykırı hareketleri neticesinde merkez şirketin sorumluluğuna gidilebileceği de unutulmamalıdır. *Binding Corporate Rules'un* dış bağlayıcılığı neticesinde[231] grup şirket merkezinin veya Birlik'te yerleşik bir üyenin, üçüncü ülkelerde meydana gelebilecek hukuka aykırılıklar için sorumluluğu üstlenmesi gerekmektedir.[232] *Binding Corporate Rules'u* Türkiye'de taahhüt eden üye şirkette meydana gelebilecek hukuka aykırılıklar için müşterek sorumlu bir şirket öngörülecektir. Dolayısıyla *Binding Corporate Rules* düzenleyen grup şirketin üçüncü ülkelerdeki üyelerinin de *compliance* sağlaması son derece önemlidir. Aksi halde müşterek sorumlu kılınan Birlik'teki şirketin bulunduğu yerdeki veri koruma otoritesi, GVKT md. 83 hükümlerince idari para cezası düzenleyebilecektir.

Yetkili veri koruma otoriteleri GVKT md. 83'de düzenlenen idari para cezalarının tutarını tayin ederken, aşağıda belirtilen hususları dikkate almaktadırlar. İlk olarak veri sorumlusu veya işleyen tarafından ilgili kişilerin zararını azaltmak için yapılanlar değerlendirilmektedir. Bunun yanında GVKT md. 25 ve 32. uyarınca öngörülen idari ve teknik tedbirler de dikkate alınmaktadır. Zararı azaltmak amacıyla yetkili veri koruma otoriteleri ile ne ölçüde iş birliği yapıldığı da dikkate alınmaktadır. Bir başka kriter olarak GVKT md. 58/2 uyarınca yetkili veri koruma otoritelerinin daha önceden yaptığı uyarılara uyulup uyulmadığı da incelenmektedir.

Yetkili veri koruma otoritesi tarafından onaylanmış bir *Binding Corporate Rules'un* varlığı bu değerlendirme açısından son derece önemlidir. Öyle ki *Binding Corporate Rules* teknik ve idari tedbirlerin alındığını göstermekte ve zarar riskini minimize etmektedir. Bunun yanında veri koruma otoriteleriyle iş birliğini de kuvvetlendirmekte ve grup şirketin güvenilirliğini arttırmaktadır. Dolayısıyla *Binding*

[230] Ayrıntılı bilgi için çalışmamızın 3.1.3. başlığına bakınız.
[231] Dış bağlayıcılık dahil tüm BCR yükümlülükleri için çalışmamızın 2.3.1. başlığına bakınız.
[232] *Zerdick'e ait kısım*, EHMANN, SELMAYR, age, s. 696.

Corporate Rules'un idari para cezaları açısından taşıdığı önem açıktır. Şirketi olası bir idari para cezasından kurtarabilecek olan *Binding Corporate Rules'a* uyulmaması ise, direkt olarak özen borcuna aykırılığı gösterecektir.[233]

2.5. BİRLİK DIŞINDAKİ ÖRNEK ÜLKELERDE BINDING CORPORATE RULES BENZERİ DÜZENLEMELER

Binding Corporate Rules benzeri taahhütler birçok hukuk sisteminde benimsenmiştir. Nitekim Türkiye'de de Bağlayıcı Şirket Kuralları adıyla benzer taahhütler düzenlenebilmektedir. Ancak Türkiye incelemesine geçmeden evvel, Birlik ile ilişkileri nedeniyle iki farklı ülkedeki düzenlemeler değerlendirilecektir. Kısa bir şekilde, Brexit ile Birlik'ten çıkan Birleşik Krallık'ta hâlihazırda onaylanmış *Binding Corporate Rules'un* akıbeti belirlenecektir. Diğer ülke incelemesi için Birlik içerisinde yer almamasına rağmen Avrupa Serbest Ticaret Birliği üyesi olan İsviçre örneği seçilmiştir.

Son olarak Asya-Pasifik Ekonomik İş Birliği *(ing. Asia-Pacific Economic Cooperation 'APEC')* içerisindeki Sınırötesi Mahremiyet Kuralları *(ing. Cross Border Privacy Rules 'CBPR')* değerlendirilecektir. Birden fazla üye devleti ilgilendiren bu kuralların uluslararası veri aktarımı açısından *Binding Corporate Rules'a* benzer bir etkileri olduğunu söylemek mümkündür.

2.5.1. Birleşik Krallık

Birleşik Krallık, 29 Mart 2017 tarihinde ABA md. 50 hakkını kullanarak Birlik'ten çıkma (Brexit) niyetini belirtmiştir. Birlik'ten çıkış ile Birlik hukukunun tüm birincil ve ikincil mevzuatı, Birleşik Krallık için bağlayıcılığını yitirecektir.[234] Dolayısıyla Tüzüğe göre üçüncü ülke konumuna düşecek Birleşik Krallığa yapılacak veri aktarımları büyük bir soru işareti teşkil etmektedir. Ek olarak Tüzüğün yürürlük tarihi itibariyle Birleşik Krallık'ta onaylanmış ve şirketlerce kullanılan otuzdan fazla *Binding Corporate Rules* mevcut olduğu görülmektedir. [235] Benzer şekilde bunca *Binding*

[233] *Golla'ya ait kısım,* AUERNHAMMER, age, s. 1216.
[234] Birlik Komisyonu'nun Brexit'e hazırlık Bildirisi, 1. Kısım. https://ec.europa.eu/info/brexit/brexit-preparedness/preparedness-notices_en Erişim Tarihi: 28.03.2020.
[235] 24 Mayıs 2018 tarihi itibariyle EU-BCR süreçleri tamamlanmış şirketler listesi https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841 Erişim Tarihi: 28.03.2020.

Corporate Rules'un Birlik açısından geçerliliği ve Brexit sonrası Birleşik Krallık'ta verilecek *Binding Corporate Rules* onayları da tartışılan hususlardır.

24 Kasım 2018 tarihinde taraflar, Birleşik Krallığın Birlik'ten çıkış şart ve koşullarını belirleyen bir Çıkış Antlaşması[236] *(ing. Withdrawal Agreement)* düzenleme kararı almışlardır. Söz konusu antlaşma Birleşik Krallık'ta toplanıp işlenen kişisel veriler açısından 31 Aralık 2020'ye kadar sürecek 21 aylık bir geçiş süreci öngörmektedir.[237] Dolayısıyla Birleşik Krallığın, Tüzük açısından üçüncü ülke konumuna indirilmesi de bu tarih sonrasına bırakılmıştır.

Birlik Kurulu'nun Çıkış Antlaşmasının henüz kesinleşmediği tarihlerde yayınlanan bir görüşünde *Binding Corporate Rules'un* akıbetine dair değerlendirme yapılmıştır.[238] Çıkış Antlaşmasının yürürlüğe girmemesi halinde, Birleşik Krallık yetkili veri koruma otoritesinin *Binding Corporate Rules* onay süreçlerinde hiçbir yetkisinin kalmayacağı belirtilmiştir. Öyle ki, her somut örnek için ayrı bir değerlendirme yapılarak Birlik'ten başka yetkili veri koruma mercilerinin baş yetkili otorite olarak atanması öngörülmüştür.[239] Çıkış Antlaşması yürürlüğe girdiğinden ötürü, geçiş süreci boyunca Birleşik Krallık yetkili veri koruma otoritesinin *Binding Corporate Rules* konusunda yetkili olduğunu söylemek mümkündür. Benzer şekilde şirketler de veri aktarımlarında uygun güvenlik önlemi olarak onaylanmış *Binding Corporate Rules'u* kullanabilecektir.

Tanınan geçiş sürecinin sona ermesiyle Birlik hukuku için Birleşik Krallık üçüncü ülke sayılacaktır. Dolayısıyla Birleşik Krallığa yapılacak veri aktarımlarında Tüzüğün öngördüğü yolların izlenmesi gerekecektir. Bu tarihten sonra, hâlihazırda onaylanmış *Binding Corporate Rules*'un Birlik açısından kazanılmış hak teşkil edip etmeyeceği ve iptal edilene kadar yürürlükte kalmasına karar verilip verilmeyeceği bilinmemektedir.[240] Geçiş sürecinin bitmesinden sonra hazırlanıp onaylanacak bir *Binding Corporate Rules'un* ise, Birlik hukuku açısından herhangi bir bağlayıcılığı olmayacaktır. Bu

[236] Söz konusu antlaşma, Birleşik Krallıkta 23.01.2020 tarihinde onaylanarak 30.01.2020 tarihi itibariyle yürürlüğe girmiştir.
[237] Çıkış Antlaşması md. 71.
[238] European Data Protection Board 'Information Note on BCRs for Companies which have ICO as BCR Supervisory Lead Authority (12.02.2019).
[239] *Kuner'e ait kısım,* KUNER, BYGRAVE, DOCKSEY, age, s. 822.
[240] Birlik Kurulu'nun hukuk güvenliğinin sağlanması adına Tüzüğün yürürlüğe girmesinden evvel onaylanan BCR'ın yürürlükte kalmasına karar verdiği bilinmektedir. Bu konuda ayrıntılı bilgi için çalışmanın 2.2.1. başlığına bakınız.

anlamda ancak Birleşik Krallığın iç hukukundaki veri koruma kanunları uyarınca hazırlanacak bir bağlayıcı şirket kurallarından söz edilecektir.

2.5.2. İsviçre

Binding Corporate Rules benzeri bir düzenleme çalışmamız tarihinde yenilenme sürecinde olan[241] 19 Haziran 1992 tarihli ve 235.1 sayılı İsviçre Veri Koruma Yasası *(alm. Datenschutzgesetz 'DSG')* içerisinde de düzenlenmektedir. İsviçre veri koruma yasası Birlik mevzuatına benzer şekilde, üçüncü ülkelere veri aktarımında 'uygun güvenlik önlemleri' aramaktadır. Kişisel verilerin İsviçre dışına aktarılması DSG md. 6'da düzenlenmektedir. Buna göre, verilerin aktarılacağı ülke hakkında İsviçre veri koruma otoritesi *(alm. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter*) tarafından verilmiş, 'eşdeğer veri koruma' seviyesi olduğuna dair bir karar yoksa, uygun güvenlik önlemlerinin alınması öngörülmüştür.

DSG md. 6/2/g'de sayıldığı şekliyle 'benimsenecek veri koruma kuralları' uygun bir güvenlik önlemi teşkil edebilmektedir. Söz konusu kuralları düzenleyebilecek çok uluslu şirketler, tek bir hukuki kişilik veya bir tek yerden yönetilen iki farklı hukuki kişilik olarak yapılanabilmektedir.[242] Yapılar arasındaki kişisel veri aktarımlarında bahsi geçen şirketler için bağlayıcı, uygun güvenlik seviyesi öngören veri koruma kuralları kullanılabilmektedir. Benimsenecek kuralların İsviçre veri koruma otoritesine bildirilmesi gerekmektedir. İsviçre veri koruma otoritesinin yurtdışına aktarılan verilerle ilgili bir muhataba sahip olabilmesi için, grup şirketlerin merkezinde bir idari merci öngörülmeli ve bildirilmelidir.[243]

Söz konusu kuralların içeriğine dair İsviçre veri koruma otoritesi tarafından yayınlanan bir rehberde[244], aşağıdaki hususlar belirtilmiştir:

- Veri koruma kuralları, asgari olarak 108 sayılı, 'Kişilerin Otomatik Yollarla Verilerin İşlenmesine Karşın Korunmasına Dair Avrupa Konseyi

[241] Datenschutz Risiken https://www.pwc.ch/de/dienstleistungen/consulting/risiken/datenschutz.html Erişim Tarihi: 03.05.2020.
[242] *Lambrou ve Steiner'e ait kısım,* MAURER-LAMBROU Urs, BLECHTA P. Gabor, Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Helbing Lichtenhahn Verlag, Basel, İsviçre 2014, s. 173.
[243] Age.
[244] EDÖB Datenübermittlung ins Ausland kurz erklärt, 10.12.2018 EDÖB Übermittlung ins Ausland https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html Erişim Tarihi: 19.04.2020.

Konvansiyonu ve Ek Protokollerinde, özel hukuk kişileri için belirlenen yükümlülüklerini taahhüt etmelidir.

- Kurallar tüm şirketler açısından bağlayıcı olarak düzenlenmeli ve pratik olarak uygulanabilirliği sağlanmalıdır.
- Söz konusu kuralların varlığı, İsviçre içinde sürdürülen veri işleme faaliyetleri açısından tâbi olunan, İsviçre Veri Koruma Yasası'nda belirlenmiş diğer yükümlülükleri kaldırmayacaktır.
- Bütün şirketler kuralları benimsemeli ve uygulamalıdır.

Görüldüğü üzere bu şirket kuralları Birlik üyesi olmayan bir devletin iç hukukunda düzenleme bulmaktadır. Bu anlamda kurallar, İsviçre dışarısına yapılacak veri aktarımları için kullanılmaktadır.

2.5.3. Asya-Pasifik Ekonomik İş Birliği ve Sınırötesi Mahremiyet Kuralları

Gizlilik Çerçevesi *(ing. Privacy Framework)* Asya-Pasifik Ekonomik İş Birliği üyesi ekonomilerce[245] 2005 yılında hayata geçirilmiş ve 2015 yılında güncellenmiştir. Bu düzenleme Asya-Pasifik Ekonomik İş Birliği üyesi birçok devleti ilgilendirmekte ve veri işleme ilkelerini ortaya koymaktadır.[246] Sınırötesi Mahremiyet Kuralları ise, bahsi geçen çerçevedeki ilkelerden yola çıkarak 2012 yılında benimsenmiştir. Şöyle ki Asya-Pasifik Ekonomik İş Birliği üye ekonomileri arasında serbest veri akışı amaçlanmıştır.

Birlik hukukuyla genel bir karşılaştırma yapmak gerekirse Tüzük'te hedeflenenin gerçek kişilerin temel hak ve özgürlüklerini korumak olduğunu söylemek mümkündür. Asya-Pasifik Ekonomik İş Birliği Gizlilik Çerçevesi ise, e-ticaretin ekonomik yararlarını korumak amacıyla geliştirilmiştir. Nitekim önsözde belirtildiği üzere sistemin amacı, *'bilgi akışının önünü kesmeyen, işler gizlilik korumaları öngörmek ve Asya-Pasifik Ekonomik İş Birliği bölgesinde ticaretin devamı ile ekonomik gelişmeyi sağlamaktır'*. Düzenlemelerin amacındaki bu farklılık, veri aktarımı hususunda benimsenecek iki temel yaklaşımı doğurmaktadır. Tüzük uyarınca veri aktarımlarında 'bölgesellik' baz alınırken,

[245] APEC'e dahil Avusturalya, Kanada, Çin, Japonya ve ABD dahil ancak bunlarla sınırlı olmayacak şekilde toplam 21 ülke bulunmaktadır.

[246] Elbette belirtmek gerekir ki GVKT, üye devletler açısından kanun niteliğindedir ve uygulama alanına giren veri sorumluları açısından bağlayıcıdır. APEC Privacy Framework ise kanun niteliğinde bir metin değildir. APEC üyesi ekonomilerin kendi veri koruma kanunlarını üzenlerken temel alacakları minimum koruma standardını belirleyen bir rehberdir. Öyle ki üye ekonomilerin bir veri koruma kanunu yoksa, ilgili kişilere sağlanacak minimum korumayı ortaya koymaktadır.

Asya-Pasifik Ekonomik İş Birliği 'organizasyon yapısını' değerlendirmektedir.[247] Sınırötesi Mahremiyet Kuralları, işletme bazlı bir veri aktarım aracıdır. Hesap verilebilirliği arttırmak amacıyla, Gizlilik Çerçevesi ilkelerini taahhüt eden özel sektör düşünülerek geliştirilmiştir.[248]

İhtiyari bir sistem olan Asya-Pasifik Ekonomik İş Birliği Gizlilik Çerçevesi'ne üye pek çok ekonominin kendi veri koruma mevzuatları bulunmaktadır. Dolayısıyla global bir veri koruma standardı getiren Asya-Pasifik Ekonomik İş Birliği Gizlilik Çerçevesi içerisindeki Sınırötesi Mahremiyet Kurallarının, *Binding Corporate Rules* yanındaki ikinci önemli uluslararası sistem olduğu söylenmektedir.[249] Ancak belirtilmelidir ki Birlik Komisyonu, Asya-Pasifik Ekonomik İş Birliği Gizlilik Çerçevesi'nin Tüzüğe göre yeterli koruma sağlamadığını söylemektedir.

Asya-Pasifik Ekonomik İş Birliği'nin benimsediği bu veri aktarım yolu temel olarak hesap verilebilirlik ilkesine bağlanmıştır. Şöyle ki, Gizlilik Çerçevesi'nin 26. prensibinde veriler üçüncü ülkeye aktarıldığında, verileri aktaran Asya-Pasifik Ekonomik İş Birliği üyesi ekonomideki veri sorumlusunun yükümlülüklerinin devam edeceği düzenlenmiştir. Prensibin devamında üçüncü ülkede meydana gelecek herhangi bir ihlalde, veriyi aktaranın ilgili kişiye karşı sorumlu olacağı da düzenlenmektedir.

Sınırötesi Mahremiyet Kuralları için şirketlerce hazırlanacak düzenlemelerden evvel, ilk olarak üye ekonomilerin ülkesel bir kabulü ve düzenlemesi gerekmektedir. Sınırötesi Mahremiyet Kuralları'na katılmak isteyen ülkeler için üç aşamalı bir süreç öngörülmüştür. İlk olarak veri koruma yükümlülüklerini düzenleyen bir çerçeve geliştirilmelidir. Ardından bağımsız hesap verilebilirlik mercileri *(ing. accountability agents)* seçme ve onaylama sistemleri yerleştirilmelidir. Son olarak da Sınırötesi Mahremiyet Kuralları düzenleyecek şirketleri denetleyebilecek bir yerel yürütme mekanizması *(ing. domestic enforcement mechanism)* öngörülmelidir. Amerika Birleşik Devletleri, 2012 yılında Sınırötesi Mahremiyet Kuralları sistemini hayata geçiren ilk ülke olmuş ve yerel yürütme mekanizması olarak Federal Ticaret Komisyonu'nu atamıştır.[250]

Yerleşik oldukları ülke şayet Sınırötesi Mahremiyet Kuralları sistemine katılmışsa, çok uluslu şirketler kendi kurallarını düzenleyebilmektedir. Düzenlenen

[247] MOEREL 2012, age, s. 59.
[248] Age, s. 60.
[249] Age.
[250] SULLIVAN, age, s. 380-397.

kuralların değerlendirilmesi için, öngörülen bağımsız kuruluşa başvurulmaktadır.[251] Düzenlenen Sınırötesi Mahremiyet Kuralları'nın uygunluğu akredite hesap verilebilirlik mercilerince elli maddelik bir önerge[252] uyarınca değerlendirilmektedir. Sınırötesi Mahremiyet Kuralları onaylandığı takdirde, düzenleyen şirkete bir sertifika sağlamaktadır. Öyle ki onaylanan Sınırötesi Mahremiyet Kuralları temelde, katılan işletmelerin Gizlilik Çerçevesi içerisindeki ilkeleri taahhüt ettiklerini gösteren bir sertifikadır.[253]

Amacı itibariyle incelendiğinde Sınırötesi Mahremiyet Kuralları'nın çok uluslu büyük şirketlerin ekonomik gelişimini desteklemeye müsait olduğu aşikârdır. Nitekim Amerika Birleşik Devletleri'nde Sınırötesi Mahremiyet Kuralları'nın işletme yanlısı ve daha az kısıtlayıcı bir sistem olduğu belirtilmektedir. Bu anlamda *Binding Corporate Rules'a* kıyasla tercih edilmektedir.[254]

[251] ABD'de şirketlerin düzenledikleri CBPR'ı uyum *(ing. compliance)* için denetleme yetkisine sahip hesap verilebilirlik merci *(ing. accountability agent)* olarak TrustArc Inc. örnek verilebilmektedir.
[252] APEC Cross-Border Privacy Rules System Program Requirements
[253] MOEREL 2012, age, s. 61.
[254] SULLIVAN, age, s. 380-397.

BÖLÜM 3. TÜRKİYE'DE BAĞLAYICI ŞİRKET KURALLARI

Çalışmamızda üye devletlerin ve Avrupa Ekonomik Alanındaki ülkelerin Tüzüğün direkt uygulama alanında olduklarından bahsettik.[255] Bunun yanında sınırötesi *(ing. extraterritorial)* uygulanabilirliği ile üçüncü ülkelerdeki şirketler için de önemini ortaya koyduk. Birlik'teki yeni veri koruma kurallarının, veri aktarımına dayalı ticareti derinden etkilediği aşikardır. Özellikle gelişmekte olan ülkelerdeki ekonominin büyük kısmını oluşturan dijital veri işleme faaliyetleri ve verilerle alakalı diğer tüm iş alanları söz konusu mevzuattan etkilenmektedir. Öyle ki bu iş alanları finansal muhasebe, vergi beyanları, insan kaynakları, sağlık transkriptleri, müşteri hizmetleri, çağrı merkezleri şeklinde örneklenebilir. Bahsi geçen iş alanlarının gelişmekte olan ülke ekonomilerine katkısının elli milyon dolar civarında olduğu bilinmektedir.[256] Türkiye'nin de arasında bulunduğu bu ekonomilerdeki şirketlerin Birlik mevzuatına uyumu, rakiplerine karşı avantaj da teşkil edebilecektir.

Dolayısıyla Tüzüğün Türkiye açısından önemi iki temel noktayla ele alınabilir. Bunlardan ilki, Birlik'teki kişilere mal hizmet sunan Türkiye'deki veri sorumlularının Tüzüğün sınırötesi uygulama alanına girmesidir. İkinci olarak Birlik şirketlerinin Türkiye'deki iştirakleri/ortakları ve bu iştiraklere Birlik'ten veri aktarılması gündeme gelmektedir. Özellikle ikinci husus sebebiyle Türkiye'deki veri sorumlularına bir *Binding Corporate Rules* iletilmesi ve Tüzüğe uyumunun beklenmesi olasıdır.

Bu başlık altında, Birlik mevzuatı uyarınca hazırlanmış bir *Binding Corporate Rules'un* Türk Kanunları açısından uygulaması ortaya konulacaktır. *Binding Corporate Rules'a* uyumun Kişisel Verilerin Korunması Kanunu uyarınca meydana getirebileceği aykırılıklar belirlenecektir. Bunun yanında, Türkiye'deki şirketin *Binding Corporate Rules'da* verdiği taahhütlere aykırı hareketlerinde Birlik'teki şirketin potansiyel sorumluluğu da incelenecektir. Son olarak, Türk mevzuatı açısından yeni benimsenmiş, Kişisel Verilerin Korunması Kanunu uyarınca hazırlanacak Bağlayıcı Şirket Kuralları değerlendirilerek, avantajları ortaya koyulacaktır.

---

[255] Bkz. dn. 213
[256] MATTOO, MELTZER, age, s. 769-789.

3.1 BİRLİK'TEKİ ANA ŞİRKETTEN GELEN BINDING CORPORATE RULES'UN TÜRKİYE'DE UYGULANMASI

Tüzüğün ilgili kişilerin verilerinin korunması için son derece kapsamlı ve yenilikçi bir düzenleme olduğu bilinmektedir. Ancak Dünya Ticaret Örgütü, Tüzüğün potansiyel olarak sorun yaratabileceğini de öngörmektedir. Öyle ki bu sorun, dijital ticaret imkânlarını korurken, aynı zamanda ülkelerin iç hukuklarındaki mahremiyet kurallarına uymak olarak tespit edilmiştir.[257] Dünya Ticaret Örgütü'nün belirlediği bu sorun açısından da *Binding Corporate Rules* taahhütleri potansiyel bir çözüm olarak incelenebilecektir. Zira bu taahhütler hem global ticarete etki etmekte hem de farklı iç hukuklara tâbi sorumlular için aynı kuralları öngörmektedir.

Bilindiği üzere *Binding Corporate Rules,* grup şirket yahut ekonomik iş birliği içindeki tüm şirketler için bağlayıcı şekilde düzenlenmelidir. Dolayısıyla *Binding Corporate Rules* düzenleyen yapının Türkiye'deki üyesi de taahhütlere uymakla yükümlü olacaktır. Bu noktada, Türkiye'deki şirkete uyum sağlaması için iletilen *Binding Corporate Rules*, Kişisel Verilerin Korunması Kanunu açısından bazı uyumsuzluklar yaratabilecektir. Bu uyumsuzluklar iki ana başlıkta incelenebilecektir.

Uyumsuzluğun kaynaklanabileceği ilk başlık, *Binding Corporate Rules'da* taahhüt edilen Tüzük yükümlülüklerinin, Kişisel Verilerin Korunması Kanunu'na aykırılık teşkil etmesidir. Bu noktada Kişisel Verilerin Korunması Kanunu ve Tüzük için yapılacak genel bir karşılaştırma, dikkat edilmesi gereken potansiyel çatışmaları ortaya koyacaktır. Bu çatışmalar incelenen *Binding Corporate Rules* özelinde değerlendirilmelidir.

Binding Corporate Rules şirketin kendi ihtiyaçlarına göre şirkete özel hazırlanan çözümlerdir.[258] Dolayısıyla verilecek taahhütler Tüzüğü ihlal etmediği sürece grup şirketin karar merciinin inisiyatifine bırakılmaktadır. Bu nedenle potansiyel uyumsuzlukların kaynaklanabileceği ikinci bir nokta, hazırlanan *Binding Corporate Rules'da* grup şirketin karar mercilerince Kişisel Verilerin Korunması Kanunu'na aykırı yükümlülüklerin öngörülmesidir. Bu halde *Binding Corporate Rules'un* Türk

[257] MATTOO, MELTZER, age, s. 769-789.
[258] *Spies'e ait kısım,* FORGO Nikolaus, HELFRICH Marcus, SCHNEIDER Jochen, Betrieblicher Datenschutz, 3. Auflage, C.H. Beck, München, Almanya 2019, s. 610.

kanunlarına aykırılık teşkil eden yükümlülüklerin belirlenmesi ve grup şirket içinde görüşülmesi gerekmektedir.

Belirtilmelidir ki GVKT md. 47/2/m uyarınca *Binding Corporate Rules* hazırlanırken şirket, üçüncü ülkelerde kişisel verilerin korunmasına dair ilgili mevzuatı araştırmakla yükümlüdür. Öyle ki kişiler için dezavantaj yaratabilecek düzenlemeler belirlenmeli ve ilgili mercilere raporlanmalıdır. Dolayısıyla *Binding Corporate Rules'u* hazırlayan yapının Türkiye'de bir üyesi mevcutsa, Kişisel Verilerin Korunması kanunu hakkında genel bir değerlendirme yapılacaktır. Benzer konuları düzenleyen bu iki mevzuatın, farklı şekilde öngördüğü hususlar aşağı başlıkta incelenmiştir.

3.1.1. Veri Koruma İlkelerinin Uygulanması

Bilindiği üzere *Binding Corporate Rules,* Tüzüğün düzenlediği veri işleme ilkelerini taahhüt etmektedir. Bu nedenle söz konusu ilkelerin Kişisel Verilerin Korunması Kanunu'ndaki karşılıkları *Binding Corporate Rules* özelinde incelenmelidir. Çalışmamızın 1.1. başlığında veri işleme ilkeleri incelenirken, Kişisel Verilerin Korunması Kanunu'ndaki karşılıkları da belirlenmiştir. Aşağıda ise Tüzük'teki veri işleme ilkelerinin *Binding Corporate Rules'daki* genel görünümleri ve Türk hukuku açısından yaratabilecekleri potansiyel uyumsuzluklar değerlendirilecektir.

Binding Corporate Rules'un şeffaflığı arttırmayı amaçladığı çalışmamızda ortaya konulmuştur. Şüphesiz ki GVKT md. 5/1/a'da düzenlenen hukuka uygun ve adil işleme ile şeffaflık ilkesi[259] bu anlamda *Binding Corporate Rules* için önemlidir. Tüzüğe göre hukuka uygun veri işleme için, veri işleme ilkelerinin yanında GVKT md. 6/1 kataloğunda sıralanan hukuka uygunluk gerekçelerinden birinin de varlığı aranmaktadır. Benzer şekilde Kişisel Verilerin Korunması Kanunu'nda da kişisel verileri işleme şartları öngörülmüştür. Tüzük ile benzer bu şartlar KVKK md. 5'de yer almaktadır. Ancak buna rağmen GVKT md. 6/1 kataloğu *Binding Corporate Rules* uyumu sağlayacak Türkiye'deki şirket için de bağlayıcı şekilde uygulanmalıdır.[260]

Şöyle ki hukuka uygun veri işleme ilkesi için uygulamada farkın yoğun hissedileceği hususlardan biri veri işleme şartı olan rızaya ilişkindir. Nitekim

[259] Hukuka uygun ve adil işleme ile şeffaflık ilkesine dair ayrıntılı inceleme için çalışmanın 1.1.1. başlığına bakınız.
[260] *Kamp'a ait kısım*, von dem BUSSCHE, VOIGT, age, s. 349.

çalışmamızın bir sonraki başlığında rıza ve açık rıza kavramı arasındaki farklar ayrıntılı incelenecektir. Bu başlık altında rıza, ancak hukuka uygun veri işleme örneği olarak değerlendirilmiştir.

Öyle ki KVKK md. 5/1'de kişisel verilerin işlenmesi için açık rıza aranmaktadır. Bir başka ifade ile zımni bir şekilde verilen rıza kabul edilmemektedir. Maddenin 2. fıkrasında ise açık rıza harici hukuka uygun veri işleme halleri sayılmıştır. Tüzük açısından ise kişisel verilerin işlenmesi için ilgili kişinin rızası yeterli sayılmaktadır ve 6. maddede sayılan hukuka uygunluk sebeplerinden biridir.

Bu nedenle *Binding Corporate Rules* uyumu sağlayan Türkiye'deki şirket, ilgili kişinin rızasını alırken KVKK md. 5/1'de öngörülen şekilde açık rıza almalıdır. Öyle ki, hukuka uygun veri işlenmesi için GVKT md. 6/1/a uyarınca alınan rıza, Türk hukukunda aranan açık rıza için yeterli olmayabilir.[261]

GVKT'nin 5/1/b hükmünde düzenlenen amaçla sınırlılık ilkesi[262] ise, pratik açıdan Kişisel Verilerin Korunması Kanunu'nda karşılık bulmaktadır.[263] Bu ilke *Binding Corporate Rules* içinde taahhüt edilirken, grup şirket veya ekonomik iş birliği içerisindeki iştiraklerin tüm üyelerinin veri işleme amaçları belirlenmelidir. Dolayısıyla yapıya dahil olan Türk şirketi, kendi veri işleme faaliyetlerine dair tüm amaçları belirleyerek bunları bildirmelidir.[264]

Amaçla sınırlılık ilkesinin veri işleyen *Binding Corporate Rules*'unda gündeme geldiği hususlardan biri veri işleme sözleşmelerini ilgilendiren veri aktarımlarıdır. Bilindiği üzere *Binding Corporate Rules* grup şirket yapısı içerisindeki veri aktarımları açısından uygun güvenlik önlemi teşkil etmektedir. Ancak grup şirket içindeki bir üyenin imzaladığı özel bir veri işleme sözleşmesi gereğince üçüncü ülkelerdeki grup şirket üyelerine yapılacak aktarımlarda, imzalanan veri işleme sözleşmesinde belirlenen amaçların dışına çıkılamamaktadır.[265] Öyle ki *Binding Corporate Rules* içerisinde veri işleme amaçları daha geniş bir şekilde belirlenebilmektedir. Buna rağmen üyeler arasında imzalanan veri işleme sözleşmesinde, işleme amaçları sınırlanmış olabilir. Dolayısıyla

[261] GVKT'nin düzenlediği biçimde geçerli rızaya dair ayrıntılı bilgi için bkz. KÜHLING, KLAR, SACKMANN, age, s. 156, 157.
[262] Amaçla sınırlılık ilkesine dair ayrıntılı inceleme için çalışmanın 1.1.2. başlığına bakınız.
[263] KÜZECİ, age, s. 206.
[264] *Kamp'a ait kısım*, von dem BUSSCHE, VOIGT, age, s. 349.
[265] Age.

grup şirket üyeleri arasında imzalanan veri işleme sözleşmesi gereğince aktarılan veriler, ancak bu sözleşmede belirlenen amaçlarla işlenebilmektedir.

Bu nedenle *Binding Corporate Rules'da*, üçüncü ülkelerdeki kanuni düzenlemeler sebebiyle, veri işleme sözleşmelerinde belirlenen yükümlülüklere uyulamaması ihtimali için de somut önlemler öngörülmelidir. Kural olarak üçüncü ülkedeki veri işleme sözleşmesi yükümlülüklerine aykırı düzenlemeler, veri işleme faaliyeti öncesinde veri işleme sözleşmesinin karşı tarafı ile paylaşılmalıdır.[266]

Dolayısıyla *Binding Corporate Rules* açısından amaçla sınırlılık ilkesinin Türk şirketine iki farklı etkisi mevcuttur. İlk olarak Türk şirketinin faaliyetleri dolayısıyla gündeme gelen veri işleme amaçları belirlenmeli ve *Binding Corporate Rules'a* dahil edilmelidir. İkinci olarak grup şirketin diğer üyeleriyle Türkiye'deki üye arasında imzalanmış veri işleme sözleşmelerindeki amaçlar incelenmelidir. Bu amaçlar için de Türk mevzuatına aykırı bir hüküm olup olmadığını değerlendirilmelidir.

Sırasıyla GVKT md. 5/1/c ve 5/1/e'de düzenlenen asgari düzeyde veri işleme[267] ve sınırlı muhafaza[268] ilkeleri Türk hukukuna yabancı değildir. Söz konusu ilkelerin yerine getirilmeleri için *Binding Corporate Rules'da* şirket politikası olarak, özellikle verilerin muhafaza sürelerinin belirlenmesi gerekmektedir.[269] Elbette ki Türkiye'deki şirket, işlediği kişisel verilerin saklanma sürelerini, Türk hukukunda kanunda öngörülen saklama sürelerine göre düzenleyecektir. Kanunda özellikle bir saklama süresi öngörülmediği hallerde, verinin kaynaklandığı sözleşme ilişkisinden doğabilecek taleplerin zamanaşımı süreleri, saklama süresi olarak belirlenebilecektir.

Binding Corporate Rules'da belirlenen saklama sürelerinin, Türk hukuku uyarınca şirketin verileri saklamakla yükümlü olacağı sürelere aykırı olmadığından da emin olunmalıdır. Bu durum için verilebilecek bir örnek, Türk hukuku açısından özlük dosyalarının iş ilişkisinin bitiminden itibaren on yıl[270] saklanma yükümlülüğüdür. Velev ki *Binding Corporate Rules* özlük dosyalarının iş ilişkisi bitiminden beş yıl sonra silinmesini öngördüyse, bu yükümlülük Türk şirketin tâbi olduğu iç hukuka aykırıdır.

---

[266] Age.
[267] Asgari düzeyde veri işleme ilkesine dair ayrıntılı açıklama için çalışmanın 1.1.3. başlığına bakınız.
[268] Sınırlı muhafaza ilkesine dair ayrıntılı açıklama için çalışmanın 1.1.5. başlığına bakınız.
[269] *Kamp'a ait kısım*, von dem BUSSCHE, VOIGT, age, s. 351.
[270] 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu md. 93 ve md. 102.

İncelenmesi gereken diğer bir ilke GVKT md. 5/1/d'de düzenlenen doğruluk[271] ilkesidir. İlke uyarınca, kişisel verilerin doğruluğunun kontrolü için alınacak idari ve teknik tedbirler *Binding Corporate Rules'da* belirtilmelidir. Belirlenen bu tedbirlere Türk şirketi de uymalıdır.[272] Alınacak tedbirlere örnek olarak, müşteri kişisel verilerinin her beş ayda bir kontrol edilmesi veya farklı veri gruplarının ayrı yerlerde şifrelenerek depolanması verilebilir.

Doğruluk ilkesiyle ilişkili şekilde GVKT md. 16 kişisel verilerin düzeltilmesi ve GVKT md. 17 unutulma hakkı da önem kazanmaktadır. GVKT md. 19 uyarınca kişisel verilerin silinmesi yahut işlenmesinin kısıtlanması halinde bu durum, verilerin aktarıldığı kişilere de bildirilmelidir. *Binding Corporate Rules* veri aktarımını ayrıntısıyla düzenlediğinden, söz konusu GVKT md. 19 bildirim sürecinin nasıl yürütüleceğini de öngörmelidir.[273] Şüphesiz ki *Binding Corporate Rules* taahhüdü, verilerin aktarım sürecini şeffaf bir şekilde ortaya koyduğundan, bu yükümlülüğün yerine getirilmesini de kolaylaştıracaktır.

Son olarak Tüzüğün şeffaflığın sağlanması adına ağırlık verdiği verilerin, tasarım itibariyle ve varsayılan olarak korunması *(ing. data protection by design and default)*[274] kavramları incelenmelidir. *Binding Corporate Rules* gibi etik düzenlemeleri, bir yandan bu ilke yükümlülüğünü yerine getirme amacı taşımaktadırlar. Nitekim GVKT 108. gerekçe maddesi *Binding Corporate Rules'un* genel veri koruma ilkeleri yanında, verilerin tasarım itibariyle ve varsayılan olarak korunmasını taahhüt etmesi gerektiğini belirtmektedir.

Verilerin, tasarım itibariyle ve varsayılan olarak korunması kavramları Kişisel Verilerin Korunması Kanunu içerisinde yer almamaktadır. Ancak bu kavramlar şüphesiz ki kanunun düzenlenme amacıyla[275] paralel niteliktedirler. Nitekim T.C. Kalkınma Bakanlığı tarafından konu üzerine hazırlanan bir raporda, verilerin tasarım itibariyle ve varsayılan olarak korunmasının önemi vurgulanmıştır. Raporun devamında verilerin

[271] Doğruluk ilkesine dair ayrıntılı açıklama için çalışmanın 1.1.4. başlığına bakınız.
[272] *Kamp'a ait kısım*, von dem BUSSCHE, VOIGT, age, s. 353
[273] Age.
[274] Verilerin tasarım itibariyle ve varsayılan olarak korunması çalışmanın 1.1.1. başlığında incelenmiştir.
[275] KVKK md.1 Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumayı amaçlamaktadır.

tasarım itibariyle ve varsayılan olarak korunmasının, Kurul kararlarıyla hazırlanacak ikincil düzenlemelerde dikkate alınması gerektiği belirtilmiştir.[276]

3.1.2. Rıza ve Açık Rıza Kavramı

Tüzük içerisinde rıza ve açık rıza kavramları arasında bir ayrım yapılmıştır. Alınacak tüm rızaların kişinin kendi verilerinin işlenip işlenmemesine, işleniyorsa da hangi bağlamlarda işleneceğine dair gerçek rızasını belirtmesi gerekmektedir.[277] Açık rızanın temel farkı ise yazılı veya sözlü açık bir ifade içermesidir.[278] İlgili kişi, bir ifadeyi açıkça onayladığını belirten bir hareketi ile rıza verebilmektedir. Açık rıza için ise mutlaka, onaylama ve rızanın kelimelerle ifade edilmesi gerekmektedir.[279]

Burada belirtmek gerekir ki Divan'ın *Planet49* kararı, hukuka uygun bir rıza için aktif bir hareket aramaktadır.[280] Öyle ki rıza bir kutucuğa tıklanarak verilebilmektedir. Ancak halihazırda işaretlenmiş bir kutucuğun varlığı ve rıza verilmiyorsa kutucuğa tıklanarak geri çekilmesi, hukuka uygun rıza için yeterli sayılmayan pasif bir hareket olarak değerlendirilmektedir.[281]

Rıza GVKT md. 6 uyarınca kişisel verilerin işlenmesi için öngörülen hukuka uygunluk sebepleri arasında merkezi bir rol oynamaktadır.[282] Nitekim rıza, ilgili kişinin verisinin işlenmesine dair hür iradeyle vereceği, belirli, bilgilendirmeye dayanan ve kesin olarak düzenlenen bir hukuka uygunluk sebebidir. [283] Açık rıza ise ancak GVKT md. 9/2/a uyarınca düzenlenen özel nitelikli kişisel verilerin işlenmesi için aranmaktadır. Bunun yanında GVKT md. 22/2/c uyarınca ilgili kişi, otomatik yollarla veri işlenmesi (profilleme) için de açık rıza vermektedir.

---

[276] T.C. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Haziran 2017 tarihli Avrupa Birliği Genel Veri Koruma Tüzüğünün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi Konulu Çalışma Raporu
http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf
Erişim Tarihi: 30.04.2020.
[277] *Buchner ve Petri'ye ait kısım*, KÜHLING, BUCHNER, age, s. 220.
[278] What is explicit consent? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ Erişim Tarihi: 08.01.2021.
[279] Age.
[280] AAD C - 673/17, 62
[281] AAD C - 673/17, 37, 52, 55, 57, 62.
[282] *Buchner ve Petri'ye ait kısım*, KÜHLING, BUCHNER, age, s. 220.
[283] *Frenzel'e ait kısım,* PAAL, PAULY, age, s. 108 vd.

GVKT md. 7 rızanın geçerliliği için pek çok koşul öngörmektedir.[284] Öyle ki, her zaman için verildiği kadar kolay biçimde geri çekilebilmesi ve bu hakkın nasıl kullanılacağının kolay anlaşılır ve erişilir şekilde açıklanması gerekmektedir. Ek olarak, rızanın bir hizmet sunumu açısından ön koşul olarak düzenlenmesi halinde, hür iradenin sakatlanacağı ve rızanın geçersiz sayılacağı da belirtilmiştir.[285]

Tüzük aksine Kişisel Verilerin Korunması Kanunu rıza ve açık rıza ayrımı yapmamakta ve hukuka uygun veri işleme sebebi olarak açık rızayı temel almaktadır. [286] Kişisel Verilerin Korunması Kanunu'nda düzenlenen açık rıza, belirli bir konuya ilişkin verilen, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade etmektedir. Tüzük düzenlemesine paralel şekilde, Kişisel Verilerin Korunması Kanunu da açık rızanın hizmet sunumuna önkoşul olarak düzenlenemeyeceğini belirtmiştir. Öyle ki, Kurul'un Amazon Türkiye hakkında verdiği güncel kararda[287], alınan açık rızanın hizmet sunumuna önkoşul olarak düzenlendiğinden bahsedilmiş ve hür iradenin sakatlandığı sonucuna varılmıştır. Söz konusu gerekçe dahil Kanun'a tüm aykırılıklar sebebiyle toplam 1.200.000 TL tutarında idari para cezası uygulanmasına karar verilmiştir.

Dolayısıyla Türkiye'de açık rıza kavramının Tüzüğe yakın şekilde; benzer ilkeler üzerinden yorumlandığı söylenebilecektir. Ancak belirtmek gerekir ki Tüzüğe göre rızanın yeterli sayıldığı hallerin, Kişisel Verilerin Korunması Kanunu'nun aradığı açık rızayı karşılamaması mümkündür. Bu anlamda *Binding Corporate Rules* taahhüdü veren Türkiye'deki üye şirket hukuka uygunluk sebebi olarak açık rızaya dayanıyorsa, rızanın KVKK md. 5/1'e uygun şekilde alınmasını sağlamalıdır.

---

[284] Buna göre rıza, eğer herhangi bir hizmet sunumu benzeri bir koşula bağlanmışsa, hür iradeyle verilmiş sayılmamaktadır. Ek olarak rızanın açık bir onaylayıcı hareketle verilmesi gerekmektedir. Ayrıca rızayı geri çekmek için veri sorumlusunun öngördüğü sistem, ilgili kişiye rızayı vermeden evvel iletilmelidir. Rızanın geçerliliği için sağlanması gereken bilgilere dair ayrıntılı açıklama, GVKT gerekçe md. 42'de yer almaktadır.

[285] GVKT gerekçe md. 42

[286] KVKK md. 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 islenmesinin 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 hallerinde ilgili kişinin açık rızası olmaksızın kişisel verileri işlenebilmektedir.

[287] Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Kararı https://www.kvkk.gov.tr/Icerik/6739/2020-173 Erişim Tarihi: 24.05.2020.

3.1.2.1. İş İlişkisi Kapsamında Açık Rıza

KVKK md. 6/2 özel nitelikli kişisel verilerin[288], ilgili kişinin açık rızası olmadan işlenmesini yasaklamıştır. İş ilişkisinden doğan özel nitelikli kişisel verilerin işlenmesi (ör. çalışanların parmak izi, sağlık verileri, ceza mahkumiyeti, eski tip nüfus cüzdanlarında yer aldığı şekliyle dini inançları vs.) değerlendirilmesi gereken hassas noktalardan biridir. Uygulamada şirketlerin çoğu, hukuka uygunluk temeli oluşturması için çalışanlardan özel nitelikli kişisel verilerinin işlenmesine dair açık rıza metinleri almaktadırlar. Söz konusu açık rıza metinlerinin, taraflar arasındaki güç ilişkisinden ötürü işçinin özgür iradesini yansıttığı söylenemeyecektir. Öyle ki bu rızanın Tüzüğe göre geçersiz olduğu bilinmektedir.[289]

Nitekim Danıştay 5. daire henüz Kişisel Verilerin Korunması Kanunu yürürlüğe girmediği tarihte, Birlik hukuku ve Anayasa md. 20/3'den yararlanarak iş ilişkisi kapsamında alınan parmak izine dair bir değerlendirme yapmıştır. Parmak izi verisinin Kişisel Verilerin Korunması Kanunu kapsamında biyometrik veri olduğu ve özel nitelikli kişisel veri olarak değerlendirildiği bilinmektedir. Kararda mesai takibi için çalışanlardan parmak izi alınmasının, kamusal alanda olsa dahi özel hayatın gizliliği ilkesini ihlal ettiğine hükmedilmiştir.[290]

Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesiyle şart ve koşulları açıkça düzenlenen biyometrik veri işleme faaliyetine dair, Kurul'un 25/03/2019 ve 31/05/2019 tarihinde verdiği kararlar ise konu hakkında açıklayıcı olmuştur. Giriş çıkış kontrollerini biyometrik veri işleyerek sağlayan iki ayrı spor salonu hakkında yapılan değerlendirmede, veri işleme faaliyetinin KVKK md. 4/2'de düzenlenen 'işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma' ilkesiyle bağdaşmadığına hükmedilmiştir. Karardaki önemli bir başka husus olarak, hizmet sunumunun biyometrik veri işlenmesi

[288] KVKK md. 6/1 uyarınca 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 özel nitelikli kişisel veridir.

[289] BRAUN, A. Cihan, İşçilerin İşyerinde Video Kamerayla İzlenmesinin Kişisel Verilerin Korunması Hakkı ve Genel Kişilik Hakkı Çerçevesinde Değerlendirilmesi, Yeditepe Üniversitesi Hukuk Fakültesi 8-9 Aralık 2018 tarihli Avrupa ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Konulu Uluslararası Sempozyum, 2018.

[290] Danıştay 5. daire 2013/5342 E. 2013/9525 K.

için verilen açık rızaya bağlandığı tespit edilmiş ve bu durumun Kanun'a aykırı olduğu ortaya konulmuştur.[291]

Yukarıdaki açıklamalardan anlaşıldığı üzere özel nitelikli kişisel verilerin işlenmesi için alınan açık rıza değerlendirilirken iki temel nokta incelenmektedir. İlk olarak veri sorumlusu ve ilgili kişi arasındaki güç ilişkisi değerlendirilmektedir. Şüphesiz ki bu ilişki açık rızada hür iradenin tespiti için önemlidir. İkinci olarak amaç incelenmektedir. Öyle ki yapılan işin niteliği, yüksek koruma gerektiriyorsa ilgili kişiden özel nitelikli kişisel verilerin alınması gerekli olabilecektir. Örneğin çalışma alanı tehlikeli bir nükleer santral ise, parmak izine kıyasla daha az güvenlik sunan kartlı geçiş sisteminin getirilmesi mümkün olmayabilir. Ancak sıradan pek çok örnek için böyle bir durumun mevcut olmadığı açıktır. Bundandır ki, çalışanların özel nitelikli verilerinin açık rıza ile işlenmesinin, bir önceki paragrafta açıklandığı şekliyle hem Tüzüğe hem de Kişisel Verilerin Korunması Kanunu'na aykırı olacağını söylemek isabetlidir.

İş ilişkisi kapsamında değerlendirilmesi gereken bir diğer nokta ise çalışanların sağlık verileridir. Öyle ki sağlık verileri Kişisel Verilerin Korunması Kanunu ve Tüzük uyarınca özel nitelikli kişisel veri sayılmaktadır. İşveren 6331 sayılı İş Sağlığı ve Güvenliği Kanunu uyarınca çalışanlardan alacağı sağlık verilerini, kanunun 15. maddesi 5. bendi uyarınca gizli tutmakla yükümlüdür. Sağlık verileri işyeri hekimliğince işlenmektedir.[292] Dolayısıyla sağlık verilerine dair *Binding Corporate Rules'da* grup şirket politikası olarak, Türk hukukunun aradığı korumanın altında bir yükümlülük öngörülmemesine dikkat edilmelidir.

3.1.3. Yurtiçi ve Yurtdışı Veri Aktarımına Dair Yükümlülükler

Binding Corporate Rules grup şirket içinde üçüncü ülkelerdeki üyelere yapılacak aktarımlarda GVKT md. 47 uyarınca uygun güvenlik önlemi sayılmaktadır. Bu nedenle *Binding Corporate Rules'u* taahhüt eden grup şirket üyeleri arasında, başkaca bir taahhüt verilmeden, serbest veri akışı sağlanmaktadır. Ancak *Binding Corporate Rules* sadece bu taahhüdü veren, üye şirketlere yapılacak veri aktarımlarında uygun güvenlik önlemi

[291] Kurul'un 25/03/2019 tarihli ve 2019/81 numaralı kararı.
Kurul'un 31/05/2019 tarihli ve 2019/165 numaralı kararı.
https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 Erişim Tarihi: 04.08.2020.

[292] Kişisel Verileri Koruma Kurumu 27.03.2020 tarihli Kamuoyu Duyurusu https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler- Erişim Tarihi: 08.01.2021.

oluşturmaktadır. Dolayısıyla üçüncü ülkedeki üye şirket kendisine aktarılan kişisel verileri, grup şirket yapısı içerisinde olmayan diğer şirketlere aktarırken başkaca uygun güvenlik önlemlerini almakla yükümlüdür.[293]

Örneğin Türkiye'deki üye şirket kendisine aktarılan verileri, Türkiye'deki üçüncü şirketlere aktarırken hem Tüzük'ten hem de Kişisel Verilerin Korunması Kanunu'ndan doğan veri aktarım yükümlülüklerine uymalıdır. Zira Tüzük'te veri aktarımına dair düzenlenen yükümlülükler, ileri aktarımlar[294] için de geçerlidir. Nitekim bu ihtimal çalışmamızın 1.3.1. ve 1.3.3. başlıklarında ayrıntısıyla açıklanmıştır. Öyle ki *Binding Corporate Rules* ileri aktarım ihtimalini de gözeterek ne gibi güvenlik önlemlerinin alınacağını belirlemelidir.[295]

Binding Corporate Rules'da ileri aktarımlar için öngörülen güvenlik önlemlerinin Kişisel Verilerin Korunması Kanunu'na aykırılık teşkil etmeyeceğinden emin olunmalıdır. Unutulmamalıdır ki Türkiye'deki şirketin yapacağı veri aktarımları, ilk olarak Kişisel Verilerin Korunması Kanunu'na tâbidir. Şayet böyle bir aykırılığın bulunmadığı halde *Binding Corporate Rules'da* belirlenen yüksek koruma standartları Türkiye'deki ileri veri aktarımlarında da geçerliliğini koruyacaktır.

Şöyle ki, kişisel verilerin aktarılması, KVKK md. 8'de kural olarak ilgili kişinin açık rızasına bağlanmıştır. Açık rıza haricindeki hukuka uygun veri işleme halleri maddenin ikinci fıkrasında düzenlenmektedir. Kanun'a göre kişisel verilerin hukuka uygun işlenmesi için öngörülen haller [296], verilerin aktarılması[297] için de geçerlidir. Ancak Türkiye'de yapılacak ileri veri aktarımlarında bu hallerin *Binding Corporate Rules* yükümlülükleri ile uyumlu olmasına dikkat edilmelidir.

---

[293] *Wieczorek'e ait kısım*, SPECHT, MANTZ, age, s. 188.

[294] GVKT kapsamında bir veri sorumlusu/işleyenin kendisine aktarılan kişisel veriyi, bir başka veri sorumlusu/işleyene aktarmasına 'ileri/sonraki aktarım' adı verilmektedir *(ing. onward transfer, alm. Weiterübermittlung).* Kurum, hazırladığı dokümanlarda söz konusu aktarımdan, benzer şekilde 'sonraki aktarım' adıyla bahsetmiştir.

[295] *Wieczorek'e ait kısım,* SPECHT, MANTZ, age, s. 188.

[296] Rızaya dair ayrıntılı inceleme için çalışmanın 3.1.2. başlığına bakınız.

[297] KVKK md. 6/3 uyarınca sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği düzenlenmektedir. Fıkranın devamında, sağlık ve cinsel hayata ilişkin kişisel verilerin 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 düzenlenmektedir. Özel nitelikli kişisel verilerin işlenmesinde md. 6/4'de belirtildiği şekilde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

Türkiye'den yurtdışına kişisel veri aktarımı ise KVKK md. 9'da düzenlenmektedir. Buna göre kişisel verinin yurtdışına aktarımı için kural olarak, ilgili kişinin açık rızası öngörülmektedir. Ancak kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunduğu hallerde[298] açık rıza harici kanunda öngörülen diğer hukuka uygun veri işleme halleri burada da uygulanmaktadır. Şayet kişisel verilerin aktarılacağı ülkede yeterli koruma bulunmuyorsa, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri[299] ve Kurul'un izninin bulunması kaydıyla, açık rıza harici kanunda öngörülen diğer hallere yine dayanılabilmektedir.

Bilindiği üzere *Binding Corporate Rules* ancak Tüzük'ten doğan yükümlülüklere uyumu sağlamaktadır. Dolayısıyla Türkiye'deki şirketin *Binding Corporate Rules* için verdiği taahhütler Kişisel Verilerin Korunması Kanunu'ndan doğan yükümlülüklerini etkilememektedir.[300] Bundandır ki Türkiye'deki üye şirketten, grup şirketin Birlik'teki üyelerine yapılacak aktarımlar, Kişisel Verilerin Korunması Kanunu kapsamında yurtdışına veri aktarımı teşkil etmektedir. Bu nedenle Türkiye'den grup şirketin yurtdışındaki üyelerine yapılacak veri aktarımları KVKK md. 9 düzenlemesine tâbi olacaktır.

Bu anlamda şirket yapısı içerisindeki veri aktarımlarını düzenlemek adına geçerli bir Bağlayıcı Şirket Kuralları düzenlemesi, çalışmamızın 3.3. başlığında incelenecektir. Şüphesiz ki *Binding Corporate Rules'un* Türkçe'ye tercüme edilerek ve gerekli ek taahhütler verilerek Bağlayıcı Şirket Kuralı olarak onaylatılması da düşünülebilir. Ancak Bağlayıcı Şirket Kuralları düzenlenmemesi ihtimalinde Türkiye'deki şirket aşağıda belirtilen hususlara dikkat etmelidir.

Türkiye'den grup şirket yapısı içerisindeki yurtdışındaki şirketlere yapılacak kişisel veri aktarımlarında, ilgili kişinin açık rızası aranmaktadır. Kurul yeterli korumanın bulunduğu ülkeleri ilan ettiğinde, Türkiye'den kişisel verilerin aktarıldığı grup şirket

---

[298] KVKK md. 9/3 uyarınca Kurul, yeterli korumanın bulunduğu ülkeleri ilan edecektir. Çalışmamızın tarihi itibariyle henüz, hangi ülkelerde yeterli korumanın bulunduğu ilan edilmemiştir.

[299] KVKK md. 9/4 uyarınca Kurul, yabancı ülkede yeterli koruma bulunup bulunmadığına ve yeterli korumanın bulunmadığı hallerde, veri sorumlularının md. 9/2b uyarınca hazırladıkları taahhüt metnine izin verilip verilmeyeceğine; a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri, b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç, ve süresini, ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri değerlendirmek ve ihtiyaç duyması halinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

[300] ÇEKİN 2020, age, s. 120 vd.

üyelerinin bu listedeki ülkeler arasında olup olmadığı incelenmelidir. Verilerin aktarıldığı üyeler şayet yeterli korumanın bulunduğu ülkeler arasındaysa, kişisel veriler KVKK md. 5/2 ve 6/3'e dayanarak aktarılabilecektir. Kurul, söz konusu yeterli korumayı sağlayan ülkeler listesini açıklayana kadar ilgili kişilerin açık rızasının alınmasının haricinde diğer yöntemler mevcuttur. Buna göre Türkiye'den verileri aktaran grup şirket üyesiyle, verilerin aktarılacağı diğer grup şirket üyesi arasında taahhüt metni imzalanarak Kurul'un izninin alınması gereklidir. Eğer bir grup şirket yapısı mevcutsa düzenlenen Bağlayıcı Şirket Kuralları da grup şirket üyeleri arasında hukuka uygun veri aktarımı sağlayabilecektir.

3.1.3.1. AAD C-101/01 Bodil Lindqvist Kararı ve Bulut Bilişime Etkisi

Hangi veri işleme faaliyetlerinin KVKK md. 8 uyarınca aktarım sayılacağını ve hangi durumlarda KVKK md. 9 kapsamında yurt dışına veri aktarımından bahsedileceğini belirlemek önemlidir.

Veriyi yalnızca internete yükleyerek yurt dışından da erişilebilir kılmanın, üçüncü ülkelere aktarım sayılıp sayılmayacağı, Divan'ın *Lindqvist* kararında tartışılmıştır.[301] Kararda bir verinin sırf internete yüklenmesinin başlı başına yurt dışına aktarım anlamına gelmeyeceğine hükmedilmiştir.[302] *Lindqvist* kararıyla konulan kritere göre, üçüncü bir ülkeye veri aktarımından bahsedilmesi için, verilerin direkt o ülkeye gönderilmesi gereklidir. Öyle ki, verinin sadece internet üzerinden erişime açılması ve erişimin üçüncü bir ülkeden de mümkün olması yeterli değildir.

Kararda, verilerin bir internet sunucusuna yüklenerek her ülkeden erişilebilir kılınmasını sağlayan bulut bilişim teknolojisinden açıkça bahsedilmemektedir. Zira *Lindqvist* kararı döneminde, bulut bilişimin henüz kullanımda değildir.[303] Bu nedenle bulut bilişime ilişkin kriterler tartışılmamıştır. Bu karar dikkate alındığında, bulut bilişim kullanımında da verinin yalnızca internete yüklenmesinden hareketle, yurt dışına aktarım sayılmayacağı gibi bir soru akla gelebilmektedir.

Ancak *Lindqvist* kararı ilkeleri Tüzük çerçevesinde incelendiğinde, bulut bilişim hizmet sağlayıcısının sunucularının (*server)* Birlik dışında olmasının, üçüncü ülkelere

[301] AAD, C-101/01 (Lindqvist), 60-61, 68, 70, 06.11.2003 T.
[302] ÇEKİN 2020, age, s. 130.
[303] REGALDO Antonio (2011), 'Who coined Cloud Computing', MIT Technology Review https://www.technologyreview.com/s/425970/who-coined-cloud-computing/ Erişim Tarihi: 13.04.2020.

veri aktarımı için yeterli olduğu söylenmektedir.[304] Şöyle ki, kişisel verinin Birlik dışındaki sunuculara yerleştirilmesi faaliyeti, üçüncü ülkelere aktarım anlamına gelmektedir. Zira burada verinin sadece internet üzerinden erişime açılması ve erişimin üçüncü bir ülkeden de mümkün olmasından öte bir durum söz konusudur. Nitekim Avrupa Birliği Veri Koruma Denetmeni, uluslararası veri aktarımı konusunda hazırladığı bir bilgilendirme yazısında bulut bilişime açık referans vermektedir.[305]

Bulut bilişim hizmeti, depolama alanı, sunucu ya da diğer hizmetlerin internet üzerinden sunulmasını ifade etmektedir.[306] Bundandır ki barındırdığı temel risklerden biri, şeffaflığın eksik olması ve sunulan hizmete pek çok farklı ülkede kurulu hizmet sunucularının ve alt sunucuların dâhil olabilmesidir.[307] Dolayısıyla verilerin çoğu zaman nerede tutulduğunu, hangi ülkedeki sunucuda olduklarını ve nerelere aktarıldıklarını belirlemek çok kolay olmayabilir. Bu nedenle *Binding Corporate Rules* gibi veri aktarım ve işleme süreçlerinde şeffaflığı sağlayan araçlar son derece önemlidir.

3.2. TÜRK KANUNLARINA GÖRE SORUMLULUK

Türk hukukunda kişisel verilerin korunmasına dair hükümler, Kişisel Verilerin Korunması Kanunu'nun yanında pek çok farklı mevzuatta da yer almaktadır.[308] Bundandır ki, *Binding Corporate Rules* uyumu sürecinde yalnızca Kişisel Verilerin Korunması Kanunu değil, ilgili tüm mevzuat taranmalıdır. Ek olarak elbette ki, *Binding Corporate Rules* taahhüdü veren Türkiye'deki üyenin, Türkiye'deki kişilerle ilişkilerini özel hukuk düzenleyecektir. Dolayısıyla bu kapsamda doğabilecek hak ve yükümlülükler unutulmamalıdır. Bu başlıkta Birlik hukukuna göre düzenlenmiş bir *Binding Corporate Rules'u* taahhüt eden Türk şirketinin Kişisel Verilerin Korunması Kanunu ve ilgili sair mevzuattan doğabilecek sorumluluğu incelenecektir.

---

[304] TEHRANI Pardis, SABARUDDIN Johan, RAMANATHAN Dhiviya (2018), 'Cross Border Data Transfer: Complexity of Adequate Protection and Its Exceptions', Computer Law & Security Review, C. 34, s. 582-594.

[305]European Data Protection Supervisor, International Data Transfers https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en (Erişim Tarihi: 13.04.2020)

[306] ÇEKİN 2020, age, s.242.

[307] Age, 242, 243.

[308] Bu konuda ayrıntılı bir mevzuat incelemesi için bkz. KAYA M. Bedii, Kişisel Verileri Koruma Hukuku – Mevzuat ve İçtihat, 1. Basım, On İki Levha Yayıncılık, İstanbul, Türkiye 2018.

3.2.1. Kişisel Verilerin Korunması Kanunu Açısından Sorumluluk

Veri sorumluları ve veri işleyenlerin sorumluluk halleri, Kişisel Verilerin Korunması Kanunu'nun beşinci bölümünde düzenlenmiştir. Belirtmek gerekir ki, Tüzük veri sorumluları ile işleyenler arasındaki sorumluluk ilişkisini açıkça ortaya koyarken, bu ilişki Kişisel Verilerin Korunması Kanunu'nda açık değildir. Kanun idari para cezaları konusunda hemen hemen bütün sorumluluğu veri sorumlusuna yüklemektedir. Müteselsil sorumluluk halinde ise, veri sorumlusu ile işleyen arasındaki ilişkinin niteliği ve asgari şartlarına dair bir hüküm bulunmamaktadır.[309]

3.2.1.1. Tazminat

Kişisel verilerinin hukuka aykırı işlenmesi sebebiyle zarara uğrayan ilgili kişi, KVKK md. 11/1/ğ uyarınca zararın giderilmesini talep etme hakkına sahiptir. Buna ek olarak KVKK md. 14/3, kişilik hakkı ihlal edilenlerin, genel hükümlere göre tazminat haklarını saklı tutmuştur. Çalışmamızın bu bölümünde, genel hükümlere göre Türkiye'deki veri sorumlusuna yöneltilebilecek tazminat hakkı incelenecektir.

3.2.1.1.a. Haksız Fiil

Genel hükümlere göre yöneltilebilecek tazminat talebinin ilk şartı haksız bir fiilin varlığıdır. Bilindiği üzere hukuk düzeni tarafından korunan her hakkın ihlali, bir hukuka uygunluk sebebi olmadıkça hukuka aykırı kabul edilir.[310] Bu bağlamda özel kanun niteliğindeki Kişisel Verilerin Korunması Kanunu'nda düzenlenen hukuka uygunluk sebepleri dikkate alınacaktır. Zira hukuka uygun veri işleme için KVKK md. 4'de sayılan işleme ilkelerine riayet edilmesi ve KVKK md. 5'de düzenlenen işleme şartlarından birinin varlığı gerekmektedir.

3.2.1.1.b. İlliyet Bağı

Tazminat sorumluluğu için bilindiği üzere, hukuka aykırı fiilin hayatın normal akışında, kişinin zararını meydana getirmeye elverişli olması aranmaktadır.[311]

---

[309] ÇEKİN 2020, age, s. 197.
[310] OĞUZMAN M. Kemal, ÖZ M. Turgut, Borçlar Hukuku Genel Hükümler Cilt – II, 14. Bası, Vedat Kitapçılık, İstanbul, Türkiye 2018, s. 15.
[311] Age, s. 45.

Dolayısıyla veri sorumlusunun hukuka aykırı veri işleme faaliyetinin, ilgili kişinin zararını meydana getirmeye elverişli olması beklenmektedir.

Burada belirtmek gerekir ki, ilgili kişinin zararı, her biri tek başına zararı meydana getirmeye elverişli olmayan, birden çok hukuka aykırı işleme sonucu meydana gelmiş olabilir. Örneğin ilgili kişinin zararı, *Binding Corporate Rules* ile kişisel verinin Birlik'teki üye şirkete, KVKK md. 9 yükümlülüklerine uymadan aktarılması ve Birlik'teki şirketin veri depolarında yeterli tedbirlerin alınmaması dolayısıyla bir siber saldırıya maruz kalması halinde meydana gelmiş olabilir. Bu durumda ortak illiyet bağından söz edilecektir.[312]

3.2.1.1.c. Kusur

Kişisel Verilerin Korunması Kanunu lafzında açıkça belirtilmediği için tartışmalı olan bir konu, tazminat isteminde kusur sorumluluğunun mu sebep sorumluluğunun mu benimseneceğidir. Değerlendirme yapılırken, KVKK md. 12 uyarınca veri sorumlusu ve işleyen için veri güvenliğine dair öngörülen yükümlülükler dikkate alınmalıdır.[313] KVKK md. 12 uyarınca, veri sorumlusu her türlü önlemi değil, 'gerekli önlemleri' almakla yükümlü tutulmuştur. Dolayısıyla kanun koyucunun burada, neticeye bağlı bir sorumluluk öngörmediği söylenebilecektir. Öyle ki, KVKK md. 12 hükmünde öngörülen yükümlülükleri yerine getiren veri sorumlusunun yine de sorumluluğuna gidilmesi, maddenin amacını ve pratik işlerliğini engelleyecektir.[314]

Bu anlamda KVKK md. 12 ile veri güvenliğine ilişkin öngörülen yükümlülükler, veri sorumlusunun özen borcuna işaret etmektedir. Öyle ki, zararın meydana gelmesi, özensiz davranıldığına işaret edecektir. Özen seviyesinin belirlenmesinde ise veri işleme faaliyetinin içerdiği risk dikkate alınmalıdır. Veri işleme faaliyeti ne kadar riskli ise veri sorumlusunun özen derecesi de o kadar yüksek olmalıdır.[315] Bağlayıcı Şirket Kuralları gösterilecek özen derecesini öngörmek açısından yararlı olacaktır. Zira bu kurallar hazırlanırken veri koruması etki değerlendirmesi ve risk analizi yapılması öngörülecektir. Böylece şirketin veri işleme faaliyetlerindeki risk ve bu bağlamda gösterilecek özen ortaya konulacaktır.

---

[312] Age, s. 51.
[313] ÇEKİN 2020, age, s. 172.
[314] Age., s. 173.
[315] Age, s. 173, kn. 364.

Özen borcunu yerine getirmeyen veri sorumlusunun tazminat yükümlülüğü, sebep sorumluluğu niteliğini taşıyacaktır.[316] Bu sebeple kural olarak zarar meydana geldiğinde veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini yerine getirmediği kabul edilmelidir.[317] Bu anlayış şüphesiz ki ilgili kişi de yararınadır. Ancak veri sorumlusunun ilgili hükümde öngörülen bütün koşulları yerine getirdiğini ispat etmesi halinde kendisine kurtuluş imkânı tanınmalıdır.[318] Bu noktada Bağlayıcı Şirket Kuralları'nın önemi ortaya çıkmaktadır. Zira Bağlayıcı Şirket Kuralları KVKK md. 12 yükümlülüklerinin yerine getirildiğine dair ispat aracı olarak kullanılabilecektir.

Şüphesiz ki Birlik hukukundaki görüşe paralel[319] bu bakış, ilgili kişiye ispat açısından kolaylık sağlayacaktır. Dolayısıyla Kişisel Verilerin Korunması Kanunu amacıyla da bağdaşmaktadır. Zira, kusur sorumluluğunda veri sorumlusunun kusurunu, zarara uğrayan ilgili kişi ispat etmek durumundadır. Sebep sorumluluğu kabul edildiğinde ise hukuka aykırı fiilin ve zararın ispat edilmesi yetecektir.[320]

Bahsedilen korumanın zayıf noktası, ilgili kişi ile veri sorumlusu arasında çift yönlü bir iletişimin sağlanamayışıdır. Öyle ki, KVKK md. 11 uyarınca veri sorumlusuna başvurup bilgi talebinde bulunan ilgili kişi, sunulan bilginin güvenilirliğini kontrol edememektedir. Örneğin, veri sorumlusu ilgili kişinin verisini yurtdışına aktardığında ve bu hususu ilgili kişiye ifşa etmediğinde, ilgili kişinin kendi verisinin akıbetini belirlemesi; zararı tespit etmesi zor olacaktır.[321] Bu durum en başta, ilgili kişinin anayasal bir hak olarak md. 20/3'te düzenlenen, 'kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkının'[322] kullanılmasını zorlaştırmaktadır.

Yukarıdaki tartışma düşünüldüğünde, *Binding Corporate Rules'un* ilgili kişilerin kişisel verilerin korunması hakları için pratikte ispat kolaylığı sağlayabileceği açıktır. Nitekim çalışmamızın 3.3.2. başlığında inceleneceği üzere Bağlayıcı Şirket Kuralları da

---

[316] ÇEKİN S. Mesut (2016), '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, s. 629-644, s. 638.
[317] Age.
[318] Age.
[319] *Eßer'e ait kısım,* AUERNHAMMER, age, s. 1210.
[320] ÇEKİN 2020, age, s. 174.
[321] ÇEKİN 2016, age, s. 638.
[322] T.C. Anayasası 20. Maddeye, 2010 tarihinde yapılan eklemeyle, özel hayatın gizliliğinin bir görünümü olarak kişisel verilerin korunması hakkı, anayasal koruma kazanmıştır.

KVKK md. 12 yükümlülüklerini hem veri sorumlusu şirket hem de verilerin aktarıldığı üçüncü kişiler için bağlayıcı biçimde düzenlemektedir. Buna ek olarak KVKK md. 12'de öngörülen veri güvenliğine ilişkin yükümlülüklerin pratik uygulanabilirliğini sağlamak için, veri sorumlusu şirket içerisinde bir yapı da öngörülmektedir.

Şeffaflığı ve hesap verilebilirliği arttıran bu durum, ilgili kişilere verilecek bilgilerin güvenilirliğini arttıracak ve doğruluğunu taahhüt altına alacaktır. Aynı zamanda Kurul'un da söz konusu şirketi gözetim ve denetim süreçleri, daha rahat işler bir hale gelecektir. Bu nedenle Bağlayıcı Şirket Kuralları'nın, Kişisel Verilerin Korunması Kanunu yükümlülüklerinin yerine getirildiğine dair ispat aracı olarak kullanılması da kolaylaşacaktır.[323] Bu durum elbette ki, ilgili kişilerin yanında veri sorumlusu şirketlere de kolaylık sağlayacaktır.

3.2.1.1.d. Maddi ve Manevi Zarar

KVKK md. 14/3'ün saklı tuttuğu şekilde kişilik hakları ihlal eden kişilerin tazminat hakkı, Türk Medeni Kanunu ('TMK') md. 25'de düzenleme bulmaktadır. Buna göre davacı, maddî ve manevî tazminat istemlerinin yanında, hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde de bulunabilecektir.

Kişisel verilerin hukuka aykırı işlenmesi halinde meydana gelebilecek maddi zarar düşünüldüğünde, değerlendirilmesi gereken ilk husus kişisel verilerin ekonomik değeridir. TMK md. 23 hükmü, kimsenin hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemeyeceğini, kimsenin özgürlüklerinden vazgeçemeyeceğini veya onları hukuka ya da ahlaka aykırı biçimde sınırlayamayacağını düzenlemektedir. Böylece adeta, kişiyi kendisinden korumak amaçlanmakta ve özel yaşamın da satılamayacağı ortaya konulmaktadır.[324] Buna rağmen, bir anlamda kişisel verilerle işleyen günümüz veri ekonomisinde, dijitalleşme ve gelişme için kişisel verilerin metalaştığı ve ciddi bir ekonomik değere sahip olduğu bilinmektedir.[325] Bu anlamda somut miktarı belirlemek güç olsa da kişisel veriyi işleyen veri sorumlusunun bir kazanç sağladığı aşikârdır.

[323] BŞK'nin kullanım alanlarına dair ayrıntılı inceleme için çalışmanın 3.3.1. başlığına bakınız.
[324] SEROZAN Rona Medeni Hukuk Genel Bölüm – Kişiler Hukuku, 4. Baskı, Vedat Kitapçılık, İstanbul, Türkiye 2011, s. 412.
[325] Kişisel verilerin ekonomik değerine dair ayrıntılı bir inceleme ve somut meblağlar için bkz. van LIESHOUT, Marc (2015), 'the Value of Personal Data', IFIP Advances in Information and Communication Technology, C. 457, S. 5, s. 26-38.

İlgili kişinin, kişisel verilerinin hukuka aykırı işlenmesinden dolayı uğrayabileceği somut bir zarar kalemi düşünüldüğünde ise, bankada kişiye kredi verilmemesi veya daha yüksek faiz oranıyla bir kredi verilmesi, kişinin işe alınmaması gibi haller gündeme gelebilecektir.[326]

Gündeme gelebilecek diğer zarar, kişilik hakkının ihlali nedeniyle duyulan acı, elem ve ıstırabın giderilmesi, en azından hafifletilmesi amacıyla[327] yöneltilecek manevi tazminat davalarında önem taşıyacaktır. Buna göre kişisel verilerin hukuka aykırı şekilde işlenmesi sebebiyle (örneğin işyerinde yetkisiz kişilerin, yeterli koruma bulunmaması nedeniyle ilgili kişinin sağlık verilerine erişip dedikodu yayması halinde) manevi zarara uğrayan ilgili kişi, veri sorumlusuna (bu örnekte yine işverene) gidebilecektir.

Son olarak belirtilmesi gereken husus, TMK md. 25 kapsamında davacının kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yerinde dava açabileceğidir. Bundan hareketle *Binding Corporate Rules'u* taahhüt etmiş üye Türk şirketinin, Birlik'teki şirkete ilgili kişinin verisini KVKK md. 9'a aykırı şekilde aktarması ve Birlik'te bir zararın meydana gelmesi halinde, ilgili kişi kendi yerleşim yerinde dava açabilecektir.

3.2.1.2. İdari Para Cezaları

Kişisel Verilerin Korunması Kanun'u Türkiye sınırları içerisinde uygulanmaktadır. Bundandır ki, Türkiye sınırları içerisinde bulunmamakla birlikte, Türkiye'deki veri işleme faaliyetlerinin büyük çoğunluğunu gerçekleştiren Google, Facebook gibi aktörlere doğrudan uygulanabilirliği söz konusu değildir.

Kanun'da yükümlülüklerin yöneltildiği kişiler olan veri sorumlusu ve veri işleyenin gerçek veya tüzel kişi olabileceği düzenlenmektedir. Veri sorumluları ve veri işleyenler için Tüzük'teki düzenlemenin aksine[328], Kişisel Verilerin Korunması Kanunu lafzı mutlaka bir hukuki kişilik aramaktadır. Kişisel Verilerin Korunması Kanunu veri sorumluları ve işleyenleri gerçek veya tüzel kişiliklerle sınırlanmaktadır. Kurul bir kararında, hukuki kişiliğin yanında kimliğin belirlenebilir olması gerektiğine de

[326] ÇEKİN 2020, age, s. 174.
[327] OĞUZMAN, ÖZ, age, s. 259.
[328] Kuruluş ilkesine dair ayrıntılı bilgi için çalışmanın 1.2.1. başlığına bakınız.

değinmiştir.[329] Kararda internetteki bir kullanıcı adı üzerinden yapılan hukuka aykırı bir kişisel veri işleme faaliyeti söz konusudur. Kurul, internetteki bu kullanıcı adının kişinin kimliğini belirlemeye yetmediğini tespit etmiştir. Kararın devamında kimliği belirsiz kişilerin veri sorumlusu/işleyen olamayacakları söylenmiş ve bir işlem yapılamayacağına karar verilmiştir.

Bundandır ki, Kişisel Verilerin Korunması Kanunu'nun beşinci bölümünde düzenlenen suçlar ve kabahatlerin uygulanabilmesi için, Türkiye'de kurulu ve tespit edilebilir bir hukuki kişilik aranması gerekmektedir. Nitekim, KVKK md. 18/2 uyarınca düzenlenen idari para cezaları, veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanmaktadır. KVKK md. 18'de veri sorumluları hakkında düzenlenen, çeşitli kabahatler sonucu 5.000 TL'den 1.000.000 TL'ye kadar öngörülmüş idari para cezaları, yalnızca Türkiye'deki yapının Türkiye'deki faaliyetlerini ilgilendirmektedir. Ancak bu noktada Kurul'un Facebook şirketi hakkında verdiği iki karar değerlendirilmelidir.

Kurul 11 Nisan 2019 tarihinde, Türkiye'de kurulu hukuki bir kişiliği olmayan Amerikan şirketi Facebook'a ait platformda meydana gelen ve Türkiye'deki ilgili kişilerin kişisel verilerini etkileyen hukuka aykırılık dolayısıyla idari para cezasına hükmetmiştir.[330] İdari para cezaları KVKK md. 12/1'e aykırılık dolayısıyla 1.000.000 TL, KVKK md. 12/5'e aykırılık dolayısıyla ise 550.000 TL olarak belirlenmiştir. Kurul 18 Eylül 2019 tarihinde ise, yine Türkiye'de kurulu hukuki bir kişiliği olmayan Amerikan şirketi Facebook'a ait platformda meydana gelen ve Türkiye'deki ilgili kişilerin kişisel verilerini etkileyen bir diğer hukuka aykırılık dolayısıyla idari para cezasına hükmetmiştir.[331] Bu kararda idari para cezaları KVKK md. 12/1'e aykırılık uyarınca 1.150.000 TL, KVKK md. 12/5'e aykırılık uyarınca ise 450.000 TL olarak belirlenmiştir.

KVKK md. 10 uyarınca aydınlatma yükümlülüğünü yerine getirmeyen veri sorumluları hakkında 5.000 TL'den 100.000 TL'ye kadar idari para cezası öngörülmüştür. Veri sorumlusu ve veri işleyenin KVKK md. 12'de yer alan veri

---

[329] Kimliği belirsiz kişi/kişilerin veri sorumlusu olarak kabul edilemeyeceği hakkında Kişisel Verileri Koruma Kurulunun 13/09/2018 Tarihli ve 2018/106 Sayılı Kararı https://kvkk.gov.tr/Icerik/5421/-Kimligi-belirsiz-kisi-kisilerin-veri-sorumlusu-olarak-kabul-edilemeyecegi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-13-09-2018-tarihli-ve-2018-106-sayili-Karari-Ozeti Erişim Tarihi: 24.05.2020.

[330] Facebook Hakkında Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Karar Özeti https://www.kvkk.gov.tr/Icerik/5450/2019-104 Erişim Tarihi: 08.01.2021.

[331] Facebook hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti https://kvkk.gov.tr/Icerik/5534/2019-269 Erişim Tarihi: 08.01.2021.

güvenliğine ilişkin yükümlülükleri yerine getirmemeleri halinde ise, 15.000 TL'den 1.000.000 TL'ye kadar düzenlenebilecek idari para cezasına dair müşterek sorumluluk[332] öngörülmüştür. KVKK md. 15 uyarınca veri sorumluları, Kurul'un inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içerisinde göndermek ve gerektiğinde yerinde inceleme yapmasına imkân sağlamakla yükümlüdürler.

KVKK md. 15'e göre Kurul'un, şikâyet üzerine veya re'sen yaptığı inceleme sonucunda bir ihlalin tespit edilmesi halinde, bu ihlalin giderilmesine karar verilmektedir. Söz konusu kararı en geç otuz gün içerisinde yerine getirmeyen veri sorumluları hakkında, 25.000 TL'den 1.000.000 TL'ye kadar idari para cezasına hükmedilebilmektedir. Son olarak KVKK md. 16 uyarınca Veri Sorumluları Siciline ('VERBİS') kayıt ve bildirim yükümlülüğüne uymayan veri sorumluları hakkında ise 20.000 TL'den 1.000.000 TL'ye kadar idari para cezasına hükmedilebilmektedir.

Binding Corporate Rules taahhüdü veren Türkiye'deki üyenin Kişisel Verilerin Korunması Kanunu'ndan doğacak sorumluluğu, temelde kendi faaliyetleri dolayısıyla meydana gelebilecek hukuka aykırılıkları kapsamaktadır.[333] Şöyle ki idari para cezaları açısından temel olarak dikkate alınan hususlar aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, Kurul tarafından verilen kararların yerine getirilmesi ve VERBİS kayıt ve bildirim yükümlülüğüdür. Bu anlamda verilen *Binding Corporate Rules* taahhütlerinin özellikle bu yükümlülüklere aykırı düşmemesine dikkat edilmelidir.

Son olarak belirtmek gerekir ki idari para cezaları için öngörülen makas oldukça geniştir. Buna ek olarak maddenin altında, tayin edilecek idari para cezası miktarının hangi usul ve esaslara göre belirleneceğinin düzenlenmemesi, belirsizlik yaratabilecektir. Tüzük dahilinde tayin olunacak idari para cezalarının belirlenme usul ve esasları, GVKT md. 83'de ayrıntısıyla düzenlenmiştir. Buna rağmen makasın geniş tutulması hususunun uygulamada tutarsızlıklara yol açabileceği yönünde eleştiriler mevcuttur.[334]

Bu tartışma Türkiye için de fazlasıyla geçerlidir. Kişisel Verilerin Korunması Kanunu gerekçesinde, idari para cezalarına dair makasın bilinçli şekilde geniş tutulduğu ve idari para cezasının veri sorumlusunun ekonomik gücü değerlendirilerek tayin

[332] Her ne kadar KVKK md. 12/2, veri işleyenin bulunması halinde, veri güvenliğine ilişkin sorumluluklara dair veri sorumlusu ile veri işleyenin müşterek sorumluluğunu düzenlemiş olsa da, bu sorumluluğun asgari şartlarına ve ilişkinin niteliğine dair ayrıntılı bir bilgi bulunmamaktadır. ÇEKİN 2020, age, s. 197.
[333] GVKT açısından sorumluluk ise, aksi şekilde global ciro üzerinden düzenlenmektedir. Ayrıntılı bilgi için çalışmamızın 3.2. başlığına bakınız.
[334]. *Eßer'e ait kısım,* AUERNHAMMER, age, s. 1211. vd.

edileceği belirtilmektedir. Ancak buna rağmen kanunda değerlendirme kriterlerine ilişkin hiçbir düzenleme yer almamaktadır. Ek olarak idari para cezasının eylem temel alınarak mı yoksa ilgili kişi temel alınarak mı tayin edileceği de açık şekilde düzenlenmemektedir. Doktrinde bu hususların, hukuki belirlilik ilkesini zedeleyebileceği, tutarsız ve haksız uygulamalara sebep olabileceği söylenmektedir.[335]

3.2.1.2.a. Türkiye'de Şube veya İrtibat Bürosu Olarak Yapılanan Uluslararası Grup Şirket yahut Ekonomik İş Birliği Halindeki Teşebbüslerin Sorumluluğu

Bilindiği üzere *Binding Corporate Rules* düzenleyebilecek yapılar grup şirket yahut ekonomik iş birliği halindeki teşebbüsler olarak düzenlenmiştir. Bu yapıya dahil olmak için ise üye teşebbüsün hukuki bir kişiliği olması gerekmemektedir. Öyle ki *Binding Corporate Rules* düzenleyen yapı, üçüncü bir ülkede irtibat bürosu yahut bir ofis üzerinden faaliyet gösteriyor olabilir. *Binding Corporate Rules* yapısının Türkiye'deki üyesinin hukuki bir kişiliği olmaması hali Kişisel Verilerin Korunması Kanunu açısından incelenmelidir. Zira yukarıda belirtildiği üzere Kişisel Verilerin Korunması Kanunu, sorumluluğu değerlendirirken hukuki bir kişilik aramaktadır.

Tüzüğün benimsediği kuruluş ilkesi uyarınca[336] hukuki bir kişilik olmadan fiziki bir oluşum adı altında yürütülen faaliyetler Tüzük ile düzenlenmektedir. Bunun yanında *Google Spain* kararı ile Birlik dışında kurulu şirketlerin Birlik içindeki yapıları arasındaki ilişkiye dair ilkeler ortaya konmuştur. Öyle ki Birlik içindeki şirketin faaliyeti, Birlik dışındaki ana şirketten ayrı düşünülemiyorsa ana şirket de Tüzüğün uygulama alanında olacaktır. Kişisel Verilerin Korunması Kanunu ise buna benzer bir düzenleme içermemektedir. Dolayısıyla Türkiye'de herhangi bir hukuki kişiliği bulunmadan veri işleyen yabancı şirketlerin sorumlulukları bir soru işaretidir.

Somut olayda bu sorunu daha iyi kavrayabilmek açısından, irtibat bürolarının ve şubelerin durumunun incelenecektir. Türk Ticaret Kanunu ('TTK') md. 40/4'de düzenlendiği üzere, merkezleri Türkiye dışında bulunan ticari işletmelerin Türkiye'deki şubeleri yerli ticari işletmeler gibi tescil olunmaktadır. Bu şubeler için yerleşim yeri Türkiye'de bulunan tam yetkili bir ticari mümessil atanması öngörülmüştür. Türk kanunları açısından bir yerin şube sayılabilmesi için merkeze bağımlı olma, dış ilişkilerde

[335] KÜZECİ, age, s. 376.
[336] Çalışmamızın 1.2. başlığına bakınız.

bağımsızlık, yer ve yönetim ayrılığı gibi kriterlere de bakmak gerekmektedir.[337] Şubeler, iç işlerinde merkeze bağlı, kendi hukuki kişiliği bulunmayan, kâr ve zararı merkeze ait olan ve hak ve borçların merkez üstünde doğduğu yapılanmalardır. Ancak şubelerin dış işlerinde bağımsızlıkları gereğince merkezin yaptığı türden işlemleri (örneğin veri işleme) üçüncü kişilerle kendi başına yapabilmektedirler.[338]

Dolayısıyla her ne kadar hukuki kişiliği bulunmasa da veri işleme faaliyetinde bulunan ve ticari kazanç sağlayan şubelerin veri sorumlusu olarak değerlendirilmesi, kanunun amacına da uygun düşecektir. Bu anlamda Kişisel Verilerin Korunması Kanunu'nun gerçek veya tüzel kişi olarak belirlediği veri sorumlusu kavramı sorun yaratmaktadır. Dolayısıyla KVKK md. 18/2 uyarınca düzenlenen idari para cezalarının, yalnızca gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanması da bir sorundur.

Kurul, bu konuya dair verdiği ilgili kararında[339], veri sorumlusu kavramını isabetli biçimde, Birlik'teki hukukundaki kuruluş ilkesine[340] atıf yaparak incelemiştir. Kararda ilk olarak VERBİS'e kayıt yükümlülüğü için veri sorumlusu sıfatına haiz olunması; tüzel ya da gerçek kişiliğin bulunması gerektiği tespit edilmiştir. Kararın devamında ise, yurt dışında yerleşik tüzel kişilerin Türkiye'deki şubelerinin ayrı bir tüzel kişiliklerinin bulunmamasına rağmen, TTK md. 40'a göre şubelerin yerli ticari işletmeler gibi tescil oldukları tespit edilmiştir. Bunun yanında GVKT md. 4'e atıf yapılarak Birlik'te veri sorumlusu olma kriterleri arasında "tüzel kişi" olmanın şart olarak öngörülmediği göz önünde bulundurulmuştur. Bu nedenle kişisel veri işleme süreçleri bakımından merkezden bağımsız bir şekilde Türkiye'de veri sorumlusu kriterlerine uygun olarak hareket eden bu şubelerin veri sorumlusu sayılacağı değerlendirilmiştir. Bu karardan hareketle kanunun yenilenmesi durumunda, veri sorumlusu tanımına dair hukuki kişilik aranması halinin değiştirileceği de öngörülmektedir.

Dolayısıyla *Binding Corporate Rules'u* taahhüt etmiş grup şirketin Türkiye'deki üyesinin şube olarak düzenlenmesi hali, Kişisel Verilerin Korunması Kanunu'ndan doğacak yükümlülükleri bertaraf etmemektedir. Buna göre Türkiye'deki şube, diğer

---

[337] ARKAN Sabih, Ticari İşletme Hukuku, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayını, Ankara, Türkiye 2014, s. 37.
[338] Age, s. 38.
[339] 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 Kararı https://www.kvkk.gov.tr/Icerik/5545/2019-225 Erişim Tarihi: 24.05.2020.
[340] Ayrıntılı bilgi için çalışmamızın 1.2. başlığına bakınız.

bütün veri sorumluları gibi Kişisel Verilerin Korunması Kanunu'ndan doğan tüm yükümlülüklere uymakla mükelleftir.

İrtibat büroları için yapılan değerlendirmede ise, şubeler için öngörülenden farklı bir sonuca varılmıştır. 4875 sayılı Doğrudan Yabancı Yatırımlar Kanunu'nda ('DYYK') düzenlendiği üzere irtibat büroları, kendi hukuki kişilikleri olmayan, yurt dışındaki merkez ofis adına çalışan ve ticari faaliyet yürüten bürolardır.[341] Bu büroların çoğu, Türkiye'de yıllardır yerleşik bir yapılanmaya sahip olup birçok çalışana sahiptir. İşleyişleri gereği, pek çok gerçek kişinin verisini toplamakta, saklamakta ve yurt dışındaki merkez şirkete aktarmaktadır.

Bu anlamda veri sorumlusu olarak değerlendirilmelerinin Kişisel Verilerin Korunması Kanunu'nun amacına uygun düşeceği söylenebilecektir. Bu nedenle Türkiye'de hukuki bir kişiliği olmadan yapılanan bu büroların da yükümlülükleri bir soru işareti oluşturmaktadır. Nitekim bu nedenle Kurul ilgili kararında[342], Birlik hukukundaki kuruluş ilkesini de gözeterek, bu hususu incelemiştir.

Söz konusu kararda, Türkiye'de irtibat bürosu açılabilmesi için şirket tüzel kişiliklerinin yabancı ülke kanunlarına göre kurulması ve kurulan irtibat bürolarının Türkiye'de ticari faaliyette bulunmaması gerektiği söylenmiştir. Öyle ki irtibat bürolarının ticari faaliyet dışında haberleşme, fizibilite araştırması yapma, sosyal ve kültürel alanlarda bazı çalışmaları yürütme, şirketler arasında birleşme ve devirler için ön hazırlık yapma, tanıtım ve reklam, ülkedeki iş olanaklarının yakından takip etme ve bu konular hakkında merkez firmaya bilgi verme amacı doğrultusunda açılan bürolar oldukları belirlenmiştir. Bu nedenle irtibat bürolarının şube özellikleri bulunmadığı dikkate alınmış ve VERBİS'e kayıt olma yükümlülüğünün bulunmadığına karar verilmiştir.

Esasında, irtibat bürolarının Türk hukuku bakımından düzenlenme amacına bakıldığında, ticari risk almayı tercih etmeyen yabancı yatırımcılara, Türkiye pazarı ile ilgili gerekli bilgileri ilk elden edinmesi, gözlemleri yapması ve piyasaları test etmesi için elverişli bir çözüm sağladığı bilinmektedir. DYYK md. 3/h'ye göre yalnızca yabancı şirketlere, Türkiye'de ticarî faaliyette bulunmamak kaydıyla irtibat bürosu açma izni

[341] KARA Hacı (2019), 'Türk Hukukunda İrtibat Bürosu ve Özellikleri', İzmir Barosu Dergisi, C. 83, S. 3, s. 167-198.

[342] 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 Kararı https://www.kvkk.gov.tr/Icerik/5545/2019-225 Erişim Tarihi: 24.05.2020.

verilmektedir.[343] Bu anlamda Kurul'un bahsi geçen kararında, irtibat bürolarını VERBİS yükümlülüğünün dışında bırakması anlaşılabilmektedir.

Dolayısıyla *Binding Corporate Rules* dahilindeki grup şirket yahut ekonomik iş birliği halindeki teşebbüslerin Türkiye ayağı, şayet bir irtibat bürosu olarak yapılandıysa, söz konusu yapının VERBİS'e kayıt yükümlülüğü bulunmayacaktır. Bu karardan hareketle, Kurul aksi yönde karar verene kadar, irtibat bürolarının veri sorumlusu olarak değerlendirilmeyeceği ve Kişisel Verilerin Korunması Kanunu'nun öngördüğü diğer yükümlülüklere de uymasının gerekmeyeceğini söylemek mümkündür.

Ancak bu anlayışın Birlik hukukuna ters olduğunu belirtmek gerekir. Öyle ki irtibat büroları her ne kadar kendi adlarına ticari bir faaliyette bulunmasalar da kişisel verileri işlemektedirler. Ayrıca faaliyetleri dolayısıyla ana şirket ekonomik kazanç sağlamaktadır. Öyle ki irtibat bürolarının faaliyetlerinin ana şirketten ayrı değerlendirilemeyeceğini söylemek mümkündür. Dolayısıyla Divan'ın *Google Spain* kararıyla getirdiği ilkelere göre,[344] irtibat bürolarının da Kişisel Verilerin Korunması Kanunu kapsamına alınması isabetli olabilirdi.

3.2.1.3. Cezai Sorumluluk

KVKK md. 17'nin ortaya koyduğu üzere kişisel verilere ilişkin suçlar bakımından Türk Ceza Kanunu ('TCK') md. 135 ile 140 hükümleri uygulanmaktadır. Bu anlamda, Ceza Kanunu'nun dokuzuncu bölümünde yer alan, özel hayata ve hayatın gizliliğine karşı suçlar değerlendirilecektir.

İlk olarak belirtilmelidir ki TCK md. 135 uyarınca hukuka aykırı olarak kişisel verileri kaydeden kimse hakkında bir yıldan üç yıla kadar hapis cezası uygulanacağı öngörülmüştür. Burada KVKK md. 5'te düzenlendiği şekilde kişisel verilerin işlenme şartları, hukuka uygunluk sebebi oluşturacaktır. Dolayısıyla Türk şirketin taahhüt edeceği *Binding Corporate Rules'da* öngörülen hukuka uygun veri işleme sebeplerinin, KVKK md. 5'e uygun olması önemlidir.

TCK md. 136 ise, kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi hakkında iki yıldan dört yıla kadar hapis cezası düzenlemiştir.

[343] KARA, age, s. 167-198.
[344] Kararın ayrıntılı incelemesi için çalışmamızın 1.2.1. başlığına bakınız. Söz konusu değerlendirme Birlik hukukunda Direktif göze alınarak yapılmıştır. Ancak ortaya konulan prensiplerden Kişisel Verilerin Korunması Kanunu kapsamında da yararlanılabilir.

Hüküm kapsamında kişisel verilerin aktarılmasından bahsedildiğinden, KVKK md. 8 ve md. 9 hükümlerine uyulması gerekmektedir. Aksi halde, Kişisel Verilerin Korunması Kanunu yükümlülüğüne aykırılığın yanında cezai sorumluluk da doğabilecektir. Bu nedenle taahhüt edilecek *Binding Corporate Rules'un* yalnızca Birlik hukukuna göre uygun güvenlik önlemi teşkil ettiğinin tekrar altını çizmek gerekir. Öyle ki Türkiye'den Birlik'teki üyelere aktarılacak verilere ilişkin KVKK md. 9 yükümlülüklerine uyulması gerekecektir. Söz konusu husus, çalışmamızın yurtdışı veri aktarımına ilişkin yükümlülükler kısmında ayrıntısıyla incelendiği için, bu noktada ilgili kısma[345] atıf yapmakla yetinilecektir.

KVKK md. 17/2, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini düzenleyen md. 7 hükmüne aykırı davranılması halinde, TCK md. 138 uyarınca bir yıldan iki yıla kadar hapis cezası verileceğini düzenlemiştir. TCK md. 138'in öngördüğü şekilde, kanunda belirlenen sürelerin geçmiş olmasına karşın verilerin yok edilmemesi halini düzenlemektedir. Bu anlamda Türk hukukunda, kanuni yükümlülükler dolayısıyla öngörülen muhtelif saklama süreleri değerlendirilmelidir. [346]

Nitekim Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmeliğin 5. maddesi uyarınca veri sorumluları, kişisel verileri silme ve imha politikası hazırlamakla yükümlüdürler. Aynı yönetmeliğin 6. maddesi ise, hazırlanacak silme ve imha politikası içerisinde hangi tip verilerin ne kadar süreyle saklanacağının belirtilmesini öngörmüştür.[347] Dolayısıyla *Binding Corporate Rules'u* taahhüt eden Türk şirketinin, Türk kanunları uyarınca öngörülen saklama sürelerini aşmamaya dikkat etmesi gerekmektedir. Bu anlamda *Binding Corporate Rules'da* öngörülen saklama süreleri karşılaştırılmalı ve iç hukuka aykırılık teşkil etmemesi sağlanmalıdır. Hazırlanacak kişisel verileri silme ve imha politikasında Türk hukukuna uygun saklama sürelerinin belirlenmesi gerekmektedir.

---

[345] Yurtdışı veri aktarımına ilişkin KVKK yükümlülüklerine dair ayrıntılı bilgi için çalışmanın 3.1.3. başlığına bakınız.

[346] Örneğin işçi verilerine ilişkin özlük dosyalarının, iş ilişkisinin bitiminden sonra on yıl için saklanması öngörülmüştür. Bu durumda BCR'da bu sürenin geçilmemesine dikkat edilmelidir.

[347] Kurul'un kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin rehberi için bkz. https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf Erişim Tarihi: 31.05.2020.

Son olarak belirtilmelidir ki TCK md. 140 hükmü, yukarıda tanımlanan suçların tüzel kişilerce işlenmesi halinde, bunlara özgü güvenlik tedbirlerine hükmolunacağını belirtmektedir.

3.2.2. Özel Hukuktan Doğabilecek Diğer Sorumluluk Halleri

Çalışmamızda belirtildiği üzere kişisel verilerin korunmasına dair hükümler, Türk hukukunda Kişisel Verilerin Korunması Kanunu yanında sair mevzuatta da yer almaktadır. Bu anlamda TMK md. 23, md. 24 ve md. 25 hükümleri ile Türk Borçlar Kanunu ('TBK') md. 49 ve devamı hükümler ile md. 58, özel hukuk bağlamında en çok gündeme gelebilecek maddelerdir. Öyle ki, KVKK md. 14/3 ve md. 11/1/ğ atfı ile genel hükümlere göre uygulanacak tazminat konusu, çalışmamızın bir önceki başlığında incelenmiştir.

Bu başlık altında, iş hukuku kapsamında yapılacak genel bir değerlendirme, kişisel verilerin korunması anlamında gündeme gelebilecek diğer bir önemli hususdur. Zira iş hukukundan doğabilecek sorumluluklar, uluslararası bir *Binding Corporate Rules'u* taahhüt eden Türk işverenini ilgilendirmektedir.

Bahsedilmesi gereken ilk husus, henüz iş ilişkisi kurulmadan iş başvurusunda bulunan kişiden istenecek kişisel verilerdir. Elbette ki işveren, iş başvurusunda bulunan kişinin işe uygunluğunu değerlendirmek adına bu kişiden, isim, soy isim, eğitim bilgileri, adres gibi bir takım kişisel veriler istemektedir. Ancak burada, işverenin başvurulara ilişkin bilgileri gizli tutması gerekmektedir; bu bilgiler üçüncü kişilerle paylaşılmamalıdır.[348] Nitekim Kurul bu konuda verdiği bir kararında, hukuki bir sebebe dayanmaksızın iş başvuru bilgilerinin üçüncü kişilerle paylaşılmasını Kişisel Verilerin Korunması Kanunu'na aykırı bularak idari para cezasına hükmetmiştir.[349]

Binding Corporate Rules düzenleyen çok uluslu şirket yapılarında işe alımların, Birlik'te yerleşik bir tek elden yönetilmesi, sık karşılaşılan bir durumdur. Bu nedenle *Binding Corporate Rules'u* taahhüt eden Türk şirketinin, bu hususa dikkat etmesi gerekmektedir. Şayet Türkiye'deki işe alımlar başka ülkelerdeki insan kaynakları

[348] KÜZECİ, age, s. 390.
[349] İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi Erişim Tarihi: 04.06.2020.

oluşumlarınca yürütülmekteyse, iş başvurularında alınan kişisel veriler hukuka uygun şekilde işlenmeli ve aktarılmalıdır.

İş ilişkisi kurulduktan sonra ise, işçinin sadakat yükümlülüğünün yanında, işverenin de işçiyi koruma borcu doğmaktadır.[350] İş Kanunu ('İK') md. 75 gereği işveren, çalıştırdığı her işçi için bir özlük dosyası düzenlemektedir. Özlük dosyası içerisinde işverenin kanuni yükümlülükleri dolayısıyla düzenlemek ve saklamak zorunda olduğu her türlü belge ve kayıtlar yer almaktadır. Aynı zamanda bu belge ve kayıtların, istendiği zaman yetkili memur ve mercilere sunulmak zorunda olduğu da düzenlenmiştir. Dolayısıyla taahhüt edilecek *Binding Corporate Rules'da*, işçi verilerinin istendiği takdirde yetkili mercilere gösterilmesi ve/veya aktarılmasına engel bir hususun olmamasına dikkat edilmelidir.

Her ne kadar İK md. 75 yalnız özlük dosyasına ilişkin bilgileri düzenlese de söz konusu hüküm TBK md. 419 kapsamında değerlendirmelidir. Eski borçlar kanununda mevcut bulunmayan TBK md. 419, tasarıda işçinin korunması amacını taşımaktadır. Teknolojik gelişmeler sonucu günlük yaşantının bir sonucu haline gelen ve bilgisayar ortamında saklanabilen verilerin kullanılması konusunda işçinin korunması amacıyla, bazı sınırlamalar öngörmüştür. Bu kapsamda işverenin, işçiye dair kişisel verileri ancak işe yatkınlığıyla ilgili biçimde veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabileceğini düzenlenmiştir.[351]

Kişisel verilerle ilişkisi sebebiyle gündeme gelebilecek bir husus da Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun ('ETK') öngördüğü yükümlülükler ve istisnalardır. ETK md. 6 uyarınca ilgili kişiye gönderilecek ticari ileti, ilgili kişinin onayına bağlanmıştır. Şekline dair herhangi bir yükümlülüğün öngörülmediği bu onaya dair aynı madde iki adet istisna tanımaktadır. Öyle ki, alıcının kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini vermesi halinde, temin edilen mal ve hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay gerekmemektedir.

Kişisel verilerin işlenmesinde böyle bir amaç değişikliği, Tüzük dahilindeki amaçla sınırlı veri işleme ilkesiyle bağdaşmayabilir.[352] Dolayısıyla, Türk şirketin taahhüt

[350] KÜZECİ, age, s. 393.
[351] UYGUR Turgut, 6098 Sayılı Türk Borçlar Kanunu Şerhi, 1. Baskı, Seçkin Yayıncılık, İstanbul, Türkiye 2012, s. 2024.
[352] Amaçla sınırlılık ilkesine dair ayrıntılı bilgi için çalışmanın 1.1.2. başlığına bakınız.

ettiği *Binding Corporate Rules'da* korunan kişisel veriler, Birlik'ten aktarılanlarla sınırlanmadıysa,[353] şirketin söz konusu istisna hükmüne dayanmaması tavsiye olunmaktadır.

ETK md. 6/2 ise, ticari elektronik ileti için öngörülen onaya dair ikinci istisna hükmünü düzenlemektedir. Buna göre, esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilecektir. Yukarıdaki açıklamalara paralel şekilde, söz konusu istisna hükmü Tüzük kurallarıyla bağdaşmamaktadır. Dolayısıyla Türk şirketin taahhüt ettiği *Binding Corporate Rules'da* korunan kişisel veriler Birlik'ten aktarılanlarla sınırlanmadıysa, şirketin yine bu istisna hükmüne dayanmaması tavsiye olunmaktadır.

Bu kapsamda bahsedilmesi gereken son husus, ETK md. 10/1/b düzenlemesine göre kişisel verilerin, ilgili kişinin onayı olmaksızın üçüncü kişilere iletilemeyeceğidir. Şayet taahhüt edilmiş *Binding Corporate Rules'da* ilgili kişilere elektronik ileti gönderilmesi ve bu tercihe dair verilerin toplanarak aktarılması öngörülmüşse, ETK md. 10/1/b hükmü dikkate alınmalıdır. Öyle ki Türkiye'de bu tercihin ilgili kişilerden Kişisel Verilerin Korunması Kanunu'na uygun şekilde alınacak onaya dahil edilmesi gerekmektedir.

Bu başlık altında incelenecek son husus, Türk Ticaret Kanunu ('TTK') md. 24'de düzenlenen ticaret sicili olacaktır. Aleni tutulan ticaret sicil kayıtlarının, elektronik ortamda tutulmasına ilişkin usul ve esaslar, TTK md. 26 uyarınca çıkartılacak bir yönetmelikle belirlenmektedir. TTK md. 27/1 uyarınca ticaret siciline tescil kural olarak istem üzerine yapılmakta olsa da tescile tâbi işlemler söz konusudur. Örneğin, müdürler/yönetim kuruluna atanan kişinin imza yetkisini gösterir sirkülerin çıkarılması, atama kararının ticaret sicilde tesciline bağlıdır.

TTK md. 24/5 hükmü, ticaret sicili kayıt işlemlerinin elektronik ortamda yapılması için toplanması ve işlenmesi gerekli olan kişisel verilerin, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuata uygun bir şekilde korunacağını öngörmektedir. Ancak bu hükme rağmen Türkiye Ticaret Sicil Gazetesinde yayınlanan kararlarda, gerçek kişilere ait pek çok kişisel verinin (isim soy isim bilgilerinin yanında örneğin kimlik numarası, yabancı kişiler söz konusuysa potansiyel

[353] Şirketler, düzenledikleri BCR'ın kapsamına girecek kişisel verileri sınırlamakta özgürdürler. Bu hususa dair ayrıntılı bilgi için çalışmanın 2.3.1.2. başlığına bakınız.

kimlik numarası, pasaport numarası gibi bilgiler) hâlihazırda sansürlenmeden veya herhangi bir tedbir alınmadan yayınlandığı görülmektedir.

Dolayısıyla *Binding Corporate Rules'u* taahhüt eden Türk şirketinin yönetim/müdürler kuruluna Birlik vatandaşı bir gerçek kişinin atanması halinde, bu kişiye ait verilerin de aleni bir şekilde yayınlanması olasıdır. Bu hususun özellikle gerçek kişiye ve *Binding Corporate Rules* düzenleyen grup şirketlerin Birlik'te atadığı ilgili sorumluya bildirilmesi ve ilgili kişiden Tüzüğe uygun biçimde rıza alınması gerekmektedir.

3.3. KİŞİSEL VERİLERİN KORUNMASI KANUNU UYARINCA DÜZENLENECEK BAĞLAYICI ŞİRKET KURALLARI

Kurum 10.04.2020 tarihinde yaptığı bir duyuru ile Türk hukuku içinde geçerli Bağlayıcı Şirket Kuralları'nı düzenlemiştir. Bu kurallar Türkiye'de yerleşik veri sorumlusu tarafından, yeterli veri koruması bulunmayan ülkelerdeki veri sorumlusu veya işleyenlere yapılacak aktarımlarda kullanılan taahhütnamelere alternatif olarak geliştirilmiştir.[354] Tüzük'te öngörülen veri işleyen ve veri sorumlusu *Binding Corporate Rules'u* ayrımı, Bağlayıcı Şirket Kuralları için mevcut değildir. Kişisel Verilerin Korunması Kanunu kapsamında Bağlayıcı Şirket Kuralları ancak veri sorumlularının kullanabileceği bir yöntem olarak düzenlenmiştir.

Duyurunun ekinde yer alan yardımcı doküman içerisinde Bağlayıcı Şirket Kuralları "Bir şirketler topluluğuna bağlı olarak Türkiye'de yerleşik bir veri sorumlusu tarafından, bu 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 tanımlanmaktadır.

Bahsi geçen duyuruda taahhütnamelerin, çok uluslu şirketler arasındaki veri aktarımlarında uygulamada yetersiz kalabildikleri belirtilmektedir. Dolayısıyla Bağlayıcı Şirket Kuralları'nın pratikteki bu açığı kapatmaya yönelik düzenlendikleri söylenmektedir. Yukarıdaki açıklamadan anlaşıldığı üzere Bağlayıcı Şirket Kuralları çok

[354] Bağlayıcı Şirket Kuralları Hakkında Duyuru https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU Erişim Tarihi: 22.07.2020.

uluslu grup şirketler tarafından kişisel veriler yurt dışına aktarılırken kullanılmaktadır. Bu kurallar, Kişisel Verilerin Korunması Kanunu'nun aradığı yeterli korumanın taahhüt edilmesini sağlamaktadır. Elbette ki bu başlık altında inceleneceği üzere Bağlayıcı Şirket Kuralları, pek çok avantaja sahiptir.

Kişisel Verilerin Korunması Kanunu'nun gerekçesinde belirtildiği üzere, Kanun'un düzenlenme amaçlarından biri Birlik hukukuna uyum sağlamaktır. Buna rağmen Kanun'un model alındığı mülga 95/46 sayılı Direktifle, Kişisel Verilerin Korunması Kanunu arasında uyumsuzluklar mevcuttur.[355] Eklemek gerekir ki, Tüzüğün yürürlüğe girmesiyle Birlik hukuku ve hatta bütün dünya, veri koruması alanında yeni bir düzenlemeyle tanışmıştır. Nitekim Kurul'un da pek çok kararında görüldüğü üzere isabetli şekilde, Tüzük'teki düzenlemeler dikkate alınmaktadır. Bu anlamda Kişisel Verilerin Korunması Kanunu'ndaki veri koruması esasları, Tüzük seviyeyesine çıkartılmaya çalışılmaktadır.

Birlik'teki veri koruması hukukunun Türkiye'ye etkisi bakımından açıktır ki, Tüzük ile önemli ölçüde bir uyum gerekmektedir. Bu uyum öncelikle, kişisel verilerin korunması alanını bütüncül biçimde düzenleyen hukukun öngördüğü korumanın tam anlamıyla uygulanabilmesini sağlayacaktır.[356] Aynı zamanda ekonomik açıdan yabancı sermayenin ülkeye çekilmesi hususunda da şüphesiz yardımcı olacaktır.[357] Bağlayıcı Şirket Kuralları'nın Tüzük ile bu uyumun yakalanması adına Türk hukukuna sağlayabileceği pek çok fayda söz konusudur.

Ancak bu noktada Bağlayıcı Şirket Kuralları'na aykırılık halinde öngörülecek yaptırımlara ilişkin soruların bulunduğunu belirtmek gerekir. Öyle ki Kişisel Verilerin Korunması Kanunu altında öngörülen idari para cezalarının hangi hallerde uygulanacakları belirlenmiştir.[358] Bu noktada bir hukuka aykırılığın meydana gelmediği ve salt Bağlayıcı Şirket Kuralları'nda verilen taahhütlere bir aykırılığın söz konusu olduğu hallerde, şirketler hakkında ne gibi bir yaptırım uygulanacağı açık değildir. Öyle ki Kişisel Verilerin Korunması Kanunu altında böyle bir ihtimal yaptırıma bağlanmamıştır. Dolayısıyla Kurum duyurusunda bu hususun aydınlatılması yararlı

[355] KAMA IŞIK Sezen, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış: 2016/679 Sayılı GVKT ile 6698 Sayılı KVKK'nın Detaylı Analiz ve Karşılaştırması, 1. Basım, On İki Levha Yayıncılık, İstanbul, Türkiye 2020, s. 357.
[356] Age, s. 358.
[357] Age.
[358] Bkz., çalışmanın 3.2.1.2. başlığı.

olurdu. Bu soru, yeni uygulanmaya başlayan Bağlayıcı Şirket Kuralları hakkında verilecek kararlar ile açıklığa kavuşturulmalıdır.

Aşağıdaki başlıklar altında Bağlayıcı Şirket Kuralları'nın Türk veri koruması hukuku için sağlayabileceği amaç ve avantajlar belirlenecektir. Bunun yanında Bağlayıcı Şirket Kuralları'nın hangi alanlarda kullanılabileceği ortaya konulacaktır. Ardından Kurum'un duyurusunun[359] ekinde yer alan yardımcı dokümandan faydalanılarak, Bağlayıcı Şirket Kuralları içinde taahhüt edilmesi gereken asgari unsurlar değerlendirilecektir. Son olarak ise yine Kurum'un hazırladığı doküman aracılığıyla, Bağlayıcı Şirket Kuralları için başvuru usul ve esasları belirlenecektir.

3.3.1. Amaç, Avantaj ve Kullanım Alanları

Bu kurallar ilk bakışta global şirket yapısı içerisindeki veri aktarımının hukuka uygun düzenlenmesini sağlamaktadır. Nitekim Kurum Bağlayıcı Şirket Kuralları'nı 'yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri koruma politikaları' olarak tanımlamaktadır.[360]

Bunun haricinde Bağlayıcı Şirket Kuralları'nın avantajları belirlenirken dikkate alınacak ilk husus, globalleşme gereğince ihtiyaç duyulan uluslararası veri koruma standartlarıdır. Global bir şirket yapısı içinde, verilerinin işlendiği yere bakılmaksızın tüm üyelerde aynı standardın benimsenmesi, bahsi geçen hedef için önemli bir adımdır. Nitekim, global düzeyde belirlenecek olası veri koruması standartlarında *Binding Corporate Rules* benzeri uluslararası etkisi olan taahhütlerin dikkate alınacağı söylenmektedir. Bu taahhütlerin uluslararası veri koruma standartları için önemi doktrinde ortaya konulmuştur.[361]

Çalışmamızda belirtildiği üzere Türkiye'de benimsenen veri korumasının Birlik standartlarına yaklaştırılması için Bağlayıcı Şirket Kuralları'nın önemi açıktır. Öyle ki Bağlayıcı Şirket Kuralları, Tüzüğün benimsediği risk odaklı bakış açısını, Türkiye'de şirket özelinde düzenlemektedir. Bu bakış açısı, hukuka aykırılığı henüz meydana gelmeden engellemeyi hedeflemektedir. Kişisel verilere dair en geniş ve doğru bilgi veri

[359] Bkz., dn. 354.
[360] Bkz., dn. 354.
[361] MOEREL 2012, age, s. 27.

sorumlusunda/işleyende bulunmaktadır. Dolayısıyla yerinde risk değerlendirmesi yapılarak uygun güvenlik önlemlerinin de yerinde belirlenmesi öngörülmektedir.

Risk odaklı bakış açısının bir görünümü olarak, zorunlu veri koruma etki değerlendirmelerinin yapılması örnek verilebilir. Bu değerlendirmeler Kişisel Verilerin Korunması Kanunu'nda yer almasa da Kanun'un amaçlarına hizmet etmektedir. Risk odaklı bakış açısının bir başka görünümü de hukuka aykırılığın meydana gelmesini önlemek adına bütün önlemlerin alınmasını içeren verilerin tasarım itibariyle ve varsayılan olarak korunması ilkesidir. Bu iki husus da hazırlanacak Bağlayıcı Şirket Kuralları ile bağlayıcı biçimde bütün grup şirket bünyesinde taahhüt edilebilecektir. Böylece Kanun'un sağladığı koruma güçlenirken, Bağlayıcı Şirket Kuralları'nı düzenleyen Türk şirketinin Birlik hukukuna uyumu artacaktır. Elbette şirketler açısından bu hususun ekonomik bir getirisi de olacaktır.

Bağlayıcı Şirket Kuralları'nın iç ve dış bağlayıcılığına dair verilen taahhütler kapsamında, şirketin veri işleme politikasının gerçekte uygulanabilirliği sağlanmalıdır. Verilen taahhütlerin yerine getirilmesi için öngörülen tüm önlemler belirtilmelidir. Bağlayıcı Şirket Kuralları'nda grup şirket üyelerinin iletişim bilgileri, tâbi oldukları veri koruma mevzuatları, üye şirketlerin her birinde yer alan önlemler, zarar gören ilgili kişinin talebini yöneltebilmesi için benimsenen yollar gibi pek çok bilginin yer alması ve değişiklik halinde güncellenmesi gerekmektedir. Dolayısıyla düzenlenen Bağlayıcı Şirket Kuralları, grup şirketin veri işleme sürecini global ölçekte şeffaflaştırmayı sağlamaktadır.

Nitekim Kurum'un duyuru ekinde yer alan Bağlayıcı Şirket Kuralları başvuru formunda[362], başvuruda bulunan şirkete yöneltilecek sorulardan biri hesap verilebilirliğe ilişkindir. Hesap verilebilirliğe dair taahhüdün yerine getirildiğini tespit edebilmek adına, şirket özelinde pek çok soru yöneltilmektedir. Bağlayıcı Şirket Kuralları aynı zamanda, Kişisel Verilerin Korunması Kanunu uyarınca çıkartılan yönetmelik ve tebliğlerle belirlenen ve Kurul Kararlarıyla şekillenen esasların öngördüğü tüm yükümlülüklerin, grup şirket bünyesinde tam ve açık bir şekilde taahhüt edilmesini sağlamaktadır. Bu anlamda Bağlayıcı Şirket Kuralları'nın hesap verilebilirlik açısından taşıdıkları önem ortadadır.

Önemli avantajlardan biri de Bağlayıcı Şirket Kuralları'nın ispat aracı olarak kullanılabilmesidir. Bilindiği üzere bu kurallar, kanuni yükümlülükleri karşılayan geniş

[362] Bkz., dn. 354.

taahhütler içermekte ve şeffaflık sağlamaktadır. Dolayısıyla gerek genel hükümlere göre tazminat sorumluluklarında, gerekse KVKK md. 18 uyarınca öngörülecek idari para cezalarında özen borcuna riayet edildiğine ilişkin ispat aracı olarak kullanılabileceklerdir.

Uygulamada veri koruma projeleri hazırlanırken değerlendirilebilecek bir ihtimal, merkezi Türkiye'de olmayan uluslararası bir grup şirketin düzenlediği *Binding Corporate Rules'un* Türkçeleştirilerek, Bağlayıcı Şirket Kuralı başvurusu yapılmasıdır. Elbette bu durumda Türkçe çevirisi yapılan metnin, Kişisel Verilerin Korunması Kanunu'nun aradığı bütün taahhütleri de içerdiğinden emin olunmalıdır. Kurallar üzerinde gerekli ekleme ve değiştirme yapıldıktan sonra, söz konusu metin ile Bağlayıcı Şirket Kuralı başvurusu yapılabilecektir. Bu ihtimalin pratikte sağlayabileceği kolaylık açıktır. Zira metnin Bağlayıcı Şirket Kuralları olarak onaylanması halinde, Türkiye'den grup şirket içerisinde yapılacak veri aktarımları da hukuka uygun hale gelecektir[363].

Son olarak belirtilmelidir ki Türkiye merkezli çok uluslu bir grup şirketin Bağlayıcı Şirket Kuralları düzenleyerek, Birlik'te sertifikalanması gündeme gelebilecektir. Belirtildiği üzere Bağlayıcı Şirket Kuralları'nda Kurum'un aradığı şekliyle taahhüt edilmesi gereken hususlar, niteliği itibariyle şirketi Tüzüğün aradığı standartlara yaklaştırmaktadır. Böyle bir durumda şirketlerin Birlik hukukuna uygun şekilde Birlik'te sertifikalanmalarının ekonomik ve ticari açıdan büyük bir avantaj sağlayacağı söylenebilir.[364]

3.3.2. Bağlayıcı Şirket Kuralları İçeriğinde Taahhüt Edilecek Hususlar

Kurum duyurusu ekindeki yardımcı dokümanda, Bağlayıcı Şirket Kuralları'nın onaylanması için sekiz adet uygunluk kriteri belirlenmiştir. Bu kriterler 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, yardımcı bilgi ve belgelerdir. Yayınlanan rehberde bu kriterlerin yerine getirilmesi için özel yöntemler de öngörülmüştür. Söz konusu

[363] Çalışmamızda *Binding Corporate Rules'un* yalnızca Birlik hukukuna göre bir uygun güvenlik önlemi oluşturduğundan bahsetmiştik. Bu nedenle Türkiye'den grup şirketin diğer ülkelerdeki üyelerine yapılacak aktarımlarında KVKK md. 9 yükümlülüklerine uyulması gerekmektedir.

[364] Birlik hukuku uyarınca benimsenen sertifika sisteminin ayrıntılı incelemesi için çalışmamızın 1.3.3.4. başlığına bakınız.

yöntemler, Bağlayıcı Şirket Kuralları içerisinde taahhüt edilmesi gereken hususlara işaret etmektedir ve aşağıda incelenecekleridir.

3.3.2.1. Bağlayıcılık Unsuru

Bağlayıcı Şirket Kuralları'nın geçerli olması için iç ve dış bağlayıcılığının bulunması gerekmektedir. Tüzük'ten tanıdığımız iç ve dış bağlayıcılık, Kişisel Verilerin Korunması Kanunu kapsamında da paralel bir düzenleme içermektedir.[365] İç bağlayıcılık, grup şirketin tüm üyeleri ve çalışanları için hukuken geçerli ve ispatlanabilir biçimde bağlayıcı olarak düzenlenmesi anlamına gelmektedir. Bağlayıcı Şirket Kuralları başvurularında bu kriterin hangi evrak ve yöntemle sağlandığına ilişkin bilgi talep edilmektedir. Dış bağlayıcılık unsuru ise, kuralların ilgili kişi nezdinde bağlayıcılığını ifade etmektedir. Öyle ki, ilgili kişinin haklarını kullanabilmesi ve Bağlayıcı Şirket Kuralları'nın ihlal edildiğine dair iddiaları için şikâyet imkânı tanınmalıdır.

Bağlayıcı Şirket Kuralları, Kişisel Verilerin Korunması Kanunu'nun ilgili kişiye tanıdığı bütün haklara ek olarak başkaca taahhütler de içermelidir. Şöyle ki verilerin yurtdışında yerleşik grup şirket üyelerince işlenmesinden doğan birtakım hususlar da taahhüt edilmelidir. Önemli bir nokta da grup şirket üyeleri haricinde, grup şirket verileri için veri işleme faaliyeti yürüten üçüncü kişilerle imzalanacak sözleşmelere ilişkindir. Üçüncü kişilerle imzalanacak bu hizmet sözleşmeleri, Bağlayıcı Şirket Kuralları'nda öngörülen taahhütleri içermek durumundadır.

Bağlayıcılığa dair bir başka önemli husus, yabancı ülkedeki grup şirket üyelerinin tâbi oldukları yerel mevzuatlarda yer alan veri koruması hükümlerine ilişkindir. Yerel mevzuatta Bağlayıcı Şirket Kuralları'nda verilen taahhütlere aykırı düşen hükümlerin belirlenmesi ve Kurum'a bildirilmesi gerekmektedir. Bunun yanında, Bağlayıcı Şirket Kuralları'nın uygulanması bakımından geçerli mevzuatın Kişisel Verilerin Korunması Kanunu olduğu açıkça yazılmalı ve Kurul yetkili otorite olarak belirlenmelidir.

Bağlayıcı Şirket Kuralları uygulamasında, üçüncü ülkelerin iç hukukundan doğabilecek, devlet otoritelerinin denetim yetkisine dair bir istisna düzenlenmiştir. Söz konusu istisna 'her halükârda demokratik bir devlet düzenlemesinin gereklerini aşmayacak şekilde' ifadesiyle, muğlak bir biçimde düzenlenmiştir. Bu husus şüphesiz ki,

[365] BCR'ın iç ve dış bağlayıcılığına dair çalışmanın 2.3.1.3. başlığına bakınız.

özellikle *Schrems II* kararıyla getirilen kıstaslardan sonra, Birlik standartları için fazla belirsiz kalacaktır.[366]

Bağlayıcılık başlığı altında incelenecek son husus ise tazminat ödemelerine ilişkindir. Grup şirketin Türkiye'deki merkezi veya Türkiye'de yerleşik yetkilendirilmiş üyesi yahut veriyi aktaran veri sorumlusu, Bağlayıcı Şirket Kuralları'na aykırılık dolayısıyla gündeme gelebilecek tazminat ödemelerini ve ihlalin giderilmesi yükümlülüklerini kabul etmelidir. Grup şirketin politikaları nedeniyle, yükümlülüğün tek bir üyece üstlenilmesi mümkün değil ise, yurtdışındaki üye şirket nezdinde meydana gelecek ihlallerde üye şirketin bireysel sorumluluğu düzenlenebilir. Bu ihtimalin özellikle merkezi yurtdışında olan grup şirketler için cazip olduğu görülmektedir.

3.3.2.2. Etkili Uygulama

Bağlayıcı Şirket Kuralları'nın geçerliliği için etkili bir biçimde uygulanmaları sağlanmalıdır. Kurum, hazırladığı yardımcı dokümanda[367] etkili uygulama sağlanması için kullanılabilecek yöntemler öngörmüştür. Buna göre, veri sorumlusu özellikle kişisel verilerle temas halinde olan çalışanları için, eğitim ve farkındalık çalışmaları yürütülmelidir. Bunun yanında, talep halinde Kurum'a sunulmak üzere yürütülen çalışmaların kayıtları tutulmalıdır.

Etkili uygulama için elbette ki ilgili kişilerin haklarını etkin bir biçimde kullanabilmeleri son derece önem arz etmektedir. Dolayısıyla Bağlayıcı Şirket Kuralları içerisinde etkin bir şikâyet yöntemi öngörülmelidir. Şikâyet süreci açık ve anlaşılır biçimde açıklanmalı ve şikâyetleri değerlendirme süreleri ile yöntemleri belirtilmelidir. Söz konusu başvuru sistemi kurulurken elbette, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[368] ile öngörülen yükümlülükler yerine getirilmeli ve tebliğin de öngördüğü şekilde bir başvuru sistemi oluşturulmalıdır. Bu noktada Birlik hukukuna paralel bir yorum yapacak olursak etkin uygulama kriteri, Türk vatandaşları açısından Kişisel Verilerin Korunması Kanunu'ndaki hak ve imkânların, verilerin aktarıldığı üçüncü ülkelerde de benzer kolaylıkta kullanılabilmesidir.

---

[366] Bu konuda ayrıntılı bilgi için çalışmamızın 1.3.2.2. başlığına bakınız.
[367] Bkz., dn. 354.
[368] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm Erişim Tarihi: 04.06.2020.

Kurum'un etkili uygulama açısından aradığı bir başka husus ise, Bağlayıcı Şirket Kuralları içerisinde uyum ve denetim sürecinin öngörülmesidir. Grup şirket bünyesinde Bağlayıcı Şirket Kuralları'na uyulduğuna ilişkin denetimin, kimin tarafından yürütüleceği belirlenmelidir. Bunun yanında denetimin hangi aralıklarla ve ne yöntemler kullanılarak gerçekleştirileceği de öngörülmelidir. Bu anlamda Bağlayıcı Şirket Kuralları içerisinde görevli bir personel de atanmalıdır.

3.3.2.3. Kurum ile Koordinasyon

Bağlayıcı Şirket Kuralları içerisinde Kurum ile koordinasyonun nasıl sağlanacağı belirtilmelidir. Buna ek olarak grup şirketin, herhangi bir konuda Kurum'un tavsiyelerine uymayı kabul ettiğine dair bir yükümlülük bulunmalıdır. İçeriği tam olarak belirlenemeyen bu yükümlülük, özellikle yabancı merkezli grup şirketler için sorun oluşturabilecektir. Nitekim *Schrems II* kararından sonra Divan, Birlik dışına veri aktarımlarında üçüncü ülkede öngörülemeyen Devlet dahlini en aza indirmeye çalışmaktadır.[369]

3.3.2.4. Kişisel Verilerin İşlenmesi ve Aktarılması

Kurum, Bağlayıcı Şirket Kuralları kapsamında yapılacak veri işleme faaliyetlerinin Kişisel Verilerin Korunması Kanunu'na uygunluğunu sağlamak için bazı taahhütler aramaktadır. İlk olarak benimsenen kuralların kapsamı ve aktarımların genel bir tanımı yapılmalıdır. Kişisel verilerin işlenmesine dair kanuni yükümlülükler taahhüt edilirken, Kurum'un aydınlatma yükümlülüğüne ilişkin tebliğinden yararlanılabilecektir.[370] Kişisel verilerin niteliği, kategorileri, veri konusu kişi grubu belirlenmelidir.

Bunun yanında, grup şirket içerisinde Bağlayıcı Şirket Kuralları'na dayanarak yapılacak aktarım süreçleri açıklanmalıdır. Aktarımların hangi yöntemle, ne sürelerde yapılacağı, kişisel verilerin grup şirket içerisindeki dağılımı gibi bilgilere yer verilmelidir. Bağlayıcı Şirket Kuralları ile grup şirket içerisinde yapılan kişisel veri aktarımlarının

[369] Ayrıntılı bilgi için çalışmamızın 1.3.2.2. başlığına bakınız.
[370] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ https://kvkk.gov.tr/Icerik/5443/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESINDE-UYULACAK-USUL-VE-ESASLAR-HAKKINDA-TEBLIG
Erişim Tarihi: 04.06.2020.

üçüncü kişilere ileri aktarımı *(ing. onward transfer)* da düzenlenmelidir. Tercihen, ileri aktarımlarda da Bağlayıcı Şirket Kuralları'nın geçerli olacağı taahhüt edilmelidir. Nitekim aşağıda inceleneceği üzere, Bağlayıcı Şirket Kuralları'nın veri güvenliğine ilişkin kısımda verilecek taahhütlerin, ileri aktarımlarda da geçerliliği aranmaktadır.

Veri işleme ve aktarım sürecinin şeffaflığını sağlamak adına grup şirket yapısı açıkça ortaya konmalıdır. Bir anlamda Kişisel Verilerin Korunması Kanunu'ndaki veri sorumlusu temsilcisi görevini, grup şirketin tamamında yürütmesi için bir temas kişisi atanmalıdır. Bu kişi, Bağlayıcı Şirket Kuralları'nı taahhüt eden grup şirket üyelerinin güncel iletişim bilgilerini tutmalı ve değişiklik halinde Kurum ile ilgili kişileri haberdar etmelidir.

3.3.2.5. Raporlama ve Kayıt Değişikliği Mekanizmaları

Bağlayıcı Şirket Kuralları nitelikleri itibariyle, grup şirketin ihtiyaçları ve yapısındaki değişimler uyarınca değiştirilebilir ve güncellenebilir bir metindir. Yapılacak bu değişikliklerin, gecikmeksizin Kurum'a ve tüm grup şirket üyelerine iletileceği taahhüt edilmelidir. Değişikliklerin Kurum'a iletilmesine dair öngörülen süre, değişikliğin niteliğine göre değişmektedir. Bağlayıcı Şirket Kuralları'nın koruma seviyesini etkileyen yahut başka bir nedenden ötürü esaslı sayılan değişiklikler, Kurum'a derhal bildirilmelidir. Bağlayıcı Şirket Kuralları veya grup şirket üyelerinde yapılacak esaslı sayılmayan diğer değişikliklerin ise, açıklamalarıyla birlikte Kurum'a yıllık olarak bildirileceği taahhüt edilmelidir. Kurum ile iletişimin sağlanması ve söz konusu raporlamanın yapılması için, bir önceki başlıkta açıklandığı şekliyle yetkili bir kişi atanmalıdır.

3.3.2.6. Veri Güvenliği

Kurum'un hazırladığı rehbere göre Bağlayıcı Şirket Kuralları kapsamına alınacak kişisel veriler sınırlanabilmektedir.[371] Bağlayıcı Şirket Kuralları'nda taahhüt edilecek veri koruma ilkeleri, yalnızca Türkiye'den yapılan aktarımları ya da ileri aktarımları kapsar biçimde düzenlenebilmektedir.

[371] Bkz., dn. 354.

Bağlayıcı Şirket Kuralları'nın kapsamına alınacak kişisel verilere dair açıklamanın lafzındaki muğlaklık nedeniyle, sınırlama olanağının amacı anlaşılamamaktadır. Zira, yalnızca ileri aktarımlara dair taahhüt içeren bir Bağlayıcı Şirket Kuralları pratik olarak uygulanabilir değildir. Açıklamadan anlaşıldığı kadarıyla, Bağlayıcı Şirket Kuralları kapsamında veri koruma ilkelerine dair verilecek taahhüt Türkiye'den yapılacak aktarımlarla sınırlanabilmektedir. Ancak Bağlayıcı Şirket Kuralları kapsamında korunan kişisel verilere dair ileri aktarımlarda da KVKK md. 9 uyarınca öngörülen yeterli güvenlik önlemlerinden birinin bulunması gerekmektedir.

Veri koruma ilkelerine dair verilecek taahhüt, KVKK md. 4/2/a-d hükümlerini içermelidir.[372] Söz konusu taahhütlerden işlendikleri amaçla bağlı ve sınırlı olma ilkesinin bir uzantısı olarak, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmelik[373] önem kazanmaktadır. Burada yer alacak taahhütlere ilişkin Kurum'un hazırladığı ilgili rehberden faydalanılabilecektir.[374] Bunun yanında özel nitelikli kişisel veriler işlenirken, Kişisel Verilerin Korunması Kanunu'nun aradığı ek yükümlülükler de taahhüt edilmelidir.

Bağlayıcı Şirket Kuralları içerisinde, alınan teknik ve idari tedbirler de açıkça taahhüt edilmelidir. Bu tedbirler belirlenirken, Kurum'un idari ve teknik tedbirlere ilişkin hazırladığı rehberden[375] yararlanılabilecektir. Bu tedbirler dahilinde, grup şirketin bir üyesindeki herhangi bir kişisel veri ihlali halinde, Türkiye'deki merkez veya yetkili üyeye bildirim yapılması gerekecektir. Kişisel veri ihlaline ilişkin bildirim ilgili veri koruma birimine ve ihlalden etkilenmesi muhtemel ilgili kişiye de iletilecektir. Bu bildirim esası Bağlayıcı Şirket Kuralları içerisinde taahhüt edilmelidir.

Veri güvenliği başlığı altında, Bağlayıcı Şirket Kuralları düzenleyecek grup şirket ağına dahil yabancı şirketlerin, tâbi oldukları yerel mevzuatlar da incelenmelidir. Yerel mevzuatın grup şirket üyesinin Bağlayıcı Şirket Kuralları'na uymasını engellediği durumlara ilişkin şeffaflık sağlanmalıdır. Bağlayıcı Şirket Kuralları'na uyulmasını

---

[372] Veri koruma ilkelerine dair ayrıntılı açıklama ve GVKT ile karşılaştırma için çalışmanın 1.1. başlığına bakınız.

[373] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm Erişim Tarihi: 04.06.2020.

[374] Kurum'un kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin rehberi için bkz. https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf Erişim Tarihi: 31.05.2020.

[375] Veri Güvenliği Rehberi https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf Erişim Tarihi: 04.06.2020.

önemli ölçüde etkileyen yerel mevzuat hükümleri hakkında, Türkiye'deki merkez veya yetkili üye şirkete bilgilendirme yapılacağı taahhüt edilmelidir. Kurum'un bu durumdan haberdar edileceği de düzenlenmelidir.

Birlik hukukunda, ulusal mevzuat ile taahhüt edilen *Binding Corporate Rules'un* çatışması halinde izlenecek yol açıkça belirtilmiştir.[376] Ancak Bağlayıcı Şirket Kuralları kapsamında bu husus ihtiyari olarak, şirketlerce düzenlenebilecektir. Her ne kadar bu ilişkinin Bağlayıcı Şirket Kuralları'nda ortaya konulması ihtiyari olarak belirtilse de şirket açısından avantajlıdır. Böylece potansiyel bir çatışma halinde grup şirketin izleyeceği yol bilinecektir. Ek olarak bu düzenleme şeffaflığı ve hesap verilebilirliği de arttırmaktadır.

3.3.2.7. Hesap Verilebilirlik ve Diğer Araçlar

Grup şirketin her veri sorumlusu üyesi, Bağlayıcı Şirket Kuralları'na uyum sağlamakla yükümlüdür. Bu yükümlülüğün yerine getirilmesi için tüm kategorilerdeki veri işleme faaliyetlerinin kaydı tutulmalı ve talep halinde Kurum ile paylaşılmalıdır. Çalışmamızda belirtildiği üzere hesap verilebilirlik, Kişisel Verilerin Korunması Kanunu içerisinde açıkça düzenlenen bir ilke değildir.[377] Dolayısıyla içeriği Kurum duyurusu ile belirlenen Bağlayıcı Şirket Kuralları'na açıkça dahil edilmesi değerlendirilmelidir.

Çalışmamızın ilgili kısmında açıklandığı üzere hesap verilebilirlik, Kanun'da ayrı bir ilke olarak düzenlenmese de hesap verilebilirliğin sağlanması için bazı araçlar öngörülmüştür.[378] Öyle ki hesap verilebilirlik, veri sorumlularının KVKK md. 12 uyarınca düzenlenen veri güvenliğine ilişkin yükümlülükleri yerine getirdiğini ifade etmektedir. Dolayısıyla bu amacın yerine getirilmesi için öngörülecek araçların hesap verilebilirlik başlığı altında toplanması, fikrimizce Kanun'un amacına da uygundur.

Nitekim Bağlayıcı Şirket Kuralları'nın önemli avantajlarından biri, çalışmanın 3.3.1. başlığında açıklandığı üzere KVKK md. 12 yükümlülüklerine dair hesap verilebilirliği arttırması ve ispat aracı olarak kullanılabilmesidir. Bağlayıcı Şirket Kuralları içinde hesap verilebilirliğin arttırılması amacıyla, ilgili kişilerin hak ve özgürlükleri üzerinde yüksek risk arz eden veri işleme faaliyetleri için risk analizi

[376] BCR'da taahhüt edilen bir hususun ulusal mevzuatla çatışması halinde öngörülen hükümlere dair çalışmanın 2.3.1.13. başlığına bakınız.
[377] Bkz., çalışmanın 1.1.7. başlığı.
[378] Bkz. çalışmanın 1.1.7. başlığı.

yapılması taahhüt edilmelidir. Yapılan risk analizi ışığında, riski en aza indirmek için gerekli önlemlerin alınacağı ve yüksek risk halinde, işleme faaliyetinden evvel Kurum'a danışılacağı düzenlenmelidir.

3.3.2.8. Yardımcı Bilgi ve Belgeler

Kurum tarafından hazırlanan yardımcı rehberde[379] Bağlayıcı Şirket Kuralları'na dahil edilmesi zorunlu tutulmayan yardımcı belgeler belirlenmiştir. Buna göre aktarımın yapılacağı ülkelerin taraf olduğu ve kişisel verilerin korunması konusunda hüküm içeren uluslararası sözleşmelere dair bilgi verilmesinin yararlı olacağı yazılmıştır. Benzer şekilde kişisel verinin aktarılacağı ülkede, veri koruma otoritesinin varlığına dair bilgi verilmesi de ihtiyari tutulmuştur.

3.3.3. Başvuru Usul ve Esasları

Kurum tarafından yapılan duyuruda belirtildiği şekliyle, Bağlayıcı Şirket Kuralları düzenleyebilecekleri öngörülmüş şirketlerin, duyuru ekinde öngörülen başvuru formunu doldurup gerekli talimatları izleyerek, Kurum'a başvuru yapmaları gerekmektedir.[380] Bağlayıcı Şirket Kuralları düzenleyen grup şirketlerin Türkiye'de yerleşik merkezi, başvuruyu yapmaya yetkili addedilmiştir. Grup şirketlerin Türkiye'de yerleşik merkezi olmaması halinde ise, grubun Türkiye'de yerleşik bir üyesi, kişisel verilerin korunması konusunda yetkilendirilmelidir. Bu durumda, başvuru yapma yetkisi söz konusu üyeye ait olacaktır.

Kurum, başvuruda sunulacak bilgi ve belgeler dahilinde, Bağlayıcı Şirket Kuralları ve forma ek olarak ilgili gördüğü diğer tüm evrakı talep edebilmektedir. Doldurulacak formda, veri aktarımının yapılacağı tüm ülkeler ve grup şirket yapısının kapsadığı tüm üyelerin iletişim bilgileri belirtilmelidir. Bir yıl içerisinde değerlendirip sonuca bağlanması öngörülen başvuru süreci, altı ay daha uzatılabilmektedir.

Bağlayıcı Şirket Kuralları başvuru formunda, değerlendirme kriteri olarak sekiz soru başlığı belirlenmiştir. İlk olarak hazırlanan yapının iç ve dış bağlayıcılık unsuruna ilişkin sorular yer almaktadır. Bağlayıcı Şirket Kuralları başvurusunun uygun bulunabilmesi için ulusal mevzuata uygun olarak, tüm grup şirket üyelerini bağlayıcı bir

[379] Bkz., dn. 354.
[380] Bkz., dn. 354.

etkiye sahip olması gerekmektedir. İlk bölümde yer alan sorular, söz konusu bağlayıcılık unsurunun bulunup bulunmadığının tespit edilmesini sağlamaktadır.

İkinci soru başlığı ise hazırlanan Bağlayıcı Şirket Kuralları'nın etkin uygulanmasına ilişkindir. Bu bölüm altında etkin bir uygulama için grup şirket bünyesinde hangi mekanizmaların nasıl kullanıldığına ilişkin sorular yer almaktadır. Üçüncü olarak ise Kurum ile koordinasyonun sağlanması için öngörülen yöntemlere ilişkin sorular yöneltilmektedir. Dördüncü soru başlığı ise, Bağlayıcı Şirket Kuralları'nı düzenleyen grup şirket içerisindeki veri aktarımına ilişkindir. Bu başlık altında grup içerisindeki kişisel veri işleme süreçlerinin açık ve anlaşılır şekilde tanımlanması gerekmektedir.

Beşinci başlıkta Bağlayıcı Şirket Kuralları'nda ilgili kişilerin haklarını etkileyecek türden değişikliklerin Kurum'a bildirilmesi süreci değerlendirilmektedir. Bu bildirimin yapılması için öngörülen mekanizmalara dair sorular yöneltilmektedir. Altıncı soru başlığında veri güvenliğini sağlamak adına alınan tüm teknik ve idari tedbirlerin, detaylarıyla açıklanması istenmektedir. Bağlayıcı Şirket Kuralları içerisinde bu konuların nasıl düzenlendiği, destekleyici dokümanlarla belirtilmelidir.

Yedinci başlıkta ise, hesap verilebilirlik esas ve araçlarına dair sorular yer almaktadır. Bu başlık altında yer alan önemli bir husus, grup üyesi her bir veri sorumlusunun veri işleme faaliyetlerinin kaydının nasıl tutulacağının açıklanmasıdır. Formda belirtildiği üzere, hesap verilebilirliğin sağlanması amacı ile kişisel veri işleme envanterinin hazırlanması gerekmektedir. Haliyle Tüzük'te yer almayan envanter tutma zorunluluğunun[381], Bağlayıcı Şirket Kuralları dahilindeki grup şirket üyelerinin her biri için ayrıca gündeme gelip gelmeyeceği sorusu doğmaktadır. Bu anlamda Kurum'un hazırladığı yardımcı dokümanda yalnızca, grup şirket üyelerinin tüm kategorilerdeki veri işleme faaliyetlerinin yazılı şekilde kaydını tutması ve talep halinde Kurum'a sunması gerektiği yazmaktadır. Formdaki son soru başlığı ise, aktarımın yapılacağı ülkelerin taraf olduğu ve kişisel verilerin korunması konusunda hüküm içeren uluslararası sözleşmelere ve grup şirket üyelerinin ulusal kişisel verileri koruma mevzuatlarına ilişkindir.

[381] Kişisel veri işleme envanteri, Veri Sorumluları Sicili Hakkında Yönetmelik md. 4/1(h) ile "Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter..." olarak tanımlanmaktadır.

Kurum'un yukarıdaki açıklamasının işaret ettiği şekilde, Birlik hukukuna göre düzenlenmiş bir *Binding Corporate Rules'u* taahhüt eden Türk üyenin, iletilen metni tercüme ederek, bu evrak ile grup adına Bağlayıcı Şirket Kuralları başvurusu yapması da mümkün olabilecektir. Elbette bu başvuru yapılmadan önce, tercüme edilen metnin Kurum'un Bağlayıcı Şirket Kuralları içeriğine dair aradığı tüm hususları taahhüt ettiğinden emin olunmalıdır. Böyle bir ihtimal gerçekleştirildiği takdirde hem Birlik'ten Türkiye'ye hem de Türkiye'den Birliğe, grup şirket üyeleri arası yapılacak veri aktarımları hukuka uygun hale gelecektir. Böylece Kişisel Verilerin Korunması Kanunu'na da Tüzüğe de uyum sağlanmış olacaktır. Yalnız bu husus bile Bağlayıcı Şirket Kuralları gibi düzenlemelerin, yeknesak uluslararası veri koruma esasları için önemini ortaya koymaktadır.

SONUÇ

Birlik hukukunda grup şirketler veya ekonomik iş birliği içerisindeki teşebbüsler *Binding Corporate Rules* düzenleyebilmektedir. Bu metinler grup şirketin kendi ihtiyaçlarına göre hazırlanmakta ve Tüzüğün öngördüğü yükümlülükleri taahhüt etmektedir. *Binding Corporate Rules'un* geçerli olması için grup şirket veya ekonomik iş birliği içerisindeki teşebbüs üyelerinin tamamı tarafından taahhüt edilmeleri gerekmektedir. Yetkili veri koruma otoritesince onaylanan *Binding Corporate Rules,* grup şirket içerisindeki kişisel veri aktarımları açısından uygun güvenlik önlemi niteliği kazanmaktadır. Grup şirketin üçüncü ülkelerdeki üyelerine, başkaca bir önlem alınmadan veri aktarılabilmektedir. Ancak verilerin üçüncü ülkeden ileri aktarımları için başkaca güvenlik önlemlerinin alınması gerekecektir. *Binding Corporate Rules* yalnızca Birlik hukukuna uyumu göstermektedir ve yalnızca Tüzük uyarınca uygun güvenlik önlemi teşkil etmektedir. Dolayısıyla üçüncü ülkedeki üyeden Birlik'teki üyelere yapılacak veri aktarımlarında, üçüncü ülkedeki üyenin tâbi bulunduğu iç hukukta öngörülen veri aktarım kurallarına uyulması gerekmektedir.

Çalışmamızda Tüzüğün düzenlediği ve *Binding Corporate Rules'da* taahhüt edilecek veri işleme ilkeleri incelendikten sonra üçüncü ülkelere veri aktarımları değerlendirilmiştir. Verilerin serbestçe aktarılabileceği güvenli ülke listesi incelenmiştir. Şayet verilerin aktarılacağı ülke bu listede yer almıyorsa, Tüzük'te öngörülen uygun güvenlik önlemlerinden birinin varlığı gerekecektir. *Binding Corporate Rules'un* da arasında bulunduğu bu uygun güvenlik önlemleri karşılaştırılmış ve her birinin taşıdığı farklı avantajlar ortaya konulmuştur. Üçüncü ülkelere veri aktarımlarında genel prensipler ortaya koyan *Schrems I* ve *Schrems II* kararları değerlendirilmiştir. *Schrems I* kararının iptal ettiği *Safe Harbor* anlaşmasının etkileri incelenmiştir. Yapılan bir araştırmada *Safe Harbor* taahhütlerini vermiş Amerikan şirketlerinin çoğunun bu taahhütlere uymadığı belirlenmiştir. İlerideki çalışmalarda, benzer bir ampirik araştırmanın *Binding Corprote Rules* taahhütleri için de yapılması son derece ilginç olacaktır. Özellikle Tüzük ile getirilen yüksek idari para cezalarının ve *Schrems I ve II*

kararlarının taahhütleri veren şirketlerin uyumuna etkisi, önemli bir araştırma noktası olacaktır.

Schrems I ve II kararları ışığında üçüncü ülkelere veri aktarımı kurallarının temelde, Birlik vatandaşlarının haklarını üçüncü ülkelerde de benzer bir kolaylıkla kullanabilmelerini hedeflediği belirlenmiştir. Verisi işlenen Birlik vatandaşı, Birlik hukukundaki veri koruması kanunlarında sahip olduğu hakları, üçüncü ülkede de kullanabilmektedir. Kararlar aynı zamanda verilerin aktarıldığı üçüncü ülkedeki devlet otoritelerinin kişisel verilere erişimini ve denetim hakkını da değerlendirmiştir. Öyle ki karardaki somut olayda, Birlik'ten aktarılan verilere devlet otoritelerinin öngörülemeyen erişim hakkı ölçüsüz bulunmuştur. Ek olarak devlet otoritesinin ulusal güvenlik sebebiyle Birlik vatandaşlarını izleyebileceğine dair iç hukuk düzenlemeleri de ölçüsüz bulunmuş ve Birlik hukukuna aykırı olduğuna karar verilmiştir. Kararlarla getirilen kriterler gerek güvenli ülke listesi için gerekse alınan uygun güvenlik önlemlerinin hukuka uygunluğu değerlendirilirken dikkate alınmaktadır.

Uygun güvenlik önlemleri için yapılan karşılaştırmada *Binding Corporate Rules'un* pek çok başka avantaja da sahip olan geniş bir taahhüt metni olduğu belirtilmiştir. Çalışmamızda açıklandığı şekliyle *Binding Corporate Rules* ve benzeri sistemler, global dünyada iyiden iyiye önem kazanan veri ekonomisi kavramı için kritik önem taşımaktadır. Günümüzde kişisel veri aktarımları, uluslararası ticaretin kaçınılmaz bir parçasıdır. Dolayısıyla uluslararası ticaretin güvenli bir şekilde gelişmesi için global veri koruması standartlarının benimsenmesi gerekmektedir. Çalışmamızda *Binding Corporate Rules* ve Sınırötesi Mahremiyet Kuralları gibi global düzenlemelerin bu anlamdaki önemlerine de değinilmiştir. Asya-Pasifik Ekonomik İş Birliği tarafından getirilen Sınırötesi Mahremiyet kurallarının uluslararası veri aktarımını düzenlerken, *Binding Corporate Rules'dan* farklı bir anlayış benimsediği tespit edilmiştir. Hesap verilebilirlik üzerinden ilerleyen bu sistem, bir anlamda ekonomik gelişime hizmet etmeyi amaçlamaktadır.

Söz konusu sistemler global şirketlere, grup şirket bünyesinde yapılan kişisel veri aktarımları için pratik ve güvenli bir yöntemler sağlamaktadırlar. *Binding Corporate Rules* benzeri veri işleme taahhütlerini grup şirket bünyesinde düzenleyen metinler, aynı zamanda ilgili kişilerin verilerini korumayı ve hesap verilebilirliği arttırmayı hedeflemektedir. Böylece ilgili kişilere deyim yerindeyse 'grup şirketin verileri aktardığı

her yerde kişisel verilerinin peşine düşebilme' hakkı tanınmaktadır. Bundandır ki, taahhüt altına aldıkları belirli hususlar sayesinde grup şirketin hesap verilebilirliği de artmaktadır.

Binding Corporate Rules sayesinde grup şirket veya ekonomik iş birliği halindeki teşebbüslere dahil tüm şirketler ve bu şirketlerin arasındaki ilişki açıkça ortaya konmaktadır. Grup şirket bünyesinde verilerin toplanmasından yok edilmesine kadar olan işleme süreci açık ve anlaşılır biçimde düzenlenmektedir. Yetkili veri koruma otoritelerinin denetiminden geçen bu süreç sonucunda verilerin aktarılması dahil tüm işleme sürecinde şeffaflık sağlanmaktadır. Şeffaflık ve hesap verilebilirliğe dair sağladığı bu avantajlarla *Binding Corporate Rules,* ispat gücü olan bir doküman niteliği kazanmaktadır. Bu anlamda olası hukuka aykırılıklarda özen borcuna riayet edildiğine işaret etmektedir. Şüphesiz ki bu husus, ilgili kişilerin olası zararlarından doğacak tazminat talepleri için de idari para cezaları için de önemli bir avantajdır.

Çalışmamızda çoğunlukla Tüzük kapsamında, amacı, avantajları, içerdiği taahhütler ve geçerlilik şartları değerlendirilen *Binding Corporate Rules'un,* Türkiye'deki bir üyece taahhüt edilmesi de incelenmiştir. Somut örnekler üzerinden Türk hukuku kapsamında karşılaşılabilecek sorunlar belirlenmiştir. İdari para cezaları ile tazminat başta olmak üzere, yöneltilebilecek hak iddiaları değerlendirilmiştir. Bu değerlendirme Kişisel Verilerin Korunması Kanunu ile Tüzük arası bir karşılaştırmayı gerektirmiştir. *Binding Corporate Rules'u* taahhüt eden grup şirketin Türkiye'deki üyesi için pek çok avantaj taşıyacağı sabittir. Öyle ki, *Binding Corporate Rules'da* verilen taahhütleri uygulayan Türkiye'deki üye şirket, Tüzüğün veri koruması standartlarına taşınacaktır. Bu husus şüphesiz ki büyük bir ekonomik avantajdır.

Son olarak *Binding Corporate Rules* sisteminden etkilenerek, Kurum'un benimsediği Bağlayıcı Şirket Kuralları incelenmiştir. Grup şirket bünyesinde serbest veri aktarımı için uygun güvenlik önlemi teşkil edecek bu sistemin avantajları değerlendirilmiştir. Bağlayıcı Şirket Kuralları içerisinde taahhüt edilmesi gereken hususlar ve başvuru esasları değerlendirilmiştir. İçeriğinde taahhüt edilecek hususlarla Kişisel Verilerin Korunması Kanunu'nda sağlanan veri koruması standartlarının Tüzüğe yaklaştığı belirlenmiştir. İleride yapılacak araştırmalarda, onaylanacak Bağlayıcı Şirket Kuralları'nın uygulamada incelenmesi ve Kurum'un bu kurallara uyulmaması halinde uygulayacağı yaptırımlar, yararlı inceleme noktaları olacaktır.

Çalışmamızda Bağlayıcı Şirket Kuralları düzenleyen şirketlerin teoride Birlik standartlarına yaklaşan bir yapı kuracağı tespit edilmiştir. Ancak kişisel veri envanteri tutma gibi yükümlülüklerin, grup şirketin potansiyel olarak yabancı üyelerine de yöneltilmesinin uygulamada güçlük çıkarabileceği saptanmıştır. Bunun yanında Türk hukukuna göre yetkili veri koruma mercilerine Birlik ülkelerindeki şirketler üzerinde muğlak denetim yetkileri tanındığı ortaya konulmuştur. Bu hususun *Schrems I* ve *Schrems II* kararlarıyla, üçüncü ülkedeki devlet otoritelerinin denetim yetkisine dair benimsenen kriterlere aykırı düşebileceği kanısına varılmıştır.

Kurum, Bağlayıcı Şirket Kuralları düzenleyebileceğini öngördüğü grup şirket yapısını, merkezi Türkiye'de olan şirketlerle sınırlamamıştır. Öyle ki, yabancı merkezli bir grup şirketin, Türkiye'deki üyesinin yetkilendirilmesi halinde Bağlayıcı Şirket Kuralları düzenlemesi mümkündür. Bu imkân, *Binding Corporate Rules'a* sahip yabancı merkezli grup şirketler için söz konusu taahhütlerin, incelenip gözden geçirilerek ve gerektiği yerlerde eklemeler yapılarak, Kurum nezdinde Bağlayıcı Şirket Kuralları olarak taahhüt edilebilmesini sağlamaktadır. Böylece grup şirket içerisindeki veri aktarımları hem Tüzük hem de Kişisel Verilerin Korunması Kanunu kapsamında hukuka uygun hale gelecektir. Bu imkân *Binding Corporate Rules* benzeri düzenlemelerin uluslararası veri koruması standartları için önemini göstermektedir. Çalışmamızda gösterildiği şekilde globalleşen dünyada ihtiyaç duyulan uluslararası standartların hazırlanması için, bu düzenlemeler önem taşımaktadır.

KAYNAKÇA

KİTAPLAR

ARKAN Sabih, Ticari İşletme Hukuku, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayını, Ankara, Türkiye 2014.

AUERNHAMMER Herbert, Datenschutz-Grundverordnung Bundesdatenschutzgesetz und Nebengesätze Kommentar, 7. Auflage, Carl Heymanns Verlag, Köln, Almanya 2020.

von dem BUSSCHE Axel, VOIGT Paul, Konzerndatenschutz: Rechtshandbuch, 2. Auflage, C.H. Beck, München, Almanya 2019.

ÇEKİN S. Mesut, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 3. Baskı, Onikilevha Yayınları, İstanbul, Türkiye 2020.

DAMMAN Ulrich, SIMITIS Spiros, Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlag, Baden-Baden 2011.

EHMANN Eugen, SELMAYR Martin, Datenschutz-Grundverordnung Kommentar, 2. Auflage C.H. Beck, München, Almanya 2018.

FORGO Nikolaus, HELFRICH Marcus, SCHNEIDER Jochen, Betrieblicher Datenschutz, 3. Auflage, C.H. Beck, München, Almanya 2019.

GRABITZ Eberhard, HILF Meinhard, das Recht der Europäischen Union, 40. Auflage, C.H. Beck, München 2009.

KAMA IŞIK Sezen, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış: 2016/679 Sayılı GVKT ile 6698 Sayılı KVKK'nın Detaylı Analiz ve Karşılaştırması, 1. Basım, On İki Levha Yayıncılık, İstanbul, Türkiye 2020.

KAYA M. Bedii, Kişisel Verileri Koruma Hukuku – Mevzuat ve İçtihat, 1. Basım, On İki Levha Yayıncılık, İstanbul, Türkiye 2018.

KLECHA Robert, Datenübermittlungen in die USA nach dem Safe Harbor Urteil des EuGH, Verlag Dr. Kovac, Hamburg, Almanya 2018.

KREMPELMEIER Sebastian, STAUDINGER Isabel, WEISER Katharina, Datenschutzrecht nach der DSGVO – zentrale Fragenstellungen,, Jan Sramek Verlag, Salzburg, Avusturya 2018.

KUNER Christopher, Transborder Data Flows and Data Privacy Law, 1st Edition, Oxford University Press, Birleşik Krallık 2013.

KUNER, Christopher, BYGRAVE, Lee, DOCKSEY, Christopher, The EU General Data Protection Regulation: A Commentary, Oxford University Press, Oxford, Birleşik Krallık 2020.

KÜHLING Jürgen, BUCHNER Benedikt, Datenschutz-Grundverordnung Kommentar, 2. Auflage, C.H. Beck, München 2018.

KÜHLING Jürgen, KLAR Manuel, SACKMANN Florian, Datenschutzrecht, 4. Auflage, C.F. Müller, Heidelberg, Almanya 2018.

KÜZECİ Elif, Kişisel Verilerin Korunması, 3. Baskı, Turhan Kitabevi, Ankara, Türkiye 2019.

von LEWINSKI Kai, die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, Mohr Siebek Verlag, Tübingen, Almanya 2014.

MAURER-LAMBROU Urs, BLECHTA P. Gabor, Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Helbing Lichtenhahn Verlag, Basel, İsviçre 2014.

MOEREL Lokke, Binding Corporate Rules: Fixing Regulatory Patchwork of Data Protection [n.n.] Tilburg, Hollanda 2011.

MOEREL Lokke, Binding Corporate Rules: Corporate Self Regulation of Global Data Transfers, Oxford University Press, Birleşik Krallık 2012.

MOOS Flemming, SCHEFZIG Jens, ARNING Marian, Die Neue Datenschutz-Grundverordnung, De Gruyter Yayınevi, Berlin, Almanya 2018.

OĞUZMAN M. Kemal, ÖZ M. Turgut, Borçlar Hukuku Genel Hükümler Cilt – II, 10. Bası, Vedat Kitapçılık, İstanbul, Türkiye 2013.

OĞUZMAN M. Kemal, ÖZ M. Turgut, Borçlar Hukuku Genel Hükümler Cilt – II, 14. Bası, Vedat Kitapçılık, İstanbul, Türkiye 2018.

PAAL Boris, PAULY Daniel, Datenschutz-Grundverordnung, 2. Auflage, C.H. Beck, München, Almanya 2018.

SCHNEIDER Jochen, Datenschutzrecht nach der EU-DSGVO, 2. Auflage, C.H. Beck, München, Almanya 2019.

SCHRÖDER Christian, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, 1. Auflage, Nomos Verlag, Frankfurt, Almanya 2007.

SEROZAN Rona Medeni Hukuk Genel Bölüm – Kişiler Hukuku, 4. Baskı, Vedat Kitapçılık, İstanbul, Türkiye 2011.

SIMITIS Spiros, HORNUNG Gerrit, SPIECKER Indra, Datenschutzrecht DSGVO mit BDSG, 1. Auflage, Nomos Verlag, Baden-Baden, Almanya 2019.

SPECHT Louisa, MANTZ Reto, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, C.H: Beck, München, Almanya 2019.

TREACY Bridget, SIMPSON Aaron, An Introduction Do Data Protection Law, Lexis Nexis, London, Birleşik Krallık 2019.

UYGUR Turgut, 6098 Sayılı Türk Borçlar Kanunu Şerhi, 1. Baskı, Seçkin Yayıncılık, İstanbul, Türkiye 2012.

VOSKAMP Frederike, Transnationaler Datenschutz, 1. Auflage, Nomos Verlag, Frankfurt, Almanya 2015.

WEAVER Russel, FRIEDLAND Steven, GILLES William, BOUHADANA Irene, Privacy in a Digital Age Perspective from Two Continents Volume IV, Carolina Academic Press, North Carolina, Amerika Birleşik Devletleri 2017.

WEBER H. Rolf, STEIGER N. Dominic, Transatlantic Data Protection in Practice, Springer, Berlin-Heidelberg, Almanya 2017.

MAKALELER

BOTTA Jonas (2020), ‘Eine Frage des Niveaus: Angemessenheit drittstaatlicher Datenschutzregime im Lichte der Schlussanträge in „Schrems II“ - Der Prüfungsmaßstab der Gleichwertigkeit und seine Reichweite im Bereich der nationalen Sicherheit’, Computer und Recht, C. 36, S. 2, s. 82-89.

BOWMAN John, GUFFLET Myriam (2017), ‘Meeting the Challenge of a Global GDPR and BCR Programme’, European Data Protection Law Review, C. 3, S. 2, s. 257-261.

ÇEKİN S. Mesut (2016), ‘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, s. 629-644.

DEMETZOU Katerina (2019), ‘Data Protection Impact Assessment: A tool for accountability and the unclarified concept of high risk in the General Data Protection Regulation’, Computer Law & Security Review, C. 35, S. 6, (Article 105342).

FILIP Alexander (2013), ‘BCR aus der Sicht einer Datenschutzaufsichtsbehörde – Praxiserfahrungen mit der europaweiten Anerkennung von BCR’, ZD, C. 2, s. 51-60.

KARA Hacı (2019), 'Türk Hukukunda İrtibat Bürosu ve Özellikleri', İzmir Barosu Dergisi, C. 83, S. 3, s. 167-198.

KENNEDY, B. John 'When Woman is Boss: An Interview with Nikola Tesla', Colliers, January 30, 1926.

KULEZSA, Joanna (2014), 'Transboundary data protection and international business compliance', International Data Privacy Law, C. 4, S. 4, s. 298 – 306

KUNER Christopher (2017), 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', German Law Journal, C. 18, S. 4, s. 864.
KUNER Christopher (2014), 'The European Union and the Search for an International Data Protection Framework', Groningen Journal of International Law, C. 2, S. 2, s. 55-71.

KÜHLING Jürgen, MARTINI Mario (2016), DSGVO: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW, C.6, s. 448.

MARTIN, Nicholas, FRIEDEWALD, Michael (2019), 'Warum Unternehmen Sich Nicht an Recht und Gesetz Halten', Datenschutz und Datensicherheit, C. 43, s. 493-497.

LACHAUD Eric (2016), 'Why the Certification Process Defined in the GDPR Cannot Be Successful', Computer Law & Security Review, C. 32, s. 814–826.

van LIESHOUT, Marc (2015), 'the Value of Personal Data', IFIP Advances in Information and Communication Technology, C. 457, S. 5, s. 26-38.

MASOCH, Daniela (2019), 'Why Should Companies Invest in Binding Corporate Rules?' ICLG.com online journal, publishing date 03.07.2019.

MATTOO Aaditya, MELTZER Joshua (2019), 'International Data Flows and Privacy: The Conflict and Its Resolution', Journal of International Economic Law, C. 21, S. 4, s. 769-789.

RICHARDS M. Neil, KING H. Jonathan (2014), 'Big Data Ethics', Wake Forest Law Review, C. 49, s. 395-432.

SPIEKERMANN Sarah, BÖHME Rainer, ACQUISTI Alessandro, HUI Kai-Lung (2015), 'Personal Data Markets', Electron Markets, C. 25, s. 91–93.

SULLIVAN Claire (2019), '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. 35, s. 380-397.

TEHRANI Pardis, SABARUDDIN Johan, RAMANATHAN Dhiviya (2018), ‚Cross Border Data Transfer: Complexity of Adequate Protection and Its Exceptions', Computer Law & Security Review, C. 34, s. 582-594.

QUELLE Claudia (2018), '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.

WAGNER Julian (2018), 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide Adequate Protection?', International Data Privacy Law, C.8, S. 4, s. 318-337.

İNTERNET KAYNAKLARI

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

A Brief History of Big Data Everyone Should Read
https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/
Erişim Tarihi: 09.01.2020.

Bağlayıcı Şirket Kuralları Hakkında Duyuru
https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU
Erişim Tarihi: 22.07.2020.

Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği, 'Guiding Principles on Business and Human Rights, New York and Geneva 2011'
https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
Erişim Tarihi: 07.06.2020.

Centre for Information Policy Leadership, 'The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society'
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf
Erişim Tarihi: 07.06.2020.

The Data Deluge https://www.economist.com/leaders/2010/02/25/the-data-deluge
Erişim Tarihi: 09.01.2020.

Data Protection Schemes Active in Europe https://www.researchgate.net/figure/Data-protection-certification-schemes-active-in-Europe-in-2016_tbl1_305821630
Erişim Tarihi: 29.04.2020.

Datenschutz Risiken
https://www.pwc.ch/de/dienstleistungen/consulting/risiken/datenschutz.html

Erişim Tarihi: 03.05.2020.

EDÖB Datenübermittlung ins Ausland kurz erklärt, 10.12.2018 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwixxpjw2fTpAhWmThUIHTbfAPYQFjABegQICRAB&url=https%3A%2F%2Fwww.edoeb.admin.ch%2Fdam%2Fedoeb%2Fde%2Fdokumente%2F2018%2FDaten%25C3%25BCbermittlung%2520kurz%2520erkl%25C3%25A4rt.pdf.download.pdf%2FUebermittlung%2520ins%2520Ausland%2520kurz%2520erkl%25C3%25A4rt%2520d.pdf&usg=AOvVaw1kc15YWTVuO-Fpx2uJZzux
Erişim Tarihi: 19.04.2020.

EDÖB Übermittlung ins Ausland
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html
Erişim Tarihi: 19.04.2020

Edward Snowden: the Whistleblower Behind NSA Surveillance Revelations
https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
Erişim Tarihi: 18.11.2020.

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: 20.08.2020.

GDPR Certification https://www.eugdpr.institute/gdpr-certification/
Erişim Tarihi: 09.03.2020.

Guide to Codes of Conduct https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/
Erişim Tarihi: 08.03.2020

GVKT'nin yürürlüğe girmesinden önce Direktif döneminde hazırlanıp onay süreçleri biten BCR listesi https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841
Erişim Tarihi: 19.03.2020.

How Much Data Do We Create Everyday?
https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#26747cd960ba
Erişim Tarihi: 09.01.2020.

Kişisel Verileri Koruma Kurumu 27.03.2020 tarihli Kamuoyu Duyurusu
https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-
Erişim Tarihi: 08.01.2021.

Multimedia und Rechts Zeitschrift (MMR) 2015, 753 ve 754
https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2015%2Fcont%2Fmmr.2015.753.1.htm&anchor=Y-300-Z-MMR-B-2015-S-753-N-1
Erişim Tarihi: 30.04.2020.

Personal Data Protection Factsheet of the European Parliament
https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection
Erişim Tarihi: 18.04.2020.

REGALDO Antonio (2011), 'Who coined Cloud Computing', MIT Technology Review
https://www.technologyreview.com/s/425970/who-coined-cloud-computing/
Erişim Tarihi: 13.04.2020

Safe Harbor – Edward Snowden Gratuliert Max Schrems
https://www.derstandard.at/story/2000023298761/edward-snowden-gratuliert-max-schrems
Erişim Tarihi: 12.03.2020.

United Nations Conference On Trade And Development, 'Data Protection Regulations And International Data Flows: Implications For Trade And Development' New York and Geneva 2016 https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
Erişim Tarihi: 07.06.2020.

United Nations "Protect, Respect and Remedy" Framework for Business and Human Rights
https://www.business-humanrights.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf
Erişim Tarihi: 07.06.2020.

What is explicit consent?
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/
Erişim Tarihi: 08.01.2021.

24 Mayıs 2018 tarihi itibariyle EU-BCR süreçleri tamamlanmış şirketler listesi
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841
Erişim Tarihi: 28.03.2020.

MEVZUAT

Alman Federal Veri Koruma Kanunu (‘BDSG’)

Alman Medeni Kanunu (‘BGB’)

İsviçre Veri Koruma Yasası (‘DSG’)

95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi (‘Direktif’)

2016/679 sayılı Avrupa Parlamentosu ve Konseyi Tüzüğü (‘GVKT’)

6698 Sayılı Kişisel Verilerin Korunması Kanunu (‘KVKK’)

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (‘ETK’)

4857 sayılı İş Kanunu (‘İK’)

6098 sayılı Türk Borçlar Kanunu (‘TBK’)

5237 sayılı Türk Ceza Kanunu (‘TCK’)

4721 sayılı Türk Medeni Kanunu (‘TMK’)

6102 sayılı Türk Ticaret Kanunu (‘TTK’)

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu.

Avrupa Birliği Veri Koruma Kurulu Standart Veri Koruma Maddeleri SET I, SET II ve SET III https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
Erisim Tarihi: 07.03.2020.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ
https://kvkk.gov.tr/Icerik/5443/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESINDE-UYULACAK-USUL-VE-ESASLAR-HAKKINDA-TEBLIG
Erişim Tarihi: 04.06.2020.

European Treaty Series No: 108 ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm
Erişim Tarihi: 04.06.2020.

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm
Erişim Tarihi: 04.06.2020.

KARARLAR

Avrupa Adalet Divanı, C-101/01 (Lindqvist)

Avrupa Adalet Divanı, C-131/12 (Google Spain)

Avrupa Adalet Divanı, C-230/14 (Weltimmo)

Avrupa Adalet Divanı, C-362/14 (Schrems I)

Avrupa Adalet Divanı, C-311/18 (Schrems II)

Avrupa Adalet Divanı, C-673/17 (Planet49)

Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Kararı https://www.kvkk.gov.tr/Icerik/6739/2020-173 Erişim Tarihi: 24.05.2020.

Birlik Komisyonu 2000/520 sayılı *Safe Harbor* kriterleri kararı

Birlik Komisyonu 2016/1250/EU *Privacy Shield* kararı

Birlik Komisyonu üçüncü ülkelere veri aktarımında yeterlilik kararı
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
Erişim Tarihi: 30.01.2020

BVerfG 65,1 Sayılı 15.12.1983 tarihli Nüfus Sayımı Kararı.

Danıştay 5. daire 10.12.2013 tarihli 2013/5342 E. ve 2013/9525 K. sayılı karar.

Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, OJ L 296/41, of 23 November 2000.

Facebook Hakkında Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Karar Özeti
https://www.kvkk.gov.tr/Icerik/5450/2019-104
Erişim Tarihi: 08.01.2021.

Facebook hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti

https://kvkk.gov.tr/Icerik/5534/2019-269
Erişim Tarihi: 08.01.2021.

İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması Kararı.
https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi
Erişim Tarihi: 04.06.2020.

Kimliği belirsiz kişi/kişilerin veri sorumlusu olarak kabul edilemeyeceği hakkında Kişisel Verileri Koruma Kurulunun 13/09/2018 Tarihli ve 2018/106 Sayılı Kararı. https://kvkk.gov.tr/Icerik/5421/-Kimligi-belirsiz-kisi-kisilerin-veri-sorumlusu-olarak-kabul-edilemeyecegi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-13-09-2018-tarihli-ve-2018-106-sayili-Karari-Ozeti
Erişim Tarihi: 24.05.2020

Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Kararı ve 31/05/2019 Tarihli ve 2019/165 sayılı Kararı.
https://www.kvkk.gov.tr/Icerik/5496/2019-81-165
Erişim Tarihi: 04.08.2020.

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 Kararı. https://www.kvkk.gov.tr/Icerik/5545/2019-225
Erişim Tarihi: 24.05.2020.

GÖRÜŞLER, BİLDİRİLER VE RAPORLAR

Birlik Komisyonu Daimler Chrysler AG BCR'a Dair Görüş https://ec.europa.eu/justice/article-29/press-material/public-consultation/bcr/2003_bcr/daimlerchrysler_en.pdf
Erişim Tarihi: 20.03.2020.

DSK Positionspaper v. 21.10.2015

European Data Protection Board - Guidelines 3/2018 on the territorial scope of the GDPR.

European Data Protection Board 'Information Note on BCRs for Companies which have ICO as BCR Supervisory Lead Authority (12.02.2019).

European Data Protection Supervisor, International Data Transfers https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en

Erişim Tarihi: 13.04.2020

TC Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Haziran 2017 tarihli Avrupa Birliği Genel Veri Koruma Tüzüğünün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi Konulu Çalışma Raporu
http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf
Erişim Tarihi: 30.04.2020.

Komisyon'un Brexit'e hazırlık Bildirisi, 1. Kısım. https://ec.europa.eu/info/brexit/brexit-preparedness/preparedness-notices_en
Erişim Tarihi: 28.03.2020.

Komisyon'un 6 Mayıs 2003 tarihli 2003/361/EC sayılı 'mikro küçük ve orta büyüklükte işletme görüşü'

Kurul'un kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin rehberi için bkz. https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf
Erişim Tarihi: 31.05.2020.

Md. 29 Çalışma Grubu görüşleri için arşiv https://ec.europa.eu/justice/article-29/documentation/opinion- recommendation/index_en.htm#maincontentSec21
Erişim Tarihi 19.03.2020.

Md. 29 Çalışma Grubu Opinion Working Paper 203

Md. 29 Çalışma Grubu Opinion Working Paper 256.

Md. 29 Çalışma Grubu Opinion Working Paper 257.

Md. 29 Çalışma Grubu Opinion Working Paper 152.

Md. 29 Çalışma Grubu Opinion Working Paper 74.

Md. 29 Çalışma Grubu Opinion Working Paper 108.

Md. 29 Çalışma Grubu Opinion Working Paper.rev01.

Md. 29 Çalışma Grubu Opinion Working Paper 153.

Md. 29 Çalışma Grubu, Opinion on Accountability 3/2010.

OECD, Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, Paris, Fransa 2013.

Veri Güvenliği Rehberi https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf Erişim Tarihi: 04.06.2020.

SEMPOZYUMLAR

BRAUN, A. Cihan, İşçilerin İşyerinde Video Kamerayla İzlenmesinin Kişisel Verilerin Korunması Hakkı ve Genel Kişilik Hakkı Çerçevesinde Değerlendirilmesi, Yeditepe Üniversitesi Hukuk Fakültesi 8-9 Aralık 2018 tarihli Avrupa ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Konulu Uluslararası Sempozyum, 2018.

ÖZGEÇMİŞ

Eğitim

- Türk Alman Üniversitesi; *2018-2020*
  Özel Hukuk Yüksek Lisans
- Universität Zürich; *2019-2020*
  Swiss-European Mobility Programme Değişim Öğrencisi
- İstanbul Bilgi Üniversitesi; *2012-2016*
  Hukuk Fakültesi Lisans
- Sankt Georg Avusturya Lisesi; *2017-2012*

İş Deneyimi

- İstanbul Barosu Avukatı; *2017*
- Muhtaranlar Avukatlık Ortaklığı; *2018*
  Avukat
- Türkekul Hukuk Bürosu; *2016-2017*
  Stajyer Avukat

Yabancı Diller

- İleri seviye İngilizce
- İleri seviye Almanca