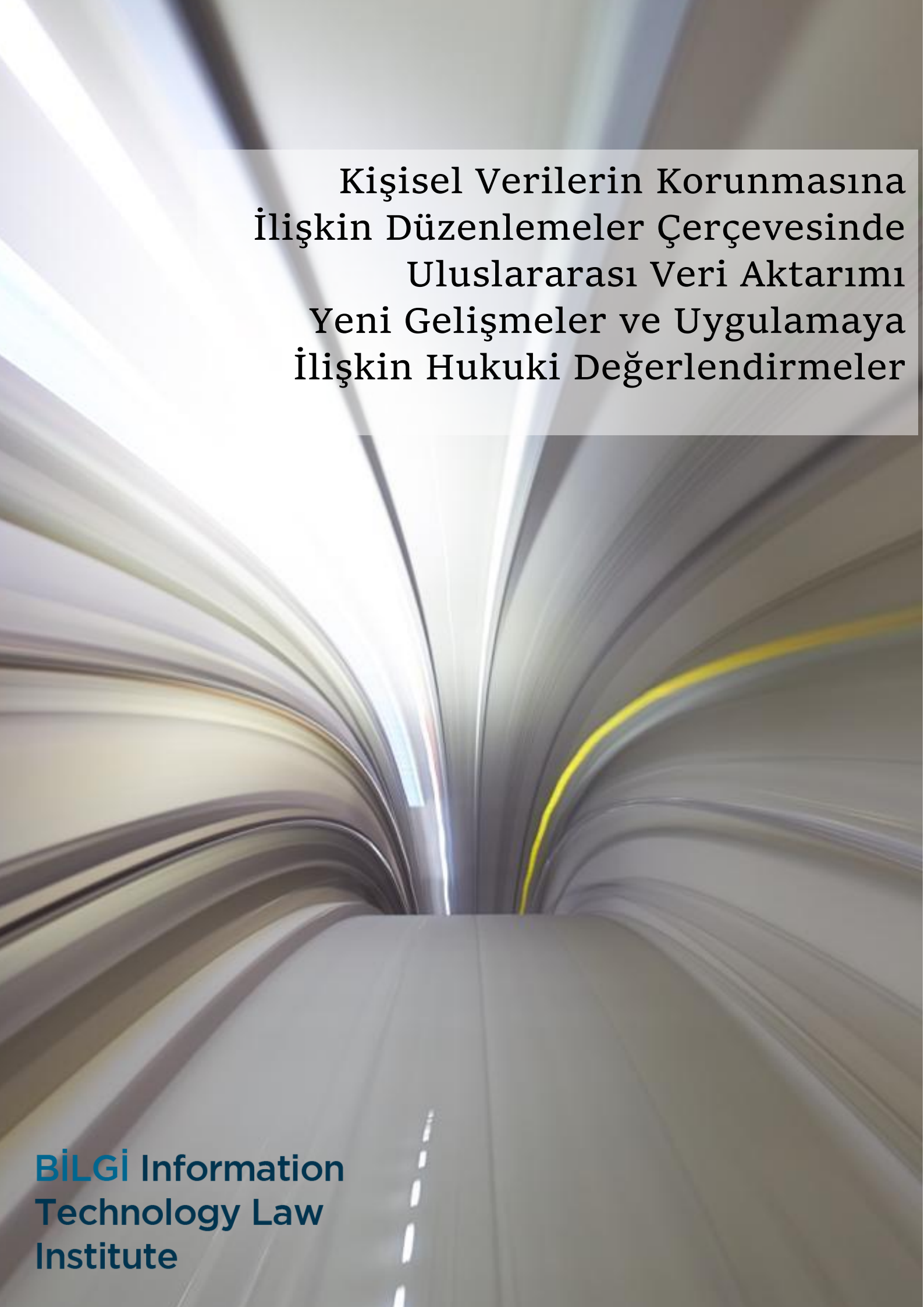


Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler

BİLGİ Information Technology Law Institute

BİLGİ Information Technology Law Institute

Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler

30.03.2020
İstanbul

Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı, Güncel Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler

İçindekiler

1. Sunuş

Bilgi ve iletişim teknolojileri alanında yaşanan baş döndürücü gelişmeler, daha önce var olmayan birçok yeni iş modelinin ve işbirliklerinin ortaya çıkmasına neden olmuştur. Yeni bir ekonomik modele işaret eden "veri temelli ekonomi" (*data driven economy*) kavramı ise, dünyadaki tüm ekonomik modellerin verinin daha iyi işlenmesi ve veriden maksimum derecede ekonomik fayda edilmesi esasına dayalı olması gerekliliğine işaret etmektedir.

Veriden değer yaratma zorunluğunun her geçen gün arttığı dünyada, bu ekonomik ve sosyal gerçeklikle bağdaşmayan, bunun uzağında kalan ve bunu engelleyen hukuki yorumlar, veri koruma hukukunun ana ekseni olan "kişiyi" koruma amacına hizmet etmekten çok; kişiyi ve veri işleyen kurumları ölçüsüzce sınırlandıran, yaratılabilecek değeri yok eden, dünya gerçeklerinden kopuk sonuçların ortaya çıkmasına neden olmaktadır.

Oldukça karmaşık iş modelleri ve teknolojiler hayatımızın içerisine girerken, bunların yaratmış olduğu etkileri hukuken yorumlama noktasında gerekli detaylara bakmadan; şekli hususlara odaklanıp, işin esasını kaçırdığımız durumlar söz konusu olabilmektedir. Kişisel verilerin korunması hukukuyla ilgili ülkemizde "uluslararası veri aktarımı" konusunda son dönemde yaşanan tartışmalar ve ortaya konan görüşler bunun tipik bir örneğidir. Bunun yanı sıra veri koruma hukukuyla ilgili Avrupa Birliğinde bu kadar zengin akademik ve hukuki kaynak olmasına rağmen bunlardan doğru şekilde istifade edememek, bu kaynaklarla Türk Hukukunu zenginleştirme – karşılaştırma çabası içerisine girememek de ayrıca değerlendirilmesi gereken bir durumdur.

Enstitümüz, kuruluş amacı doğrultusunda, ulusal ve uluslararası gelişme ve eğilimlere göre belirlediği çalışma alanlarında ülkemizde doğru akademik tartışma zemininin yaratılması için birçok çalışmada yapmış ve yapmaya devam etmektedir. Elinizdeki çalışma, bu misyonun bir gereği olarak kaleme almıştır. Bu çalışma ile "uluslararası veri aktarımı"; karşılaştırmalı hukuktaki mevzuat, yaklaşımlar, uygulama ve kaynaklar da irdelenerek mercek altına alınmaktadır. Bu çalışmada 6698 sayılı Kişisel Verilerin Korunması Kanunu[1]'nun mehaz Avrupa Birliği'ndeki düzenlemeler ve yorumları başta olmak üzere, ülkemiz içerisinde giderek derinleşen uluslararası veri transferi sorununa nasıl yaklaşılması gerektiğine dair hukuki çözüm önerileri sıralanmaktadır. Çalışmanın içerisinde aynı zamanda, Türk Anayasa Hukukunun öğretileri ile "uluslararası veri aktarımı" konusunu düzenleyen ve Türkiye'nin de tarafı olduğu, Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin sorunun çözümüne nasıl hizmet edeceğine dair hukuki yorumlar

[1] 6698 Sayılı Kişisel Verilerin Korunması Kanunu, *Resmi Gazete* 07.04.2016- 29677, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf.

da bulunmaktadır. Son olarak bu çalışma ile Enstitümüz, hukuk politikası gereği sorunun çözümü için atılması gereken adımlara ilişkin görüşlerini de ilgili tüm paydaşların dikkatine sunmaktadır.

Bu çalışmanın, ülkemizde kişisel verilerin yurt dışına aktarılması noktasında, veri koruması ve uluslararası hukukunun gereklerine uygun bir tartışma ve çözüm zemini yaratacağını ümit ediyoruz. Raporun Türk Hukuk öğretisine ve bu konuda ortaya konacak hukuki yorumlara katkıda bulunmasını dileriz.

Saygılarımızla,
İstanbul Bilgi Üniversitesi
Bilişim ve Teknoloji Hukuku Enstitüsü

2. Raporun Akademik Sentezi

Bu bölümde; raporda ortaya konulan hususların bir akademik sentezi, beş ana başlıkta soru cevap şeklinde okuyucunun dikkatine sunulmuştur:

İlk bölümde; uluslararası veri aktarımına ilişkin Türkiye'de uygulamadaki genel eğilim ve mevcut duruma yönelik tespitler ve değerlendirmeler ortaya konulmaktadır. İkinci bölümde ise; Avrupa Birliği Genel Veri Koruma Regülasyonu[2] ("**GDPR**") başta olmak üzere Avrupa Birliği ("**AB**", "**Birlik**" veya "**Avrupa Birliği**") eksenli olarak uluslararası veri aktarımına dair ortaya konulan hukuki yaklaşım irdelenmektedir. Üçüncü bölümde Türk Hukuku ile Avrupa Birliği Hukuku karşılaştırmalı olarak incelenmekte ve iki hukuk sistemi arasındaki fark yaratan noktalara işaret edilmektedir. Dördüncü bölümde uluslararası veri aktarımına yönelik dijital çağın, uluslararası hukukun ve Türk Hukukunun gereklerine uygun akademik sentezlerimiz ve bu konuda ülkemizde mevcut hukuk kaynakları ekseninde uygulanması gereken hukuki çerçeveyle ilgili önerilerimiz ortaya konulmaktadır. Beşinci ve son bölümde ise; hukuk politikası itibariyle ülkemizde uluslararası veri aktarımına yönelik sürdürülebilir ve doğru hukuk kaynaklarına dayalı hukuk politikası enstrümanları ve atılacak adımların ne olması gerektiğine dair önerilerimiz sıralanmaktadır.

Bölüm 1 – Türkiye'de Kişisel Verilerin Yabancı Ülkelere Aktarımına Yönelik Uygulamadaki Genel Eğilime ve Duruma Yönelik Tespitler

Uygulamadaki Genel Eğilime Göre Kişisel Verilerin Yabancı Ülkelere Aktarılması Şartları Nelerdir?

Uygulamadaki genel eğilime göre; Kişisel Verilerin Korunması Kanunu'nun ("**KVKK**") 9. maddesinin 1-4. fıkralarına göre kişisel veriler ancak aşağıdaki şartların varlığı halinde yurtdışına aktarılabilir.

- İlgili kişinin "açık rızası"

- İlgili kişinin açık rızası yok ise;

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, *Official Journal of the European Union* L 119/1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

- KVKK'nın 5. maddesinin ikinci fıkrası ile 6. maddesinin üçüncü fıkrasında belirtilen şartlarından birinin varlığı ile

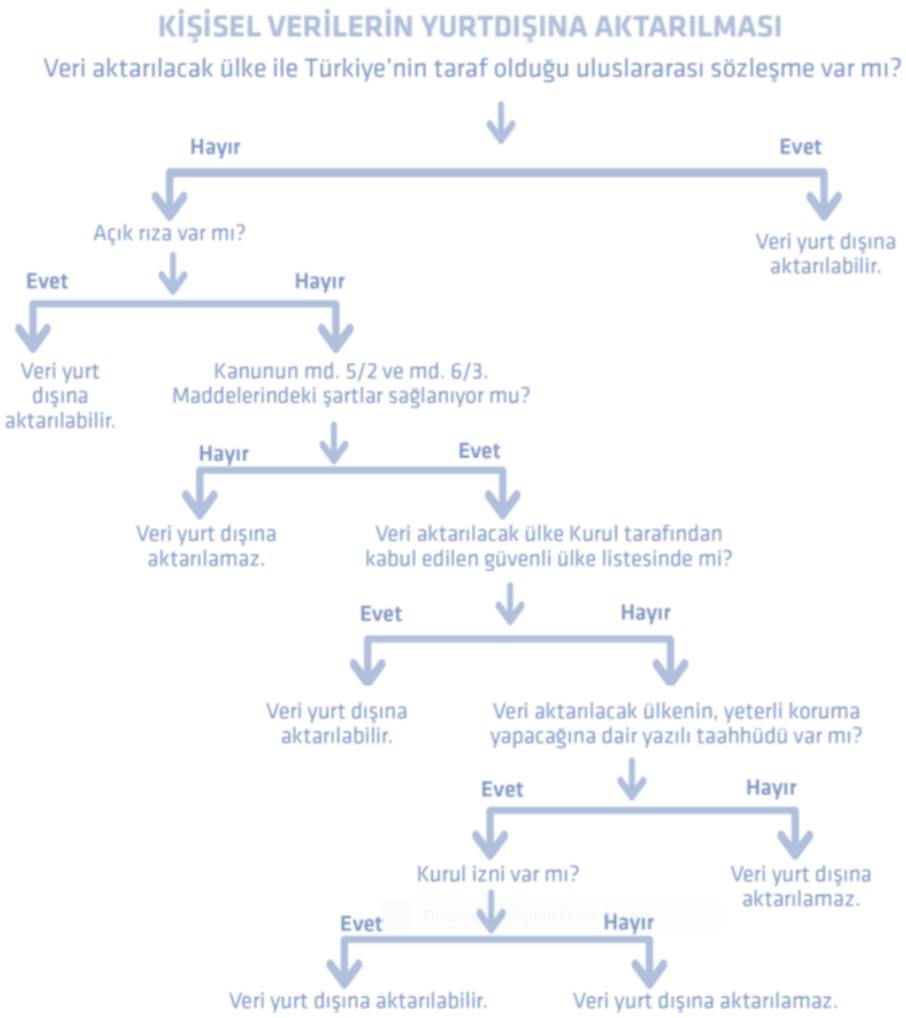
  - Kişisel verilerin aktarılacağı yabancı ülkede "yeterli korumanın" bulunması

  - Eğer kişisel verilerin aktarılacağı ülkede "yeterli koruma" yok ise; Türkiye'deki ve ilgili yabancı ülkedeki **veri sorumlularının** yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun ("**Kurul**") izninin bulunması.

Kişisel Verileri Koruma Kurumu'nun Uygulamadaki Genel Eğilime Yönelik Yaklaşımı Nasıldır?

Kişisel Verileri Koruma Kurumu'nun ("**Kurum**"), KVKK'nın 9. maddesinin uygulanmasına yönelik olarak, yurt dışına kişisel verilerin aktarılması konusunu "Kişisel Verilerin Yurtdışına Aktarılması" isimli rehberde[3] şematize ettiği görülmektedir. İlgili rehberin 6. ve 7. sayfalarında yer alan şema aşağıda belirtilmektedir.

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



Kurum'un ilgili rehberde şematize ettiği şekil dikkate alındığında; uygulamadaki genel eğilimin aksine, yurt dışına kişisel veri aktarımında öncelikle konuyla ilgili bir ***uluslararası sözleşme olup olmadığına baktığı*** görülmektedir. Bu yaklaşım; usulüne uygun olarak Türk Hukukuna aktarılan temel hak ve özgürlükleri düzenleyen uluslararası sözleşmelerin, aynı konuyu düzenleyen iç hukukumuzdaki yasalardan evleviyetle dikkate alınacağı, ilgili uluslararası sözleşme ile iç hukuktaki düzenleme çatıştığı takdirde uluslararası sözleşme hükümlerinin esas alınacağına yönelik Anayasa Hukuku prensipleriyle ve Anayasamızın bu hususu düzenleyen 90. maddesinin beşinci fıkrasının amir hükmüyle de uyumludur.

Her ne kadar yukarıdaki şekilde *"yeterli korumaya sahip olmayan"* ülkeye aktarımda KVKK'nın 9. maddesinin ikinci fıkrasının (b) bendinin düzenlediği şekilde veri sorumlularından değil de, aktarılacak ülkeden taahhüt alınacağı belirtilse de; 9. madde hükmünde mevcut olmayan bu durumun Kurum tarafından talep edilmediği, sehven tabloya bu şekilde işlendiği düşünülmektedir.

Yurt Dışına Kişisel Veri Aktarımını Düzenleyen "Diğer Kanun Hükümlerine" İlişkin Olarak Uygulamadaki Genel Eğilimin Yaklaşımı Nasıldır?

Uygulamadaki genel eğilim tarafından, KVKK'nın 9. maddesinin altıncı fıkrasında yer alan *"Kişisel verilerin yurtdışına aktarılmasına yönelik diğer kanunlarda yer alan hükümler saklıdır"* hükmünün dikkate alınmadığı görülmektedir. Diğer kanun hükümleriyle, uygulamadaki genel eğilimin evleviyetle uygulanmasına yönelik görüş belirttiği KVKK'nın 9. maddesinin birinci fıkra hükmü arasındaki ilişki dikkate alındığında;

- Hukuki yorum tekniği bakımından özel kanun – genel kanun ilişkisi ile mi konuya yaklaşılacağı,

- KVKK'nın temel hak ve hürriyetleri düzenleyen bir kanun olduğundan bahisle, bu neviden olmayan diğer kanunlara göre evleviyetle uygulanması mı gerekeceği; bu nedenle de Kurul'un bu konuya "temel hak ve özgürlükleri" koruma penceresinden yaklaşarak, ilgili KVKK hükmünün ne şekilde somut olaya uygulanacağını belirleyeceği,

- KVKK'nın 9. maddesinin bu konuda bir farklılaşma getirmeden diğer kanun hükümlerini saklı tutmasından bahisle "lafzi" yorumla, diğer kanunlardaki hükümlerin herhangi bir değerlendirme yapılmadan öncelikle uygulanması mı gerektiği,

konusu açık değildir. Bu konular ne doktrinde ne uygulamadaki genel eğilimde ne de Kurum'un yayınladığı belgelerde açıklığa kavuşturulmuştur.

Kanaatimizce; yurt dışına veri aktarımını düzenleyen "diğer kanun hükümleri";

- Öncelikli uygulanmalıdır ve bu konuları düzenleyen mevzuatın, ilgili verilerin yurt dışına aktarımı için Kurum'un ilgili rehberde kamuoyuna açıkladığı şemada, hiyerarşik olarak uluslararası sözleşmelerin altında gerekli hukuki şartı sağlayan bir unsur olarak değerlendirmesi gerektiğini düşünmekteyiz.

- Bununla birlikte KVKK'nın temel hak ve hürriyetilerin uygulanmasını düzenleyen bir nitelikte olduğundan bahisle, Kurul'un bu neviden hukuki şarta dayalı olarak yapılacak yurt dışına aktarımda, KVKK'nın yurt dışına aktarımın hukuki şartları, ilgili kişilerin temel hak ve hürriyetlerini daha kapsayıcı bir çerçevede himaye ediyorsa, bu şartlara dayalı olarak da aktarılması gerekliliğine karar verebilir diye düşünmekteyiz. Kurul'un bu yetkisini KVKK'nın 9. maddesinin beşinci fıkrasına dayalı olarak yurt dışına aktarım konusunun düzenlendiği, ilgili

kanunun uygulanması ile görevli kamu kurum ve kuruluşuna danışarak kullanması yerinde olacaktır.

- Ayrıca Kurul'un bu neviden hukuki şarta dayalı olarak yapılacak aktarımlarda; KVKK'nın 22. maddesinin birinci fıkrasının (a)-(e) ve (f) bentleri uyarınca bu aktarımlara uygulanacak ilgili kişinin temel ve hak ve hürriyetlerini daha kapsayıcı bir şekilde koruyacak güvenlik tedbirlerinin uygulanması zorunluluğunu da getirebileceğini düşünüyoruz.

Yurt Dışına Kişisel Veri Aktarımını Düzenleyen Hukuki Şartlar Arasında Sayılan "Açık Rıza"ya Dayalı Olarak Aktarımın Değerlendirilmesine Yönelik Yaklaşım Nasıldır?

Uygulamadaki genel eğilim; yurt dışına kişisel veri aktarımında, 9. maddenin lafzından hareketle, "açık rıza"nın öncelikle uygulanması gereken hukuki şart olduğunu ileri sürmektedir. Ayrıca; hiyerarşik olarak da açık rızanın öncelikle aranması gereken bir hukuki şart olduğuna işaret etmektedir.

Aynı lafızla kaleme alınan KVKK'nın 5. ve 6. maddesinin yorumlanmasında Kurul; mehaz Avrupa Birliği düzenlemeleri ve uygulamalarını esas alarak, açık rızanın hukuki şart olarak müstakil bir şekilde, diğer hukuki şartların olmadığı durumlarda dayanılması gerekliliğine işaret etmiş; hiyerarşik olarak açık rızaya dayanmayı en son kertede değerlendirilmesi gereken bir husus olarak kabul etmiştir[4]. Kurul, başka hukuki işleme şartları var iken, açık rızaya dayalı hukuki şartla kişisel veri işlemenin, dürüstlük kuralı ve açık rızaya yüklenen fonksiyonlarla örtüşmeyeceğini değerlendirmiştir[5]. Kurul'un yorum tekniğiyle geliştirdiği bu yaklaşıma katıldığımızı belirtmek isteriz.

Kişisel veri işleme şartlarına yönelik olarak, açık rızanın kullanımında Kurul'un getirdiği bu çağdaş yaklaşımın, yurt dışına veri aktarımında neden takip edilmediği ve bu konuda suskun kalındığı da bir soru işaretidir. Hiyerarşik olarak açık rızanın hukuki şartlarındaki sıralamasının dışında özellikle yurt dışına veri aktarımda bu konuya ilişkin alınacak açık rızanın, "bilgilendirmeye dayalı olma" ve "belirli bir konuya ilişkin" olma unsurlarının mehaz düzenleme ve uygulama örneklerinde olduğu gibi; ilgili

[4] Kurul, 2 Ağustos 2018 tarihinde yayımlanmış olan "Açık Rızanın Hizmet Şartına Bağlanması" başlıklı karar özetinde ("Açık Rızanın Hizmet Şartına Bağlanması," Kişisel Verileri Koruma Kurumu, erişim 15 Şubat, 2020. https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi.) açıkça *"Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği"* ifadesine yer vererek bu hususa netlik kazandırmıştır. Nitekim aynı husus, Kurum'un "Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi"nde ("Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi," Kişisel Verileri Koruma Kurumu, erişim 15 Şubat, 2020. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf.) de *"Kişisel veri işleme, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmamaktadır. Veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacaktır."* denilerek belirtilmiştir.

[5] Kişisel Verileri Koruma Kurumu- "Açık Rızanın Hizmet Şartına Bağlanması."

kişiyi daha etkili korunmak adına farklı biçimlerde ortaya konulabileceği gerçeğine de[6] ne uygulamadaki genel eğilim tarafından ortaya konulan görüşlerde ne de Kurul'un bu konuda ortaya koyduğu dokümanlarda rastlanmıştır.

Yurt Dışına Kişisel Veri Aktarımının Niteliğinin ve Amacının Uygulamaya Yön Vermesine Yönelik Uygulamadaki Genel Eğilimin Yaklaşımı Nasıldır?

Yurt dışına kişisel veri aktarımı konusunda bu aktarımın tek seferlik mi, sürekli mi olduğu hususu ile aktarımın amacının ne olduğunun, bu aktarıma uygulanacak hukuki koruma tedbirlerinin şekillenmesinde çok önemli bir değeri vardır. Mevzuatımızda bu yönde bir açıklık mevcut değildir. Ancak bu yönde yapılacak değerlendirmelerin, ilgili kişinin gereği gibi korunmasında bu aktarıma dayalı olarak ortaya çıkabilecek risklerin yönetiminde ve her şeyden önemlisi de aktarımın niteliğine göre farklı hukuki şartların uygulanmasının temininde çok önemli bir yeri vardır. Uygulamadaki genel eğilimde bu yönde herhangi bir değerlendirme yapılmadığı da gözlemlenmiştir.

Yurt Dışı Kişisel Veri Aktarımında Hiyerarşik Olarak Uygulanması Öngörülen Hukuki Şartların, Karşılaştırmalı Hukuktaki Emsalleri ile Değerlendirilerek, Hangi Hukuki Şarta Daha Yoğun Dayalı Olarak Veri Aktarımı Yapıldığına Yönelik Uygulamadaki Genel Eğilimin Yaklaşımı Nasıldır?

Uygulamadaki genel eğilim ve Kurum'un bu zamana kadarki açıklamalarında bu yönde herhangi bir değerlendirme yapılmadığı gözlemlenmiştir. Burada yapılacak tespitler, hukuk politikası bakımından yurt dışına veri aktarımında hiyerarşik olarak dikkate alınacak hukuki şartların ne şekilde sıralanması gerektiğine dair doğru görüşü oluşturma bakımından değerli olacaktır.

Bu görüş hem maddi hukuk değişiklikleri hem de mevcut mevzuatın amaçsal olarak yorumlanmasında yol gösterici olacaktır. Bu çerçevedeki görüşlerimiz aşağıda daha detaylı olarak belirtilmektedir.

Yeterli Korumaya Sahip Olmayan Ülkelere Kişisel Veri Aktarımında Aranması Öngörülen Kurul İzninde Aktarımın Nitelik, Nicelik ve Amacına Göre Bir Farklılaşma Yapılmış Mıdır?

[6] "International Transfers- Exception 1. Has the individual given his or her explicit consent to the restricted transfer?," ICO, erişim 3 Şubat 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.
Aynı şekilde: "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679," son güncelleme 25 Mayıs 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

Bu yönde KVKK'nın 9. maddesinde herhangi bir farklılık öngörülmediği gibi, Kurum'un yayınladığı belgelerde ve uygulamadaki genel eğilim çevrelerinde yapılan tartışmalarda da, bu eksikliğin yaratacağı negatifliklerle ilgili herhangi bir görüş ortaya konulmamıştır.

Oysa bu farklılıklar, mehaz Avrupa Birliği düzenlemeleri ve uygulamaları bakımından[7], özellikle Kurul izninin arandığı durumların tespitinde çok önemli bir kriter ve değer oluşturmaktadır. Bu kriterlerin önemi ve değerine çalışmamızın ilerleyen bölümlerinde değinilecektir.

Yeterli Korumaya Sahip Olmayan Ülkelere;

- **Veri İşleyenden – Veri İşleyene ya da Veri Sorumlusundan – Veri İşleyene Olan Aktarımlarda, Veri İşleyenlerden Bir Taahhüt Alınıp Alınmayacağına;**

- **Yeterli Korumaya Sahip Olmayan Ülkede Yerleşik Veri Sorumlusundan - Veri İşleyene ya da Veri İşleyenden – Veri İşleyene Yapılan Aktarımların Kurul İznine Tabi Olup Olmayacağına**

Dair Değerlendirme Yapılmış Mıdır?

Bu konuya ilgili çevrelerde oluşan görüşlerde herhangi bir açıklık getirilmediği gibi, Kurum'un yayınladığı belgelerde ve uygulamadaki genel eğilim çevrelerinde yapılan tartışmalarda da, bu eksikliğin yaratacağı negatifliklerle ilgili herhangi bir görüş ortaya konulmamıştır.

Kurum, yeterli korumaya sahip olmayan ülkede yerleşik veri işleyene, Türkiye'de yerleşik olan veri sorumlusundan yapılacak aktarımların; KVKK'nın 9. maddesinin ikinci fıkrasının (b) bendi kapsamındaki yükümlülüklere ve Kurul'un iznine tabi olacağına yönelik bir izlenim yaratmıştır[8]. Bu izlenimi; Kurul'un veri sorumlusundan veri işleyene yapılan aktarımlarda kullanılmak üzere, KVKK'nın 9. maddesinin ikinci fıkrasının (b) bendi kapsamında veri sorumlusunca hazırlanacak taahhütnamede bulunması gereken asgari unsurlar adı altında yayınladığı örnek taahhütname metni ve bu hukuki dayanak noktasına atıfta bulunduğu internet sitesi üzerindeki açıklamadan edinmek mümkündür[9]. Oysa KVKK'nın 9. maddesinin ikinci fıkrasının (b) bendi, Türkiye'deki veri sorumlusundan yeterli korumaya sahip olmayan ülkede yerleşik veri sorumlusuna yapılan aktarımları, bu aktarımlara taraf

[7] GDPR Madde 49 ve GDPR Giriş Hükmü 113.
[8] "Yurtdışına Aktarım," Kişisel Verileri Koruma Kurumu, erişim 12 Ocak 2020, https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim.
[9] Kişisel Verileri Koruma Kurumu- Yurtdışına Aktarım."

olan veri sorumlularının taahhütname vermesini ve bu neviden olan aktarımları Kurul iznine tabi kıldığını hüküm altına almıştır. İlgili madde aşağıdaki şekildedir.

"…Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki ***veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri*** *ve* ***Kurulun izninin bulunması…"***

Kurum internet sitesinde yayınladığı taahhütnamelerde; veri sorumlusundan veri işleyene olan kısmını Kanunun 9. maddesinin ikinci fıkrasının (b) bendi ile 12. maddesinin ikinci fıkrasına dayandırmıştır. Kanaatimizce bu hukuki temellendirme hatalıdır. Zira madde metninde yükümlülük sahibi olarak açıkça *veri sorumlulularından veri sorumlusuna olan aktarımlardan* bahsedilmektedir. Kurum'un, veri işleyene bu noktada veri sorumlusu üzerinden yükümlülük getirmesinin dayanak maddesi, Kurul'un yetkilerini düzenleyen KVKK'nın 22. maddesinin birinci fıkrasının (a)-(e) ve (g) bendleri olmaldır. Böyle bir gerekçelendirme Kurul'a veri sorumlusundan veri işleyene olan veri aktarımlarında 9. madde hükmü dışında farklı usul ve esaslarla hareket etme imkanı da tanıyacaktır.

Bir diğer konu da; KVKK'nın lafzından hareketle Türkiye'de yerleşik veri işleyenin yeterli korumaya sahip olmayan ülkedeki veri işleyene yapacağı kişisel veri aktarımlarının, 9. maddenin himayesi içerisinde olup olmayacağı sorunsalıdır. Lafzi yorum ile bu neviden aktarımların 9. madde kapsamı içerisinde olmayacağı değerlendirilebilir. Ancak bu değerlendirme ilgili kişileri, KVKK'nın yabancı ülkeye veri aktarımına yönelik koruma mekanizmalarının dışında bırakacaktır. Bu noktada bu neviden veri aktarımları KVKK'nın 22. maddesinin birinci fıkrasının (a) ve (e) bendlerinin Kurul'a verdiği yetkiye dayalı olarak düzenlenebilir, bu çerçevede ilgili kişiler için bir hukuki koruma zemini tesis edilebilir.

Yeterli Korumaya Sahip Ülkelerin Tespitinde Kanunen Dikkate Alınan Kriterlerle, Yeterli Korumaya Sahip Olmayan Ülkelerdeki Yerleşik Veri Sorumlusuna Kişisel Verilerin Aktarılmasında Kurul'un Vereceği İznin Dayandığı Kanuni Kriterlerin Aynı Olması Sorunsalına Uygulamadaki Genel Eğilimin Yaklaşımı Nasıldır?

Bu konuya ilgili çevrelerde oluşan görüşlerde herhangi bir açıklık getirilmediği gibi; Kurum'un yayınladığı belgelerde de bu eksikliğin yaratacağı negatifliklerle ilgili herhangi bir görüş ortaya konulmamıştır.

KVKK, Kurul'un;

- 9. maddenin dördüncü fıkrasında yabancı ülkede yeterli koruma bulunup bulunmadığına,

- 9. maddenin ikinci fıkrasının (b) bendi uyarınca aktarımı gerçekleştiren veri sorumlusuna izin verilip verilmeyeceğini,

değerlendirme noktasında dikkate alacağı kriterleri; herhangi bir ayrım gözetmeksizin her iki konu için de aynı şekilde belirlemiştir. Bu durum müessese itibariyle Kurul'un, birbirinden farklı iki konuyu aynı kanuni kriterlerle değerlendirme zarureti içerisinde kalmasına sebebiyet vermektedir. Örneğin; KVKK'nın 9. maddesinin dördüncü fıkrasının (c) ve (d) bentleri yeterli koruma kararında değil, Avrupa Birliği Hukukunda[10] spesifik olarak ilgili olaya özel kişisel veri aktarımı olarak tanımlanan durumlarda dikkate alınması gereken kriterler olarak değerlendirilmektedir. Aynı şekilde; KVKK'nın 9. maddesinin dördüncü fıkrasının (a), (b) ve (ç) bentleri ise spesifik olarak ilgili olaya özel kişisel veri aktarımı noktasında tanımlanan durumlarda değil, yeterli korumaya sahip ülkelerin tespiti kararlarında dikkate alınması gereken kriterler olarak değerlendirilmektedir. [11]

Her ne kadar Kurum, yayınlamış olduğu *"Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler"* dokümanı ile[12] kanuni olarak yaratılan bu uygunsuzluğu, yeterli korumaya sahip ülkelerin belirlenmesi penceresinden bir nebze olsun gidermeye çalışsa da; Kurul'un veri sorumlusuna vereceği izin bakımından müessesenin niteliğine göre hangi kriterlere dayalı olarak değerlendirme yapacağı konusu yine de belirsizliğini korumaktadır. Bu uygunsuzluk durumu temelde KVKK'nın 9. maddesinin yazımıyla ilgili sorunsaldan doğsa da; bu sorunun Avrupa Birliği karşılaştırmalı olarak, özellikle Avrupa Birliği hukukunda ilgili olaya özel kişisel veri aktarımı yönüyle ayrımlaştırma yapılarak çözümüne ilişkin hukuksal yorum olanaklarının neler olduğu bu çalışmanın ilerleyen bölümlerinde ele alınacaktır.

[10] GDPR Giriş Hükmü 113, açıkça veri sorumlusunun kişisel verilerin niteliği ve önerilen işleme faaliyet ya da faaliyetlerinin amacı ve süresinin yanı sıra verinin kaynağı olan ülke ile verinin gönderildiği ülkenin durumunu özellikle değerlendirmesini ve gerçek kişilerin kişisel verilerinin işlenmesine ilişkin temel hak ve özgürlüklerini korumak adına uygun güvenlik tedbirlerini almasını öngörmektedir.

[11] "Working document on Adequacy Referential, WP 254 Rev.01," Article 29 Working Party, son güncelleme 2 Şubat, 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
Aynı şekilde GDPR, Giriş Hükmü 104.

[12] "Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler," Kişisel Verileri Koruma Kurumu, erişim 12 Ocak, 2020, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/60d987a1-ba9d-4285-a8ce-c3f41ff4e47f.pdf.

KVKK'nın 9. Maddesinin Dördüncü Fıkrasında Sıralanan Kanuni Kriterlerin Varlığını Değerlendirme Noktasında Kurul'un Takdir Yetkisi Olup Olmadığına İlişkin Uygulamadaki Genel Eğilimin Yaklaşımı Nedir?

Bu konuya ilgili çevrelerde herhangi bir açıklık getirilmediği gibi, Kurum'un yayınladığı belgelerde bu eksikliğin yaratacağı negatifliklerle ilgili herhangi bir görüş de ortaya konulmamıştır.

Kanaatimizce; ilgili kanuni kriterler Kurul'un değerlendirme noktasında mutlaka dikkate alması gereken kriterler olup, varlığının tam ve mükemmel şekilde olmasının aranması noktasında Kurul'a bir mükellefiyet yüklememektedir. Kurul her somut durumun şartlarına göre bu kriterleri de göz önüne alarak ve bu kriterleri değerlendirerek bağımsız bir şekilde kararını verecektir. Örneğin yeterli korumaya sahip olmayan ülkeye kişisel veri aktarımında ilgili ülke ile Türkiye arasında çoğu zaman bir karşılıklılık ilişkisi olmayacaktır. Bu durumda bu kanuni kriterin varlığı arandığında hiçbir şekilde yeterli korumaya sahip olmayan ülkeye veri aktarımına izin verilmeyeceği anlamı çıkacaktır. Bu durum ise; ilgili madde ile getirilmeye çalışılan değerlendirme zeminini baştan yok edecek, madde metnindeki kriterlerin somut olayın şartlarına göre yorumlanması konusundaki Kurul'un takdir yetkisini de ortadan kaldıracaktır.

KVKK'nın 9. Maddesinin Üçüncü Fıkrasında "Yeterli Korumanın Bulunduğu Ülkelerin Kurulca Belirlenerek İlan Edilmesi" Kurul'a Verilen Bir Yetki mi Yoksa Kurul'a Verilen Bir Görev mi Olduğu Noktasında Uygulamadaki Genel Eğilimin Yaklaşımı Nasıldır?

Bu konuya ilgili çevrelerde oluşan görüşlerde herhangi bir açıklık getirilmediği gibi, Kurum'un yayınladığı belgelerde de bu konuda herhangi bir görüş ortaya konulmamıştır. Kanaatimizce; KVKK'nın 9. maddesinin üçüncü fıkrasında düzenlenen konu, Kurul'un somut durum ortaya çıktığı takdirde müdahale etmesini gerektiren ve bu somut durumla alakalı yerine getirmesi gereken görevlerin oluşumuna sebebiyet veren bir kamusal yetkiyi değil, *Kurul'un muhik bir neden olmadıkça gecikmeksizin yerine getirmesi gereken bir kamusal görevin varlığına işaret etmektedir*. Mehaz düzenleme ve bu konudaki diğer ülke uygulamaları da takip edildiğinde, yeterli korumaya sahip olan ülkeler tespit edilip ilan edildikten sonra, uluslararası veri aktarımına ilişkin diğer hukuki şartlar bu

kararın çevresine oturmaktadır. Avrupa Birliği hukukuna göre[13]; hiyerarşik olarak uluslararası sözleşmelerden sonra[14], uluslararası veri aktarımına uygulanacak en önemli hukuki şart olan *"yeterli korumaya sahip olan ülkelerin"* tespiti kararı verilmeden, hukuken doğru ve sürdürülebilir bir uluslararası veri aktarımı rejimi tesis edilememektedir. Aynı anlayış ve yaklaşımın ülkemiz bakımından da geçerli olduğu söylenebilir. Kısaca kanaatimize göre; Kurul kanuni görevi olan yeterli korumaya sahip olan ülkeleri belirleyip ilan etmeden, *"yeterli korumaya sahip olmayan"* ülkeler tespit edilemeyecektir.

Bölüm 2 – Avrupa Birliği Hukukuna, Özellikle Genel Veri Koruma Regülasyonu'na (General Data Protection Regulation – GDPR) Göre Kişisel Verilerin Uluslararası Aktarımına Yönelik Hukuki Çerçeve

GDPR'ın ve Avrupa Birliği Hukukunun Kişisel Verilerin Uluslararası Aktarımı Konusunda Öngördüğü Rejim Nedir?

GDPR kapsamında uluslararası veri aktarımı iki adımda ele alınmaktadır:

İlk adımda;

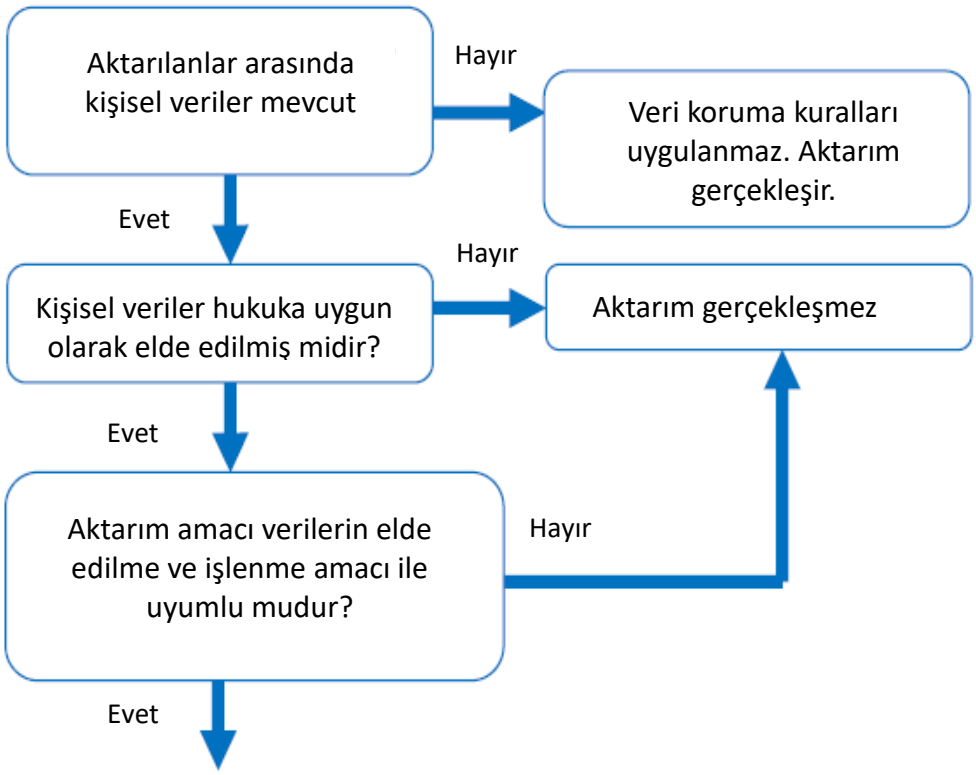
GDPR uyarınca kişisel veri aktarımı gerçekleştirilmeden önce ilk olarak aktarıma konu kişisel veriler özelinde aşağıdaki hususların tespiti sağlanır:

(i) Hukuka uygun olarak elde edilmiş ve işlenmiş midir?

(ii) Veri aktarım amacı hukuka ve verilerin elde edilme ve işlenme amacı ile uyumlu mudur?

[13] European Commission, Communication from the Commission to the European Parliament and the Council-Exchanging and Protecting Personal Data in a Globalised World (Brussels: 2017), S.4-5.
[14] GDPR – Giriş Hükmü 105.

İlk adımın şeması yukarıda belirtildiği şekildedir.[15]



Yukarıdaki aşamalardan sonra ikinci adıma geçilmektedir.

İkinci adımda; Birinci adım doğrultusunda gerekli koşulları sağlayan veri aktarım faaliyetleri için aşağıdaki hukuki şartların varlığının tespiti sağlanır:

(i) Aktarım yeterlilik (*adequacy*) kararının verildiği *yeterli korumayı haiz olan ülkeye (güvenli ülkeye)* mi yapılmaktadır?

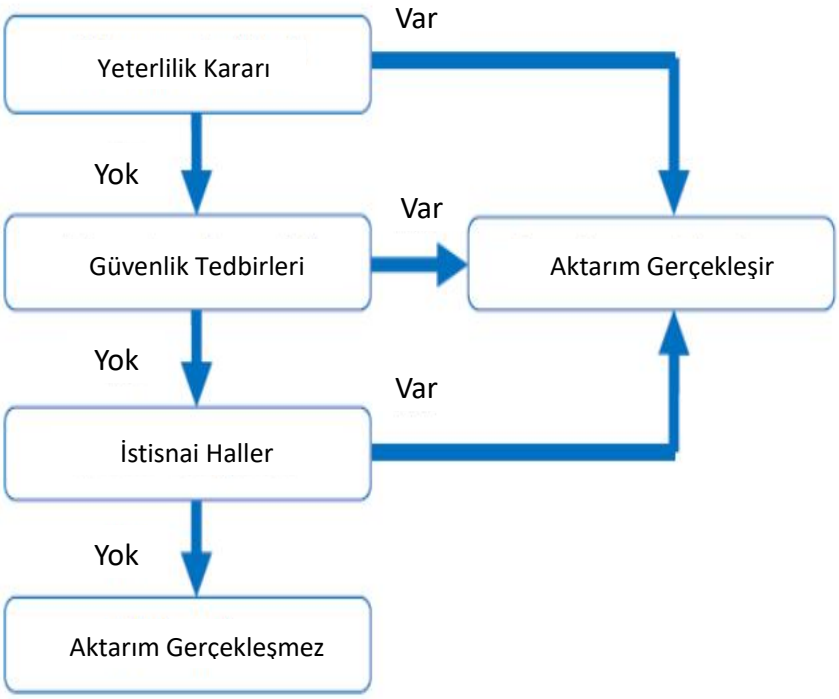
(ii) Aktarımın yapıldığı ülke güvenli ülke değilse, *güvenlik tedbirleri* uygulanmakta mıdır?

(iii) Aktarımın yapıldığı ülke güvenli ülke değilse ve güvenlik tedbirleri de uygulanmamakta ise *istisnai hallerden* birinin kapsamında değerlendirilebilecek midir?

İkinci adımın şeması aşağıda belirtildiği şekildedir[16]:

[15] "International Transfers," European Data Protection Supervisor, erişim 14 Ocak, 2020, https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en.

[16] EDPS- "International Transfers."



GDPR'a Göre Kişisel Verilerin Uluslararası Aktarımı Konusunda Dayanılan Hukuki Şartlar Yönünden Bir Hiyerarşik İlişki Var Mıdır?

Yukarıdaki başlıkta ele alınan ikinci adımda belirtilen hukuki şartlar hiyerarşik olarak belirtilmiştir. Bir başka deyişle hiyerarşik olarak üstte olan hukuki şart sağlandığı takdirde, alttaki hukuki şarta başvurulmamaktadır. Örneğin; yeterlilik kararı olan ülkeye aktarım gerçekleşiyorsa, güvenlik tedbirleri ve istisna başlığı altında listelenen hukuki şartlar uluslararası veri aktarımında dayanak konusu yapılmamaktadır. Yeterlilik kararının olmadığı bir ülkeye veri aktarımı yapılıyorsa, hiyerarşik olarak öncelikle güvenlik tedbirlerinin varlığı aranmaktadır. Güvenlik tedbirlerinin alınma imkanı var ve bu tedbirler alınmış ise, istisna içerisindeki hukuki şart uygulama konusu yapılmamaktadır.

GDPR'a Göre Yeterlilik Kararı Alma ve Bu Konuda Uygulanan Hukuki Çerçeve Nasıldır?

GDPR'ın 45. maddesine göre; Avrupa Birliği Komisyonu ("**Komisyon**"), GDPR'ın sağlamış olduğu korumaya eşdeğer bir korumanın AB üyesi olmayan devletçe sağlandığına dair belirlemeyi, "Yeterlilik Kararı" (*Adequacy Decision*) olarak anılan kararla gerçekleştirmektedir. Bu karar, KVKK'nın 9. maddesinin üçüncü fıkrası uyarınca Kurul tarafından alınan ve ilan edilen *"yeterli korumaya sahip olan ülke"* kararı ile eş değerde bir karardır.

Bu yeterlilik kararı tüm Avrupa Ekonomik Alanı ("**AEA**") ülkeleri için bağlayıcı olup Komisyon'un yeterli olarak belirlediği ülkelere veri aktarımı yapılmasına imkân verir. GDPR'a göre AB üyesi devletlerin müstakil olarak yeterlilik kararı alma yetkileri bulunmamaktadır.

Yeterlilik kararı iki şekilde ortaya konabilmektedir. İlki tam yeterlilik kararı ikincisi ise kısmı yeterlilik kararıdır.

Tam Yeterlilik Kararı (*Full Adequacy Decision*):

Komisyon'un bir devletin tamamen yeterli korumayı sağladığına dair verdiği karar, bu neviden alınan bir yeterlilik karardır. Örneğin, bu konuda en güncel yeterlilik kararı Japonya için verilmiştir. Komisyon tarafından tam yeterli olarak kabul edilen ülkelere[17] yapılan veri aktarımları AB üyesi bir ülkeye yapılıyormuş gibi kabul görmektedir.

Kısmi Yeterlilik Kararı (*Partial Adequacy Decision*)

Komisyon, ilgili devletin sadece belirli bir sektörü ya da bölgesinin veya bir uluslararası kurum veya kuruluşun yeterli korumayı sağladığına dair kararlar verilebilmekte olup bunlar kısmı yeterlilik olarak adlandırılmaktadır.

Örneğin, Amerika Birleşik Devletleri'nin, *Privacy Shield* ("**Gizlilik Kalkanı**") nezdinde almış olduğu yeterlilik kararı kısmi bir yeterlilik kararıdır. Gizlilik Kalkanı'na ilişkin detaylara "Gizlilik Kalkanı (EU-U.S. Privacy Shield Framework)" başlığında yer verilmiştir.

Avrupa Birliği mevzuatında Komisyon, AEA üyesi olmayan ülkelerin kişisel verilere ilişkin "yeterli korumayı" sağlayıp sağlamadığına karar veren otorite olarak belirlenmiştir[18]. Komisyon ilgili ülkelerin yeterli korumayı sağlayıp sağlamadığına yönelik belirlemeyi "yeterlilik kararı" olarak anılan kararla gerçekleştirmektedir. Komisyon tarafından verilen bir yeterlilik kararı tüm AEA ülkeleri için bağlayıcı olup Komisyon'un yeterli olarak belirlediği ülkelere (istisnalar söz konusu olmakla beraber) sınırlandırılmamış bir şekilde veri aktarımı yapılmasına imkân verir. Zaman geçtikçe Komisyon'un vermiş olduğu yeterlilik kararları bir "beyaz liste" oluşturmuştur. Bu beyaz listede AB ile denk bir koruma sağladığı belirlenmiş olan ülkelere yer verilmiştir[19]. Yeterlilik kararının alınması için;

[17] Komisyon tarafından yeterlilik kararı verilmiş ülkeler mevcut durumda Amerika Birleşik Devletleri (Gizlilik Kalkanı ile sınırlı olarak), Andorra, Arjantin, Faroe Adaları, Guernsey, İsrail, İsviçre, Japonya, Jersey, Kanada (ticari kuruluşlar için), Man Adası, Uruguay, Yeni Zelenda olup, güncel listeye (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en) adresinden ulaşılabilir.

[18] Söz konusu yetki, 95/46/AT sayılı Avrupa Veri Koruma Direktifi'nin 25. maddesinin altıncı fıkrası ("Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", 1995, *Official Journal of the European Communities* L. 281/31.) ve GDPR'ın 45. maddesi kapsamında verilmektedir.

[19] Komisyon tarafından yeterlilik kararı verilmiş ülkeler mevcut durumda Amerika Birleşik Devletleri (Gizlilik Kalkanı ile sınırlı olarak), Andorra, Arjantin, Faroe Adaları, Guernsey, İsrail, İsviçre, Japonya, Jersey, Kanada (ticari kuruluşlar için), Man Adası, Uruguay, Yeni Zelenda olup, güncel listeye (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en) adresinden ulaşılabilir.

- Avrupa Komisyonu tarafından bir teklif sunulması,
- Avrupa Veri Koruma Kurulu'ndan (*European Data Protection Board*- "**EDPB**") görüş alınması, ve
- Kararın Avrupalı Komisyonerlerce kabul edilmesi

gerekmektedir.

AEA dışındaki ülkelere veri aktarımı yapılmasına ilişkin Komisyon'a verilmiş olan yeterlilik kararı verme yetkisi, GDPR ile genişletilmiştir. GDPR uyarınca Komisyon'un AEA dışındaki ülkenin yeterli korumayı haiz olduğuna karar vermesine ek olarak Komisyon, üçüncü bir ülkenin *spesifik bir bölgesinin ya da sektörünün* yeterli korumayı haiz olduğuna dair de karar verebilmektedir[20].

Komisyon'un yeterlilik kararı verirken gözeteceği asgari unsurlar şu şekildedir:

- Temel veri koruma kavramlarının ve/veya ilkelerinin mevcut olması,
- Verinin hukuka uygun, adil ve meşru bir şekilde işlenmesi,
- Verinin belirli bir amaçla sınırlı olarak işlenmesi (*Amaçla Sınırlı Olma İlkesi*),
- Verinin doğru ve güncel olması (*Veri Kalitesi İlkesi*),
- Verinin işleme amacıyla orantılı olması (*Orantılılık İlkesi*),
- Verinin işleme amacının gerçekleştirilmesi için yeterli olan süreden fazla saklanmaması (*Veri Saklama İlkesi*),
- Verinin güvenliği için teknik ve idari tedbirlerin alınması (*Güvenlik ve Mahremiyet İlkesi*),
- İlgili kişilerin verilerinin işlenmesi konusunda açık bir şekilde bilgilendirilmeleri (*Şeffaflık ilkesi*),
- İlgili kişinin erişim, düzeltme, silme ve itiraz haklarının bulunması,

[20] Detaylı bilgi için bu başlık altında belirtilen "Kısmı Yeterlilik Kararı" kısmı incelenebilir. Ayrıca, Komisyonun burada bahsi geçen yetkisi GDPR'ın 45 inci maddesinin üçüncü fıkrasında düzenlenmiştir.

- Veri aktarımının ilk alıcısı tarafından yapılacak aktarımlara, diğer alıcının, yeterli düzeyde koruma sağlayan kurallara tabi olması ve veri sorumlusu adına veri işlerken ilgili talimatları izlemesi durumlarında izin verilmesi *(İleride gerçekleştirilecek aktarımların kısıtlanması*),

- Aktarım yapılan ülkenin veri koruma, ulusal güvenlik ve ileriye dönük aktarımlar hakkındaki yasaları ve içtihatları ve bunların pratikte nasıl uygulandığı ve icra edildiği,

- Veri koruma yasalarına uyumu sağlayacak ve işbu yasaları icra edecek bağımsız denetleyici otoritelerin varlığı (ya da yokluğu),

- Aktarım yapılan ülkenin verilerin korunmasına ilişkin uluslararası taahhütleri.

Yeterlilik kararının alınmasından sonra, GDPR'ın 45. maddesinin üçüncü fıkrasında Komisyon tarafından alınan bu kararlarının dinamik olması ve en az dört yılda bir gözden geçirilmesi gerektiği öngörülmektedir. Ayrıca, aynı maddenin beşinci fıkrası gereğince Komisyon'un beyaz listede yer alan ülkeleri "devam eden bir biçimde" yeterlilik kararını etkileyecek koşulların ortaya çıkıp çıkmadığı bahsiyle takip etmesi beklenmektedir. Yeterlilik kararının dinamik yapısı ve önemi nedeniyle Komisyon, ilgili ülke hakkında vermiş olduğu yeterlilik kararını ilgili ülkeye bildirimde bulunup cevap verme imkânı tanımasının akabinde herhangi bir zamanda iptal etme yetkisini de haizdir.

Eklemek gerekir ki GDPR, 95/46/AT sayılı Avrupa Veri Koruma Direktifi'nin[21] ("**Direktif**") yürürlükte olduğu dönemde Komisyon tarafından alınan yeterlilik kararlarının değiştirilmemesini veya iptal edilene kadar geçerli olacağını öngörmektedir. Dolayısıyla yeterli koruma sağladığı belirtilen ülkelerin yer aldığı Komisyon'un beyaz listesi, GDPR kapsamında geçerliliğini sürdürmeye devam etmektedir.

GDPR'a Göre Uluslararası Veri Aktarımlarında "Aktarımın Sürekli Olması veya Olmamasına" Göre Bir Ayrım Yapılmakta mıdır? Hukuki Sonuçları Bakımından Bu Ayrımlar Neye İşaret Etmektedir?

GDPR kapsamında uluslararası veri aktarımında, aktarımın nitelik olarak sürekli veya sürekli olmamasına (örn; tek seferlik veya birkaç sefer) göre bir ayrım yapıldığı görülmektedir. Bu ayrım temelde, bu neviden aktarımlara uygulanacak hukuki şartın neler olması gerektiği noktasında bir yaklaşıma işaret etmektedir.

[21] "Avrupa Veri Koruma Direktifi," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

Genel olarak süreklilik taşıyan uluslararası veri aktarımları "yeterlilik kararı" veya "güvenlik tedbirleri" hukuki şartlarına bağlı olarak gerçekleştirilebilecek iken; sürekli olmayan aktarımlarda "istisnalar" içerisinde sayılan hukuki şartlara dayalı olarak aktarımların yapıldığı gözlemlenmektedir.

Sürekli olmayan aktarım içerisinde sayılan tek seferlik aktarımın hukuki şartı olarak da, GDPR'ın 49. maddesinin ilk fıkrasının ikinci paragrafı, daha önce Direktif'te yer almayan yeni bir istisna getirmiştir. Söz konusu istisnai düzenleme ve bu istisnaya açıklık getiren gösterge; bir dizi spesifik, açıkça sayılmış koşul altında, "veri sorumlusunun zorlayıcı meşru menfaatlerinin" de gerektirmesi halinde kişisel verilerin AEA dışına aktarılabileceği düzenlemektedir. Bu istisna, GDPR 45 ve 46. madde kapsamına girmeyen ve 49. maddede sayılan diğer istisnalara da dayanmayan durumlar için son çare olarak öngörülmüştür. Açık rıza alınmasına ilişkin şartlara uyumun zorluğu ve diğer istisnaların dar kapsamı bu istisnayı veri sorumluları için çekici kılmaktadır.[22]

Veri sorumlusunun zorlayıcı meşru menfaatine dayalı olarak tek seferlik (veya aynı konuyla ilgili süreklilik taşımayacak şekilde birden fazla aktarım) veri aktarımında uygulanacak ve istisnalar içerisinde sayılan bu hukuki şarta dayanabilmek için aşağıda belirtilen koşulların varlığı aranmaktadır[23]:

- Bir yeterlilik kararı bulunmamalıdır,
- Uygun güvenlik tedbirlerine tabi olarak yapılan bir aktarım olmamalıdır,
- Diğer istisnalara dayanılarak bir aktarım yapılamamalıdır,
- Aktarım sürekli olmamalı, yinelenmemelidir (dolayısıyla bu istisna kapsamında aktarım birden fazla kez olabilmekle beraber devamlı/düzenli olmamalıdır)
- Aktarım, yalnızca sınırlı sayıda ilgili kişiyi kapsamalıdır,
- Aktarım, veri sorumlusunun zorlayıcı meşru menfaatleri doğrultusunda gerekli olmalıdır,
- Veri sorumlusunun zorlayıcı meşru menfaatlerinin, ilgili kişinin menfaatleri, hakları ve özgürlükleri ile karşılaştırıldığında ağır basması gerekir,

[22] Nikolaos I. Theodorakis. "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US," *Stanford-Vienna TTLF Working Papers*, no. 39, https://www-cdn.law.stanford.edu/wp-content/uploads/2018/09/theodorakis_wp39.pdf.
[23] ICO, "International Transfers." Aynı şekilde GDPR- Giriş Hükmü 113.

- Veri sorumlusunun veri aktarımı ile ilgili tüm durumları değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olmalıdır (Uygun güvenceler; gizlilik anlaşmaları, aktarımdan kısa bir süre sonra verinin silinmesinin gerekli kılınması veya verinin şifrelenerek aktarılması gibi güvenceler olabilir),

- Veri sorumlusu ilgili **veri koruması otoritesini aktarım hususunda bilgilendirmelidir** (Otoriteden izin alma olarak değerlendirilmemiştir),

- Veri sorumlusu, GDPR 13 ve 14. maddelerde atıfta bulunulan bilgilerin sağlanmasına ek olarak ilgili kişiyi aktarım ve gözetilen zorlayıcı meşru menfaatler hususunda bilgilendirmelidir.

Belirtmek gerekir ki; veri sorumlusunun meşru menfaatinin "zorlayıcı" olması, tek seferlik aktarımın belirleyici özelliklerindendir. Burada GDPR'ın 6. maddesinin ilk fıkrasının (f) bendinde belirtilen meşru menfaat anlayışı yeterli olmamakta, söz konusu meşru menfaatin[24] veri sorumlusu açısından "esaslı" olmasını gerektiren daha yüksek bir eşik uygulanmaktadır. Bir diğer belirleyici husus ise, aktarımın yinelemeli olmamasıdır. Yinelemeli olmaması; aktarımların bir kereden fazla olabileceğini, ancak düzenli olarak gerçekleşmeyeceğini ve örneğin rastgele, bilinmeyen koşullar altında ve ihtiyari zaman aralıkları dahilinde olağan eylemlerin dışında gerçekleşeceğini ifade etmektedir. Son olarak, aktarımın tek seferlik aktarım olmasını belirleyen unsur, sınırlı sayıda ilgili kişiyi ilgilendirmesidir. Sınırlı sayıdan ne anlaşılacağı ise; somut olay bazında değerlendirilecek olup yalnızca bu olay için zorlayıcı meşru menfaate erişebilmek adına gerekli olan ilgili kişilere ait verileri içerecektir[25].

Tek seferlik aktarım olması halinde veri sorumlusu, yukarı da açıklandığı üzere; ilgili veri koruması otoritesini aktarım hususunda bilgilendirmek ve GDPR'ın 13 ve 14. maddelerinde atıfta bulunulan bilgilerin sağlanmasına ek olarak, ilgili kişiyi aktarım ve gözetilen zorlayıcı meşru menfaatler hususunda bilgilendirmekle de yükümlü olacaktır.

---

[24] Meşru menfaate ilişkin değerlendirmenin nasıl yapılacağı, ICO ("How do we apply legitimate interests in practice?" ICO, erişim 15 Şubat, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/.) tarafından detaylıca yapılmıştır. ICO, GDPR'da zorunlu olarak öngörülmemiş olmakla birlikte, meşru menfaat kavramına ışık tutmak amacıyla "meşru menfaat değerlendirmesi (legitimate interests assesment- "**LIA**") konseptini ortaya atmıştır. Buna göre, özellikle şeffaflık ilkesinin gerekliliklerini yerine getirmek adına, ICO 3 aşamalı bir test önerisinde bulunmaktadır. LIA'in ilk aşamasında amaç testi uygulanarak meşru menfaatin ne olduğu tespit edilecek, ikinci aşamasında gereklilik testi uygulanarak söz konusu işlemenin meşru menfaate ulaşmak için gerekli olup olmadığı değerlendirilecek ve son aşamada denge testi yapılarak veri sorumlusunun meşru menfaati ile bireylerin hak ve özgürlükleri arasında veri sorumlusunun işlemesini haklı kılar bir dengenin varlığı incelenecektir. Denge testi uygulanırken işlenen kişisel verinin niteliği, ilgili kişinin makul beklentileri ve işlemenin birey üzerindeki muhtemel etkisi ile olumsuz etkileri azaltmak için herhangi bir güvenlik tedbirinin alınıp alınmadığı değerlendirme unsurları olacaktır. ICO, veri sorumlusunun yaptığı işleme faaliyetinin meşru menfaate dayandırılmasını ancak bu üç aşamalı testi aşması halinde kabul etmektedir.

[25] Tek seferlik aktarıma ilişkin detaylı bilgiler için European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".

GDPR'da "Yeterlilik Kararı Olmayan Ülkelere" Uluslararası Veri Aktarımında Dikkate Alınan ve Dayanak Yapılan Hukuki Şart Nedir? Bu Şartın İçerinde Hangi Tip "Güvenlik Tedbirleri" Belirtilmektedir?

Uluslararası veri aktarımında bir ülkeye, bölgeye veya sektöre dair alınmış bir yeterlilik kararı bulunmaması durumunda; GDPR'da sayılan "güvenlik tedbirleri"nin sağlanması ile bahsi geçen veri aktarımı gerçekleştirilmektedir. Bu güvenlik tedbirleri hem alıcı hem de gönderici tarafından, ilgili kişilerin kişisel verileri kapsamındaki hak ve özgürlüklerinin korunmasını sağlamaktadır.

Bu çerçevede güvenlik tedbirlerinin ve GDPR'ın diğer hükümlerine uyumun sağlanmasının akabinde, yurt dışına veri aktarımı gerçekleştirilebilecektir. Güvenlik tedbirleri GDPR'ın 46 ve 47. maddelerinde düzenlenmiş olup bu güvenlik tedbirleri sekiz ana başlık altında listelenmektedir:

1. Kamu Otoriteleri veya Organları Arasında Oluşturulan, Yasal Olarak Bağlayıcı ve İcra Edilebilir Enstrümanlar (*Legally Binding and Enforceable Instrument Between Public Authorities or Bodies*)

2. Bağlayıcı Şirket Kuralları (*Binding Corporate Rules*)

3. Komisyon Tarafından Kabul Edilmiş Standart Veri Koruma Maddeleri (*Standard Contractual Clauses*)

4. Bir Denetleyici Otorite Tarafından Kabul Edilen ve Komisyon Tarafından Onaylanan Standart Veri Koruma Maddeleri (*Standard Data Protection Clauses Adopted By a Supervisory Authority and Approved By The Commission*)

5. Mesleki Davranış Kuralları (*Code of Conduct*)

6. Sertifikasyon (*Certifications*)

7. Sözleşme Koşulları (*Contractual Clauses*)

8. İdari Düzenlemeler (*Administrative Arrangements*)

GDPR'da "Yeterlilik Kararı Olmayan" ve "Güvenlik Tedbiri' de Alınmayan Uluslararası Veri Aktarımlarına Uygulanan Hukuki Şart Nedir? Bu Şartın İçerinde Hangi Tür Başlıklar Belirtilmektedir?

Yeterlilik kararının bulunmamasının yanısıra; yukarıda listelenmiş güvenlik tedbirlerinden herhangi birinin de kapsamına girmeyen durumlarda, GDPR'ın 49. maddesinde çeşitli istisnalar düzenlenmiştir[26]. Buna göre, AEA dışına veri aktarmak isteyen veri sorumlusu;

- Aktarımın tekrar eden, çok geniş kapsamlı ve yapısal olmaması,
- Ayrıca aktarımın dayanabileceği başka bir hukuki şartın (yeterlilik kararı veya koruma tedbirleri) bulunmaması

şartıyla GDPR'da düzenlenen istisnalardan birine dayanabilmektedir. [27] Sözü edilen istisnalar (derogations) veri aktarımına ilişkin diğer hukuki şartlarla karşılaştırıldığında istisnai ve belirli durumlara spesifik olarak uygulandığı için bu hukuki şartlar dar yorumlanmalı ve kural haline getirilmemelidir[28].

Veri sorumluları ve veri işleyenler ilk olarak GDPR'ın 45. maddesindeki hukuki şarta dayanarak uluslararası veri aktarımını yapmalıdır. Eğer bu şarta dayanılamıyorsa 46. maddede yer alan hukuki şartlardan birisine dayalı olarak aktarım gerçekleştirmelidir; GDPR'ın 45. ve 46. maddelerinde düzenlenen hukuki şartlar yok ise ve aktarımın niteliği yukarıdaki paragrafta belirtilen koşulları taşıyorsa; 49. maddede belirtilen ve aşağıda listelenen istisnalar hukuki şart olarak kullanabilmektedir:

1. Açık Rıza (*Explicit Consent*)
2. Sözleşmenin İfası (*Contract Performance*)
3. İlgili Kişi Yararına Üçüncü Taraf Sözleşmeleri (*Third-Party Contracts in the Individual's Interest*)
4. Kamu Yararı (Public Interest)
5. Hukuki Talep ve İddialar (*Legal Claims*)
6. İlgili kişinin yaşamsal çıkarlarının korunması (Protecting Vital Interest)

[26] "Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers," European Commission, son güncelleme 10 Ocak, 2017, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15.
[27] European Data Protection Supervisor- "International Transfers"
[28] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."

7. Avrupa Birliği İçerisindeki Kamuya Açık Sicillerinden Yapılan Aktarımlar (*Transfers from EU Public Registries*)

8. Veri Sorumlusunun Zorlayıcı Meşru Menfaatleri (*Compelling Legitimate Interests of the Controller*)

GDPR Kapsamında "Eşdeğer Veri Korumasına Sahip Olmayan Ülkelere" Kişisel Veri Aktarımında Dayanak Yapılacak "Koruma Tedbirleri" ve "İstisnalar" Başlığı Altındaki Hukuki Şartların Uygulama Kapsamı ve Yoğunluğu Ne Şekildedir?

Yukarıda da ifade edildiği üzere; "eşdeğer veri korumasına sahip olmayan" ülkelere kişisel veri aktarımında dayanak yapılacak hukuki şartlar olan "Koruma Tedbirleri" ve "İstisnalar" başlığı altında belirtilen hukuki şartların uygulama kapsamı ve kullanılma yoğunluğu birbirinden çok farklıdır. Yine ifade etmek gerekir ki; bu hukuki şartların uygulanması, hiyerarşik olarak dikkate alınmaktadır. Bir başka deyişle "koruma tedbiri" niteliğindeki bir hukuki şarta dayanılma imkanı var ise, "istisnalar altında listelenen hukuki şartlardan birine dayalı olarak "eşdeğer veri korumasına haiz olmayan ülkeye veri aktarımı yapılmamaktadır.

Aşağıdaki tabloda eşdeğer veri korumasını haiz olmayan (yeterlilik kararı bulunmayan) ülkeye veri aktarımında dayanılacak hukuki şartların kapsam ve kullanım yoğunluğu bakımından karşılaştırılması yapılmaktadır:

Hukuki Şartın İsmi	Kullanım Kapsamı	Kullanım Yoğunluğu	İlgili Veri Aktarımı İçin Otoritenin Onayı
Koruma Tedbirleri (GDPR Mad. 46-47)			
Kamu Otoriteleri veya Organları Arasında Oluşturulan, Yasal Olarak Bağlayıcı ve İcra Edilebilir Enstrümanlar	İki kamu otoritesi arasında ilgili veri aktarımına özel güvenlik tedbirlerinin de alındığı bir anlaşmanın varlığı halinde uygulama alanı bulmaktadır.	Yüksek değildir.	Otoritenin onayı aranmamaktadır.

Bağlayıcı Şirket Kuralları	Şirketler topluluğu veya müşterek bir ekonomik aktivite çerçevesinde (örn. Franchise veya Joint Venture) faaliyetlerini yürüten teşebbüs ve taahhüt birlikleri arasında gerçekleşen kişisel veri aktarımlarına uygulanır.	Sınırlı uygulama kapsamı olduğu için kullanımı yüksek değildir[29].	Spesifik veri aktarımına yönelik otorite onayı aranmıyor. Sadece hukuki şartı sağlayan Bağlayıcı Şirket Kuralının otorite tarafından onaylanması gerekiyor.
Avrupa Birliği Komisyonu Tarafından Kabul Edilmiş Standart Veri Koruma Maddeleri	Değiştirilmeden veri aktarımına konu olan ilgili sözleşmelerin içerisine veya ekine konumlandırılan maddelerdir.	En fazla kullanım alanı olan hukuki şarttır. Kullanımı çok yoğundur.	Spesifik veri aktarımına yönelik otorite onayı aranmamaktadır.
Veri Koruması Otoritesi Tarafından Kabul Edilen ve Avrupa Birliği Komisyonu Tarafından Onaylanan Standart Veri Koruma Maddeleri	Burada standart veri koruması maddeleri ilgili ülkenin otoritesi tarafından yayınlanmakta ve Avrupa Birliği Komisyonu tarafından onaylanmaktadır.	Şu anda hiçbir Avrupa Birliği ülkesinin otoritesi bu neviden standart veri koruması maddeleri yayımlamamış ve Avrupa Birliği komisyonun onayına sunmamıştır. Bu nedenle uygulama alanı şu aşamada yoktur.	Spesifik veri aktarıma yönelik otorite onayı aranmamaktadır. Sadece standart veri koruması maddelerinin otorite tarafından düzenlenmesi gerekmektedir.
Mesleki Davranış Kuralları	Meslek kuruluşlarının (ticari birliklerin ve temsilcilerinin) üyeleri arasında ilgili ticari	Kullanım yoğunluğu yüksek değildir. Uygulama alanı meslek	Spesifik veri aktarımına yönelik otorite onayı

[29] Avrupa Birliği Komisyonu tarafından onaylanan ve 24 Mayıs 2018 tarihinde güncellenen "Bağlayıcı Şirket Kurulları"na sahip şirketlerin listesi: "List of companies for which the EU BCR cooperation procedure is closed," European Commission, erişim 15 Şubat, 2020, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841.

	işlemlere yönelik kişisel verilerin işlenmesi, korunması ve aktarımıyla ilgili düzenledikleri davranış kurallarıdır.	kuruluşlarının üyeleri arasındaki veri aktarımlarını kapsamaktadır.	aranmamaktadır. Sadece "Mesleki Davranış Kurallarının" otorite tarafından onaylanması gerekiyor.
Sertifikasyon	Verinin aktarıldığı kişinin (veri sorumlusu- veri işleyen) verinin aktarıldığı ülkenin otoritesi tarafından onaylanmış; kişisel verilerin işlenmesi konusunda gerekli güvenlik tedbirlerini içeren sertifikasyonu olması halleridir.	Şu anda Avrupa Birliği ülkesi otoritesinin onaylamış olduğu hiçbir sertifikasyon çerçevesi bulunmamaktadır. Dolayısıyla kullanım yoğunluğunun sınırlı olduğu söylenebilecektir.	Spesifik veri aktarımına yönelik otorite onayı aranmamaktadır. Sadece hukuki şartı sağlayan, alıcının sahip olduğu "Sertifikasyon"un otorite tarafından onaylanması gerekmektedir.
Sözleşme Koşulları	İlgili kişisel veri aktarımına ilişkin sözleşme koşullarını içeren ve bu veri aktarımını gerektiren hukuki ilişkiye özgü hazırlanmış bir sözleşmeye dayalı olarak yapılan veri aktarımlarında söz konusudur.	Sözleşme koşulları Avrupa Birliği Komisyonu tarafından onaylanan standart veri koruması maddeleri gibi standart maddeler değil, ilgili veri aktarımına özgü düzenlenen sözleşme maddeleridir. Bu nedenle her olaya özgü olarak bu maddelerin kapsamı ve koşulları değişebilmektedir. Kullanım yoğunluğu yüksek değildir.	Sözleşme koşullarının her bir aktarım özelinde otorite tarafından onaylanması aranmaktadır. EDPB bu konuda herhangi bir rehber ve yönlendirme yayınlamadığı için AB içerisindeki otoriteler bu şarta dayalı olarak herhangi bir sözleşmeye henüz onay vermemişlerdir.

İdari Düzenlemeler	İki kamu otoritesi arasındaki anlaşmaya dayalı olarak kişisel veri aktarımda uygulanır. İkiden fazla kamu kurumu arasında ve birden fazla ülkeye veri aktarımını içeren durumlarda bu hukuki şarta dayanılması için EDPB'nin görüşü ve onayı aranmaktadır.	Bu hukuki şart kişisel veri aktarımı gerektiren anlaşmaya taraf olan kamu kurumlarından en az birinin bu şekilde bir bağlayıcı anlaşma yapma yetkisi olmadığı durumlarda uygulanır. Eğer ilgili aktarımı yapan kurumların bu aktarımı gerektiren bağlayıcı anlaşmayı yapmayı yetkisi var ise bu durumda bu hukuki şart değil yukarıda belirtilen "Kamu Otoriteleri veya Organları Arasında Oluşturulan, Yasal Olarak Bağlayıcı ve İcra Edilebilir Enstrümanlar" hukuki şartına dayalı olarak veri aktarımı yapılır. Kullanım yoğunluğu yüksek değildir.	Aktaran tarafta yerleşik ilgili otoritenin anlaşmayı onaylama zorunluluğu vardır. Birden fazla kamu kurumu ve ülkeye aktarım yapılıyorsa, ilgili otoritenin yanında EDPB'nin görüşü ve onayı aranmaktadır.
İstisnalar (Derogations)			
Açık Rıza	Tüm istisnalardaki hukuki şartlarda olduğu gibi bu hukuki şarta dayanabilmek için diğer hukuki şartlara (yeterlilik kararı veya koruma tedbirleri) dayanma imkanının olmaması aynı zamanda;	Kullanım yoğunluğu düşüktür. Otoriteler uluslararası veri aktarımı için aranan açık rızanın GDPR'daki açık rızaya göre daha sert koşulara tabi olması, her zaman geri	Otoritenin onayı aranmamaktadır.

	• Aktarımın tekrarlı, çok geniş kapsamlı ve yapısal olmaması, gerekmektedir. GDPR'da açık rızanın şartlarının yanında ilgili kişinin yurtdışına veri aktarımına yönelik verdiği açık rızada daha yüksek eşik değeri ve şartlar belirtilmiştir. Örneğin açık rızaya dayalı olan bu aktarımın gerekli güvenlik tedbirleri olmadığı için yaratabileceği risklerin açık rıza almadan önce ilgili kişiye açıklanması şartı bulunmaktadır.	alınabilmesi gibi gerekçelerle bu şarta dayalı olarak uluslararası veri aktarımı yapılmasını etkin bir çözüm olarak görmemektedirler.[30]	
Sözleşmenin İfası	Tüm istisnalardaki hukuki şartlarda olduğu gibi bu hukuki şarta dayanabilmek için diğer hukuki şartlara (yeterlilik kararı veya koruma tedbirleri) dayanma imkanının olmaması aynı zamanda; • Aktarımın süreklilik taşımaması ve sözleşmenin ifası için zorunlu olan kişisel verilerle sınırlı olması ve • Sözleşmenin ifası için aktarımın zorunlu olması (sözleşmenin aktarım	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoritenin onayı aranmamaktadır.

[30] ICO, "International Transfers- Exception 1. Has the individual given his or her explicit consent to the restricted transfer?"

	olmaz ise kurulamaması ve ifa edilememesi) şartları aranmaktadır. Kamu otoriteleri bu istisnaya dayanmamaktadır.		
İlgili Kişi Yararına Üçüncü Taraf Sözleşmeleri	Yukarıdaki istisnadaki aynı şartlar geçerlidir ve kapsamı da yukarıdaki belirtildiği gibidir. Buradaki tek fark; ilgili kişinin dışında üçüncü kişilerin verileri bu sözleşmeye göre aktarılmasıdır.	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoritenin onayı aranmamaktadır.
Kamu Yararı	Tüm istisnalardaki hukuki şartlarda olduğu gibi bu hukuki şarta dayanabilmek için diğer hukuki şartlara (yeterlilik kararı veya koruma tedbirleri) dayanma imkanının olmaması aynı zamanda; • Aktarımın süreklilik taşımaması ve kamu yararının gerçekleştirilmesi için aktarımın zorunlu olması aranmaktadır. Bu istisnaya genelde kamu kurumları dayanmaktadır. Adli yardımlaşma anlaşmalarına dayalı aktarımlar bu istisna kapsamında (karşılıklılık	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoritenin onayı aranmamaktadır.

	ilkesine de bakılarak) değerlendirilmekte, adli yardımlaşma anlaşmalarının varlığı kamu yararını sağlama şartını ortaya koyduğu kabul edilmektedir. Eğer aktarım süreklilik taşıyacaksa bu istisnaya değil, koruma tedbirlerine dayalı olarak aktarımın gerçekleştirilmesi gerekliliği ortaya konulmaktadır.		
Hukuki Talep ve İddialar	Tüm istisnalardaki hukuki şartlarda olduğu gibi bu hukuki şarta dayanabilmek için diğer hukuki şartlara (yeterlilik kararı veya koruma tedbirleri) dayanma imkanının olmaması aynı zamanda; • Aktarımın süreklilik taşımaması ve bahsi geçen hukuki talep ve iddiaların aydınlatılması/yerine getirilmesi için aktarımın zorunlu olması aranmaktadır. "Hukuki talep ve iddia"nın ne olduğu da iyi değerlendirilmelidir. Potansiyel bir hukuki talep veya iddiaya dayalı olarak bu	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoritenin onayı aranmamaktadır.

	hukuki şarta dayanılamamaktadır. Kamu kurumları da bu istisnaya dayanabilmektedirler.		
İlgili Kişinin Hayati Önemdeki Bir Hakkının Korunması	Tüm istisnalardaki hukuki şartlarda olduğu gibi bu hukuki şarta dayanabilmek için diğer hukuki şartlara (yeterlilik kararı veya koruma tedbirleri) dayanma imkanının olmaması aynı zamanda; • Aktarımın süreklilik taşımaması ve bahsi geçen aktarımın ilgili kişinin hayati önemdeki hakkı olarak tanımlanan sağlını/vücut bütünlüğü korumak ile ilgili olması; aktarımın ilgili kişiye tıbbı tedavi sağlamak için zorunlu olması ve • İlgili kişinin fiziksel veya ruhsal olarak ilgili aktarıma "açık rıza" veremeyecek durumunda olması aranmaktadır.	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoritenin onayı aranmamaktadır.
Avrupa Birliği İçerisindeki Kamuya Açık Sicillerinden Yapılan Aktarımlar	Tüm istisnalardaki hukuki şartlarda olduğu gibi bu hukuki şarta dayanabilmek için diğer hukuki şartlara (yeterlilik kararı veya koruma tedbirleri) dayanma imkanının olmaması aynı zamanda;	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoritenin onayı aranmamaktadır.

	• Aktarımın süreklilik taşımaması • Bahsi geçen veri tabanlarının kamuya açık olması veya • Hukuki menfaatini ispat eden kişilere açık olması • Aktarılacak verilerin işlenme ve aktarılma amacının ilgili ülke mevzuatının bu veri tabanlarının açık olarak erişimi noktasında konumlamaya amaçladığı hukuki menfaatle ilişkili olması aranmaktadır. Aktarım veri tabanındaki tüm veriler ve kişileri kapsamamalı, veri tabanlarının açık olmasına yönelik hukuki menfaatin yerine getirilmesiyle sınırlı olmalıdır. Özel şirketler tarafından oluşturulan veri tabanları bu istisna kapsamında değerlendirilmemektedir.		

Veri Sorumlusunun Zorlayıcı Meşru Menfaatleri	Bu istisna eğer veri aktarımına yönelik diğer hukuki şartların olmadığı (yeterlilik kararı ve güvenlik tedbirleri) en önemlisi diğer istisnaların da uygulanamadığı son şart olarak çok sıkı koşullara bağlı olarak kullanılmalıdır. Bunun yanı sıra; • Aktarımın tek seferlik veya en fazla birden fazla gerçekleştirilmesi, • Zorlayıcı meşru menfaatin çok net ve otoritenin aradığı koşullarda ortaya konması, • Aktarımın veri sorumlusunun bu zorlayıcı meşru menfaatini korumak için zorunlu olması, • Sadece belirli sayıdaki ilgili kişiyi ve bu kişilerin belirli sayıdaki kişisel verilerini kapsaması, • Veri sorumlusunun meşru menfaatinin ve bu aktarımın hiçbir koşulda ilgili kişinin temel hak ve özgürlüklerini zedeleme tehlikesinin olmaması,	İlgili kapsamda kullanım yoğunluğu bulunmaktadır.	Otoriteye bilgi verilmesi gerekmektedir. Bu bilgilendirmeye istinaden otorite gerekli şartları yerine getirilmediğini düşünüyorsa aktarımı durdurabilmekte veya aktarımın yapılmasını engelleyebilmektedir

	• İlgili kişiye aktarımı zorunlu kılan "zorlayıcı meşru menfaatin" gerekçeleriyle birlikte açıklanması ve • İlgili kişiye ve otoriteye bu aktarımla ilgili bilgi verilmesi aranmaktadır.		

GDPR'daki Uluslararası Veri Aktarımına Yönelik İstisnalar Başlığı Altında Düzenlenen Hukuki Şartlardan Biri Olan "Açık Rıza"nın Hiyerarşik Olarak Uygulanma Zamanı ve Kapsamı Nedir? Türk Hukukuyla Karşılaştırıldığında Nasıl Bir Sonuç Ortaya Çıkmaktadır?

Yukarıdaki bölümlerde yapılan açıklamalar ışığında, GDPR kapsamında AEA dışına yapılan aktarımlar ile KVKK kapsamında yurt dışına yapılan aktarımların birbirinden oldukça farklı formüle edildiği görülebilmektedir. Bu çerçevede GDPR, sınır ötesi veri aktarımına daha çok imkan tanıyarak verilerin aktarımını kolaylaştıracak çok alternatifli bir mekanizma kurmuştur. KVKK düzeninde ise; kişisel verilerin ilgili kişinin açık rızası ile aktarılmadığı hallerde, daha kontrollü ve otorite merkezli bir yapı karşımıza çıkmaktadır.

İki düzenlemenin sınır ötesi veri aktarımına ilişkin farklı yaklaşımları, aktarım rejiminin ilk aşamasında karşımıza çıkmaktadır. Buna göre; KVKK kapsamındaki yurt dışı veri aktarımlarında öncelikle veri sahibinin açık rızasının arandığı görülmektedir. Oysaki açık rıza, GDPR kapsamında sınır ötesi veri aktarımına ilişkin "son çarelerden biri" olarak düşünülmüş ve "istisnalar" başlığı altında düzenlenmiştir.

GDPR ile KVKK kapsamındaki farklılık, açık rızaya başvurulmasındaki hiyerarşik sıranın ötesine de geçmektedir. GDPR çerçevesinde alınacak açık rıza için oldukça katı gereklilikler öngörülmüş, aksi takdirde aktarım için hukuki dayanak teşkil edemeyeceği düzenlenmiştir. Buradaki açık rızanın geçerli olarak kabul edilmesi için aranan genel şartlar GDPR'ın 4. maddesinin on birinci fıkrasında ve 7. maddesinde düzenlenmiştir. Buna ek olarak, Madde 29 Çalışma Grubu (*Article 29 Working Party*,

"**WP29**")[31], açık rızada bulunması gereken genel şartlara ilişkin bir rehber[32] yayımlamıştır.[33] Buna göre; geçerli bir rıza hem belirli bir amaca özgü olmalı hem de veri sahibinin aktarıma ilişkin bilgilendirilmiş olmasına dayanmalıdır.[34] Rızanın belirli bir amaca özgü olması, ilgili kişi tarafından aktarım üzerinde bir dereceye kadar kontrol sağlanmasına imkân tanımakta ve aktarımın içeriğine ilişkin şeffaflık sağlamaktadır. Rızanın belirli bir amaca özgü olması sebebiyle, bazı durumlarda gelecekteki bir aktarıma ilişkin (verilerin toplanması sırasında) rıza almanın mümkün olmayacağı açıktır. Bu gibi hallerde, veri sorumlusu, verilerin toplanmasından sonra gerçekleşse bile yapılacak aktarım için özel bir rıza alındığından emin olmalıdır.[35]

İlgili kişinin aktarıma ilişkin bilgilendirilmiş olması şartı ise; GDPR'ın 4. maddesinin on birinci fıkrasında düzenlenen kişisel verilerin işlenmesi için rıza alınması gereken hallerde ilgili kişinin bilgilendirilmesi gerektiği hükmüne dayanır. Bu genel bilgilendirme yükümlülüğünün yanı sıra; 49. maddenin birinci fıkrasının (a) bendinde **ilgili kişinin, bir yeterlilik kararı ve uygun güvenlik tedbirlerinin bulunmaması nedeniyle söz konusu aktarımların kendisine yönelik risklerinden de haberdar edilmesi gerektiği düzenlenmiştir.**[36] **Söz konusu bilgilendirmenin yapılması ilgili kişinin gerekli açık rızayı verebilmesinin önemli bir şartı olduğundan yokluğunda bu istisna uygulama alanı bulamayacaktır.**[37] Bu gereklilik, *GDPR'da düzenlenen "açık rıza"ya ek olarak, uluslararası veri aktarımında alınacak açık rızanın kapsamı ve içeriğinin ne şekilde farklılaştığı ve daha ağır koşullara tabi olması gerektiğini göstermesi bakımından anlamlıdır*.

Sonuç olarak; ilgili kişinin kişisel verilerini AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılırken veri sorumlusu aşağıdaki bilgilerin tamamını ilgili kişiye sağlamakla yükümlüdür:[38]

- Kişisel verilerin alıcıları veya alıcı kategorileri,
- Verilerin aktarılacağı ülke veya ülkeler,
- Aktarımın yapılmasını gerekli kılan sebepler,

[31] "Article 29 Working Party," European Data Protection Board, erişim 17 Şubat, 2020, https://edpb.europa.eu/our-work-tools/article-29-working-party_en.
[32] "Guidelines on Consent under Regulation 2016/679, WP 259 Rev.01," Article 29 Working Party, son güncelleme 7 Haziran, 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
[33] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[34] ICO- "International Transfers."
[35] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[36] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[37] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[38] ICO- "International Transfers."

- Aktarılacak veri türleri,

- Herhangi bir zamanda ilgili kişinin rızayı geri çekme hakkının varlığı,

- **Kişisel veriler için yeterli koruma sağlamayan ve uygun başka güvenlik önlemlerinin alınmadığı bir ülkeye aktarım yapılmasının olası riskleri**.

Öte yandan; Kurum tarafından yayımlanan Açık Rıza Rehberi[39], KVKK kapsamında alınacak açık rıza için (i) belirli bir konuya ilişkin olma, (ii) bilgilendirmeye dayanma ve (iii) özgür iradeyle açıklanma şartlarını düzenlemektedir. Buna göre veri sorumlusu ve veri işleyenlerce açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerekmektedir.

KVKK kapsamında ve Kurul'un yayınlamış olduğu karar ve rehberlerde işaret edilen "açık rıza"nın niteliği ve hukuki şart olarak kullanım kapsamı Avrupa Birliği ve GDPR ile uyumluluk taşımaktadır. Ancak 9. madde kapsamında aranacak açık rıza'nın uygulama kapsamı ve niteliğine göre Kurum herhangi bir değerlendirme yapmamıştır. Bu yönüyle GDPR'ın uluslararası veri aktarımı bakımından aradığı ağırlaştırılmış koşullara tabi ve yalnızca belirli spesifik durumlarda hukuki şart olarak kullanılabilecek olan "açık rıza" yaklaşımı, uygulamadaki genel eğilim ve Kurum'un yaklaşımında karşılık bulmamaktadır. Bu durum uluslararası veri aktarımında "açık rıza"nın GDPR ve Türk Hukuku karşılaştırılmalı kullanımında gerek nitelik gerek kapsam gerek işlevsellik ve ilgili kişilerin haklarını himaye bakımından büyük farklılıklar bulunduğuna işaret etmektedir.

GDPR'a Göre Uluslararası Veri Aktarımı İçin Otorite İzni Dizayn Edilmiş Midir? Otoriteye Götürülen Uluslararası Veri Aktarımları Hangi Neviden Veri Aktarımlardır ve Otoritenin Bu Konudaki Yetkisi Nedir? Türk Hukuku ile Karşılaştırıldığında Nasıl Bir Sonuç Ortaya Çıkmaktadır?

GDPR kapsamında spesifik uluslararası veri aktarımı için otorite izni, *yalnızca güvenlik tedbirleri içerisinde düzenlenen sözleşme koşulları (contractual clauses) kapsamında düzenlenmiştir*. Burada ***ilgili aktarıma spesifik düzenlenen sözleşmenin*** otorite tarafından onaylanmasına müteakip aktarım yapılabileceği öngörülmüştür.

Bunun yanı sıra; GDPR'da bağlayıcı şirket kuralları, mesleki davranış kuralları, sertifikasyon, idari düzenlemeler, bir denetleyici otorite tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma maddeleri altında düzenlenen güvenlik tedbirlerinin de yine ilgili otoritenin

[39] "Açık Rıza," Kişisel Verileri Koruma Kurumu, erişim 17 Şubat, 2020, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf.

onayıyla icra edilmesine yönelik bir tasarım yapılmıştır. Otoritelere verilen bu yetki; ilgili aktarım özelinde kullanacakları bir yetki olmayıp, bilakis;

- Bahsi geçen hukuksal dayanaklara yönelik kaynakların nasıl oluşturulması ve/veya yorumlanması gerektiğine (Bağlayıcı Şirket Kuralları hangi kapsamda ve nasıl yaratılmalı gibi),

- Bu kaynaklara dayalı olarak aktarım yapmak isteyen veri sorumluları ve veri işleyenler için yaratılan kaynakların onayına (X şirketi tarafından oluşturulan Bağlayıcı Şirket Kurallarına onay verilmesi gibi) yöneliktir.

Görüldüğü üzere GDPR uygulaması, koruma tedbirleri içerisinde sayılan hukuksal dayanaklar içerisinde, spesifik veri aktarımına yönelik otorite iznini yalnızca sözleşme koşulları (*contractual clauses*) hukuki şartı kapsamında öngörmüş; diğer koruma tedbirlerinde ise hukuksal şartın içeriğini şekillendiren, çerçevesini belirleyen ve bu şarta dayanarak uluslararası veri aktarımı yapmak isteyen veri sorumlusu ve/veya veri işleyenlerin ortaya koyduğu hukuksal şartı karşılayan metnin/sürecin şekli ve içeriğini onaylayan bir yetki kullanımı öngörmüştür.

Oysaki; Türkiye'de uygulamadaki genel eğilim GDPR'ın aksine, yeterlilik kararı bulunmadığı hallerde (açık rıza dışında) hukuksal dayanak olarak, yalnızca Kurul izni ile aktarımın yapılması gerekliliğini savunmaktadır. Bu durum pratikte Kurul tarafından henüz herhangi bir izin verilmediği de göz önünde bulundurulduğunda, ticari hayatı durma noktasına getirecek bir etki doğurmaktadır. Oysaki birbirinden oldukça farklı alanları kapsayan hukuki şartlar sayesinde GDPR, uluslararası veri aktarımı konusunda ticari hayatın gereksinimlerini karşılayan, ilgili kişilerin haklarını himaye eden, otoritelerin denetim ve gözetim yetkilerini kuvvetlendiren sürdürülebilir bir veri koruma mekanizması sunmaktadır.

GDPR'a Göre Veri Aktarımına Taraf Olan Hangi Süjelerin Taahhüt Verme Yükümlülüğü Vardır? Bu Taahhütler Hangi Hukuki Enstrümanlar Altında Somutlaşmaktadır? Türk Hukuku ile Karşılaştırıldığında Nasıl Bir Sonuç Ortaya Çıkmaktadır?

GDPR kapsamında öngörülen güvenlik tedbirlerinden olan standart veri koruma maddeleri, veri gönderen ve alanın sözleşmeden doğan yükümlülüklerini ve kişisel verileri aktarılan kişilerin haklarını içermekte olup, bir çeşit taahhüt verme mekanizması sunmaktadır. Komisyon tarafından kabul edilmiş standart veri koruma maddeleri (*standard contractual clauses*) ve bir denetleyici otorite tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma maddeleri (*standard data protection clauses adopted by a supervisory authority and approved by the Commission*), veri sorumluları arasında gerçekleşen veri aktarımları ve veri sorumlusu ile veri işleyen arasındaki veri aktarımlarına ilişkin taahhütnameleri içermektedir.

Halihazırda bir veri koruma otoritesi tarafından kabul edilen ve Komisyon tarafından onaylanan yeni standart veri koruma maddeleri bulunmamakla birlikte, Komisyon'un Direktif kapsamında kabul ettiği üç standart sözleşme bulunmaktadır. Veri sorumluları arasında gerçekleşen veri aktarımları için iki standart sözleşme[40], veri sorumlusu ile veri işleyen arasında gerçekleşen veri aktarımları için bir adet standart sözleşme[41] bulunmaktadır. İlan edilen bu sözleşmeler oldukça geniş kapsamlı olup uluslararası veri aktarımında kişisel verilerin korunabilmesi adına detaylı güvenceler sağlamaktadırlar.

Yukarıdaki bölümlerde de değerlendirildiği üzere; KVKK'nın 5. maddesinin ikinci fıkrası ile 6. maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması durumunda, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması halinde kişisel verileri açık rıza olmaksızın yurt dışına aktarılması mümkün olacaktır. Madde metni de göstermektedir ki KVKK kapsamındaki taahhüt, GDPR'ın aksine yalnızca veri sorumluları için öngörülmüş, veri işleyenler açısından ise herhangi bir düzenleme getirilmemiştir.

Öte yandan, Kurum, internet sitesinde yayımlanan taahhütnamelerde[42] veri sorumlusundan veri sorumlusuna aktarımların yanı sıra veri sorumlusundan veri işleyene aktarımları da dahil etmiştir. Bu şekilde, AB'deki düzenlemeye paralel olarak her iki aktarım açısından da taahhütnameler belirlenmiştir.

Her ne kadar GDPR ve KVKK bakımından, taahhütnamelerin içerikleri açısından paralellik bu şekilde sağlanmış olsa da; taahhütnamelerin işlevselliği ve üstlendiği hukuki dayanak fonksiyonu iki düzenleme arasındaki farkın derinleşmesine sebep olmaktadır.

[40] İlgili Komisyon kararları: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001, *Official Journal of the European Communities* L 181/19, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en ve Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004, *Official Journal of the European Union* L 385/74, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN.

[41] İlgili Komisyon kararı: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010, Official Journal of the European Union L 39/5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en.

[42] "Taahhütnameler," Kişisel Verileri Koruma Kurumu, son güncelleme 16 Mayıs, 2018, https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler.

GDPR'da Düzenlenen Uluslararası Veri Aktarımına Yönelik Hukuki Şartlar, AB Ülkelerinin Taraf Olduğu Uluslararası Sözleşmeler veya Kendi Hukuklarındaki Özel Kanunlardaki Düzenlemelerle Karşılaştığında Hangi Rejimin Uygulanmasına Öncelik Verilmektedir?

AB'deki rejimin ortaya konulmasından önce bu konuda temel teşkil eden kaynakların kısaca ortaya konmasında fayda olacaktır. Avrupa Kömür ve Çelik Topluluğu'nu kuran 1951 tarihli Paris Anlaşması ve Avrupa Ekonomik Topluluğu'nu kuran 1957 tarihli Roma Anlaşması ile temelleri atılan Avrupa Birliği'nin kuruluş ve işleyişine ilişkin temel sözleşmeler birçok değişikliğe uğramış ve 1992 yılında imzalanan Avrupa Birliği Maastricht Anlaşması, mevcut sözleşmelerde de değişiklik getiren kurucu anlaşmalardan biri haline gelmiştir. 2009 yılında yürürlüğe giren Lizbon Antlaşması ise Avrupa Topluluğu'nu kuran Anlaşmanın adını Avrupa Birliği'nin İşleyişi Hakkında Anlaşma olarak değiştirilmiştir[43]. Tüm bu değişiklikler neticesinde Avrupa Birliği'ne ilişkin temel düzenlemeler mevcut durumda Avrupa Birliği Anlaşması (Konsolide Versiyon 2016) ("**TEU**")[44] ve Avrupa Birliği'nin İşleyişi Hakkında Anlaşma (Konsolide Versiyon 2016) ("**TFEU**")[45] olarak ortaya çıkmaktadır.

TEU'nun 13. maddesi uyarınca Avrupa Birliği'ndeki her kurum, anlaşmalarla kendisine verilen yetkilerin sınırları dahilinde ve anlaşmalarda öngörülen usul, şart ve hedeflere uygun olarak hareket etmekle yükümlü kılınmış ve kurumların Avrupa Birliği'nin yetkilerinin kullanılması için sahip olduğu hukuki tasarruflar regülasyon, direktif, karar, tavsiye ve görüş olarak TFEU'nun 288. maddesinde düzenlenmiştir. TFEU'nun 288. maddesinde öngörülen ve genel uygulama alanına sahip, bütünüyle bağlayıcı olduğu belirtilen regülasyonlar, yürürlüğe girer girmez ulusal hukuka aktarılmasına gerek kalmadan[46] tüm üye AB ülkelerinde doğrudan ve yeknesak olarak uygulanan yasal düzenlemelerdir[47].

GDPR, TFEU'nun herkesin kendisiyle ilgili kişisel verilerin korunması hakkına sahip olduğunu düzenleyen 16. maddesine dayanılarak ve Avrupa Parlamentosu ve Avrupa Konseyi'ne sağlanan yetki ile yönetmelik şeklinde düzenlenmiştir.

---

[43] Avrupa Birliği Anlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, 2011. *T.C. Başbakanlık Avrupa Birliği Genel Sekreterliği*, Erişim 21 Şubat, 2020, https://www.ab.gov.tr/files/pub/antlasmalar.pdf.

[44] Consolidated Version of the Treaty on European Union. 2016, *Official Journal of the European Union* C 203/3, Erişim 21 Şubat, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016M/TXT&from=EN.

[45] Consolidated Version of the Treaty on the Functioning of the European Union. 2016, *Official Journal of the European Union* C 202/3, Erişim 21 Şubat, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016E/TXT&from=EN.

[46] Tüm üye devletler açısından bağlayıcı nitelikte olan regülasyonların iç hukuka aktarılması için herhangi bir işlem gerekmemekte olup Avrupa Birliği'nin resmi gazetesinde yayımlanmaları ile yönetmelikte öngörülen tarih veya yayımlamasını izleyen yirmi gün içerisinde tüm üye devletler açısından yürürlüğe girmektedirler.

[47] "Types of EU law," European Commission, erişim 17 Şubat, 2020, https://ec.europa.eu/info/law/law-making-process/types-eu-law_en.

Her ne kadar GDPR metninde Avrupa Birliği resmi gazetesinde yayımlandığı günden sonraki yirminci gün yürürlüğe gireceği ve 25 Mayıs 2018 tarihinden itibaren uygulanacağı belirtilmiş ve TFEU uyarınca yönetmeliklerin iç hukuka aktarılması için ek bir tasarrufta bulunmaya gerek olmasa da üye devletler, GDPR'ın daha ağır koşullar öngörülmesine imkan tanıyan özel hükümleri de göz önüne alınarak, iç hukuka aktarmaya ilişkin kanun çıkarma yoluna gitmişlerdir[48]. Ancak bu durum bile GDPR'ın doğrudan uygulanabilirliği ve bağlayıcılığını halel getirmemektedir. Nitekim, TFEU'nun 291. maddesi üye devletlerin hukuken bağlayıcı AB tasarruflarını uygulamak için gerekli tüm ulusal hukuk tedbirlerini almakla yükümlü olduklarını düzenlemektedir.

Tüm bu açıklamalardan da anlaşılmaktadır ki, GDPR üye devletler açısından, uluslararası sözleşme niteliğindeki TEU ve TFEU uyarınca, bağlayıcı bir düzenlemedir ve üye devletlerin bu düzenlemenin uygulanmasını sağlaması gerekmektedir. Nitekim, birçok yargı kararında ortaya konulduğu ve doğrudan etki prensibi ile de kesinleştiği üzere bağlayıcı AB hukuku tasarrufları üye devletlerin iç hukuklarına göre öncelikli olarak uygulanacaktır[49]. GDPR'ın 45. maddesinde düzenlenen yeterlilik kararı da GDPR'ın bir yönetmelik olmasından ötürü üye devletler açısından bağlayıcı nitelikte olup bu hükmün TEU ve TFEU uyarınca öncelikli olarak uygulanması gerekmektedir. Bu noktada belirtmek gerekir ki her ne kadar GDPR bir AB hukuki tasarrufu olarak öne çıkıyor olsa da Avrupa Birliği'nin hükümetlerarası ve milletlerarası bir teşkilat olması nedeniyle söz konusu yönetmelik uluslararası bir düzenleme olma karakterini de barındırmaktadır.

GDPR'ın genel karakteri açısından yapılan açıklamaların yanı sıra, GDPR, uluslararası sözleşmelerin uluslararası veri aktarımına etkisi ile ilgili ayrıca hükümler de barındırmaktadır. "Birlik hukuku çerçevesinde yetkilendirilmeyen aktarımlar veya açıklamalar" başlıklı 48. madde ve "Önceden imzalanan anlaşmalarla ilişki" ile Giriş Hükmü 102 ve 105, bu konuda beliren soru işaretlerine açıklamalar getirmektedir. GDPR'ın 48'inci maddesi ve Giriş Hükmü 115, üçüncü ülkenin resmî kurumları tarafından bir veri aktarım talebi gelmesi halinde bu aktarımın, talepte bulunan üçüncü ülke ile üye devlet arasında akdedilen hukuki yardım antlaşması gibi bir uluslararası anlaşmaya dayanılabilmesi için, söz konusu aktarımın GDPR'ın üçüncü ülkelere veri aktarımına yönelik hukuki şartları sağlaması halinde ya da açıklamanın veri sorumlusunun tabi olduğu üye devlet hukuku ya da AB hukuku kapsamında tanınan önemli bir kamu yararının gerektirmesi halinde mümkün olacaktır.

Öte yandan, GDPR'ın 96. maddesi, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması hususunda üye devletler tarafından 24 Mayıs 2016 tarihinden önce imzalanan ve bu

[48] "GDPR Implementation- Updated State of play in the Member States (11/04/2019)," European Commission, erişim 17 Şubat, 2020, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306.
[49] "Precedence of European law," European Union, erişim 18 Şubat, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14548.

tarihten önce geçerli AB hukukuna uyumlu olan anlaşmaların, değiştirilene, yenilenene veya yürürlükten kaldırılana kadar yürürlükte olacağını düzenlemektedir.

Tüm bu anlatılanları özetler nitelikte olan Giriş Hükmü 102, GDPR'ın AB ile üçüncü ülkeler arasında akdedilmiş ve güvenlik tedbirlerini de içeren uluslararası sözleşmelere halel getirmeyeceğini düzenlemektedir. Söz konusu giriş hükmü ayrıca üye devletlere GPDR'ı ve AB hukukunun herhangi bir hükmünü etkilememesi koşulu ile uygun koruma sağlayan uluslararası sözleşmelerin üçüncü ülkelerle imzalanmasına imkan tanımaktadır.

GDPR'a Göre Uluslararası Sözleşmelerin, Avrupa Birliği Komisyonu'nun "Yeterlilik Kararı" Alınmasında Bir Fonksiyonu Var Mıdır? Eğer Var ise Avrupa Konseyi'nin 108 Sayılı Konvansiyon'una Taraf Olmanın ve İç Hukuka Aktarmanın "Yeterlilik" Başvurusu Sürecinde Bir Pozitif Etkisi Olmakta Mıdır?

GDPR Giriş Hükmü 105, uluslararası sözleşmelerin yeterlilik kararı verilirken yarattıkları etkiye ilişkin açıklık getirmektedir ve bu Giriş Hükmü ile uluslararası aktarımlara ilişkin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[50] ("**108 Sayılı Konvansiyon**") ile GDPR arasındaki somut bağlantı sağlanmıştır. Giriş Hükmü 105, Komisyon'un yeterlilik kararı verirken dikkate alması gereken ilk unsur olarak üçüncü taraf ülkelerin ve uluslararası organizasyonların uluslararası taahhütlerini belirtmekte, bunun yanı sıra, üçüncü taraf ülkelerin ve uluslararası organizasyonların katıldığı çok taraflı veya bölgesel sistemlerden doğan yükümlülüklerin de Komisyon tarafında göz önünde bulundurulması gerektiğini de eklemektedir. Ancak, söz konusu giriş hükmünde özellikle 108 Sayılı Konvansiyon'a katılımın değerlendirme kapsamına alınmasının gerektiğinin ifade edilmesi, yeterlilik kararı açısından 108 Sayılı Konvansiyon'un önemine delalet etmektedir.[51]

Avrupa Konseyi'nin 108 Sayılı Konvansiyon'una Taraf Olmak ve Bu Sözleşmeyi İç Hukuka Aktarmak, Avrupa Birliği İçin Neden Otomatik Olarak "Yeterlilik" Kararı Almak İçin Yeter Şart Değildir?

Yukarıda da açıklandığı üzere; GDPR Giriş Hükmü 105, 108 Sayılı Konvansiyon'u ayrıca ifade ederek yüksek önem vermiş olmakla birlikte, bu sözleşmenin "değerlendirmede özellikle dikkate alınması" gerektiğini düzenlemektedir. GDPR'ın yeterlilik kararı verilmesine ilişkin kriterleri ortaya koyan detaylı düzenlemeleri ile birlikte düşünüldüğünde, 108 Sayılı Konvansiyon'a taraf olmanın yeterlilik kararı

[50] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," Council of Europe, 28 Ocak 1981, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.
[51] Article 29 Working Party- "Working document on Adequacy Referential".

verilmesi anlamında oldukça olumlu sonuç yaratacağı anlaşılmakta ancak tek başına taraf olmanın bu kararın verilmesinde yeterli olmayacağı sonucuna varılmaktadır.

Nitekim Komisyon'un yeterlilik kararı verirken gözeteceği, aşağıda belirtilen birçok asgari unsur bulunmaktadır.[52] Komisyon, yeterlilik kararını verme sürecinde çok boyutlu bir değerlendirme yürütmekte ve ilgili kişilerin verilerinin güvenliğinin sağlanması adına belirli güvencelerin varlığını aramaktadır. Her ne kadar 108 Sayılı Konvansiyon, kişisel verilerin güvenliğinin sağlanmasına ilişkin birtakım güvenceler ve mekanizmalar öngörse de tek başına bu gerek-yeter şart olmamaktadır.

Avrupa Konseyi Tarafından Hazırlanan Konvansiyon 108+'e Taraf Olmak ve Bu Sözleşmeyi İç Hukuka Aktarmak, Avrupa Birliği'ne "Yeterlilik" Başvurusunda Pozitif Bir Değeri Olacak Mıdır?

Modernize Edilmiş Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[53] ("**Konvansiyon 108+**") ile esnek ve çok taraflı bir yasal düzenleme getirilmiş ve imzaya açılmıştır. Bu yeni uluslararası sözleşme metni ile bir yandan kişisel verilerin korunmasına ilişkin gerekli güvenlik tedbirleri getirerek diğer yandan kişisel verilerin sınır ötesi aktarılmaları kolaylaştırılmıştır. İçerik olarak da değerlendirildiğinde 108 Sayılı Konvansiyon, modernize edilerek GDPR ile benzer/paralel bir düzeye getirilmiştir. Konvansiyon 108+'de yer alan tanımlar, ilkeler, gizliliğe ilişkin konseptler ve ilgili kişi hakları gibi düzenlemeler GDPR'a benzerlik göstermektedir. Bununla beraber 108 Sayılı Konvansiyon'un kapsamının (hem veri işleme türü hem işlenen veri türleri açısından) genişletilmesi de GDPR ile Konvansiyon 108+'in beraber uygulama bulacağı alanları artırmıştır.

Dolayısıyla Konvansiyon 108+, GDPR'a oldukça yakın bir düzenleme getirerek, Komisyon'un yeterlilik kararı vermesinde kriter olarak kullandığı birçok hususu bünyesine dahil etmiştir. GDPR'ın 108 Sayılı Konvansiyon'u özellikle değerlendirmeye almayı gerektirmesi ve bu sözleşmeye taraf olmanın kararın verilmesinde önemli bir etkisi olduğu göz önünde bulundurulduğunda, 108 Sayılı Konvansiyon'a oranla çok daha detaylı ve yüksek koruma öngören Konvansiyon 108+'in evleviyetle olumlu etki doğuracağı açıktır.

Avrupa Konseyi'nin Hazırladığı Konvansiyon 108+'in Uluslararası Veri Aktarımında Nasıl Bir Değeri ve Etkisi Vardır?

[52] Daha detaylı bilgi için Bkz. Yeterlik Kararı bölümü.
[53] Konvansiyon 108+'nın Türkçe versiyonu: Kişisel Verilerin İşlenmesi Karşısına Bireylerin Korunması için Sözleşme – 108+ Konvansiyon. 2019. *İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü*. Erişim 21 Şubat, 2020. https://itlaw.bilgi.edu.tr/media/document/2019/09/avrupa-konseyi-108plus-konvansiyon-tercume.pdf.

Konvansiyon 108+ ile taraf devletlerin, münhasıran kişisel verinin korunması amacıyla taraf devletlerle yapılan kişisel veri aktarımlarını özel izne tabii tutamayacağına ve yasaklayamayacağına -öngörülen iki istisna hariç olmak üzere- hükmedilmiştir. Sözleşmeye taraf olmayan devletlere yapılacak kişisel veri aktarımlarında eşdeğer koruma şartı Konvansiyon 108+'de da devam etmektedir. Bu tür bir koruma düzeyi, (i) uluslararası sözleşmeler dahil olmak üzere ilgili ülkenin iç hukukunca veya (ii) *ad hoc* (özel) uygulamalarla veya aktarım işlemine katılan kişiler tarafından kabul edilip uygulanan yasal olarak bağlayıcı ve uygulanabilir araçların sağladığı standart güvenlik tedbirleriyle güvence altına alınabilecektir. Sadece bahsedilen bu durumlarda veri koruma otoritelerinin bilgilendirilmesi aranmaktadır. Söz konusu sözleşme ile yurt dışına veri aktarımına dair gerekliliklerin yerine getirilememesi durumunda dahi veri aktarımının gerçekleştirilebilmesi için taraf devletlerce çeşitli seçenekler de sunulmuş, bu şekilde uluslararası veri aktarımı konusunda kolaylık sağlayan mekanizmalar sağlanmıştır. Bu rejimin değerlendirilmesi sırasında (i) GDPR ile uyumun sağlanmasının olumlu etkilerinin yanı sıra, (ii) Avrupa Birliği'nin (ve diğer uluslararası organizasyonların) Konvansiyon 108+'e taraf olabilmesi de dikkate alınmalıdır.

108 Sayılı Konvansiyon'a kıyasen daha detaylı ve kapsamlı düzenlemeler getiren, GDPR ile uyumu yakalama gayesi güden Konvansiyon 108+ uluslararası boyutta yeknesak bir düzenlemeyi pekiştiren bir düzenleme olarak büyük önem arz etmektedir. Uluslararası veri aktarımı konusunda kolaylık sağlamakla beraber sınırları netleştiren bu sözleşmenin yaygınlaşması ile pratikte ortaya çıkan sorunların çözümünde çok değerli bir etki yaratacağı söylenebilir.

Bölüm 3 –GDPR'a Göre Kişisel Verilerin Uluslararası Aktarımına Yönelik Hukuki Çerçeve ile KVKK'nın Yabancı Ülkelere Kişisel Veri Aktarımına Yönelik 9. Madde Hükmünü Yorumlayan Uygulamadaki Genel Eğilimin Karşılaştırılması

GDPR'a Göre Uluslararası Veri Aktarımını Düzenleyen Hukuki Çerçeve ile Ülkemizdeki Uygulamadaki Genel Eğilimin Dayandığı Hukuki Şartların Karşılaştırılmasına Yönelik Tablo

Veri Aktarımına Dayanak Teşkil Eden Kaynaklar	Avrupa Birliği	Türkiye	Türkiye (Uygulamadaki Genel Eğilim)
Uluslararası Anlaşmalar	X	X[54]	
Kanunlar	X	X[55]	
Yeterlilik Kararı	X	X	X
Güvenlik Tedbirleri			
Kamu Otoriteleri veya Organları Arasında Oluşturulan, Yasal Olarak Bağlayıcı ve İcra Edilebilir Enstrümanlar	X		
Bağlayıcı Şirket Kuralları	X		
Komisyon Tarafından Kabul Edilmiş Standart Veri Koruma Maddeleri	X		
Bir Denetleyici Otorite Tarafından Kabul Edilen ve Komisyon Tarafından Onaylanan Standart Veri Koruma Maddeleri	X		
Mesleki Davranış Kuralları	X		
Sertifikasyon	X		
Sözleşme Hükümleri	X		
İdari Düzenlemeler	X		
İstisnai Haller			
Açık Rıza	X	X[56]	X

[54] Türkiye Cumhuriyeti Anayasası'nın 90 ıncı maddesinin son fıkrası gereğince usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir ve temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalar ile kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınacaktır. Ayrıca, KVKK'nın 9 uncu maddesinin 5 inci fıkrasında uluslararası sözleşme hükümlerinin saklı kalacağı belirtmiştir.

[55] KVKK'nın 9 uncu maddesinin son fıkrası, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğunu düzenlemiştir. Buna göre çeşitli kanunlarda ilgili kurum ve kuruluşlara yurt dışına veri aktarımı konusunda yetki verilmiştir. Söz konusu düzenlemelerim süreçleri KVKK'da öngörülen süreçten bağımsız kabul edilmesi ve veri aktarımı konusunda yetkilendirilmiş kurum ve kuruluşların dışında ayrıca Kurul'un izni gerekmediği sonucuna varılması gerekmekle birlikte; düzenlemede ve uygulamada bu hususa açıklık getirilmemiştir.

[56] Yukarıda ilgili bölümde de açıklandığı üzere, açık rıza GDPR uygulamasında istisnalardan biri olarak ortaya çıkmakla birlikte KVKK kapsamında veri aktarımının esas hukuki dayanağı olarak düzenlenmiştir. Bunun yanı sıra, GDPR

Sözleşmenin İfası	X		
İlgili Kişi Yararına Üçüncü Taraf Sözleşmeleri	X		
Kamu Yararı	X		
Yasal Talepler	X		
Fiziksel veya Hukuki Engel	X		
Kamuya Açık Sicillerinden Yapılan Aktarımlar	X		
Veri Sorumlusunun Zorlayıcı Meşru Menfaatleri	X		
Veri Aktarılacak Ülkedeki Veri Sorumlusundan Yeterli Koruma Yapılacağına Dair Yazılı Taahhütname ve Kişisel Verileri Koruma Kurulu İzni		X[57]	X

Ortaya Çıkan Bu Resmin Hukuken ve Hukuk Politikası Bakımından Sonuçlarını Nasıl Yorumlamak Gerekmektedir?

Yukarıda ortaya konulan akademik sentez ve bu sentezin özetlendiği tablo ışığında; GDPR ve AB hukuku karşılaştırmalı olarak, Türk Hukukuna ve uygulamada gelişen duruma yönelik tespitlerimiz şu şekilde özetlenebilir:

- KVKK'nın uygulamadaki genel eğilimin yorumlarıyla kişisel verilerin yabancı ülkeleri aktarımında hayli kısıtlayıcı ve uygulanması imkansız bir yaklaşım ortaya koyduğu görülmektedir.

- KVKK'nın uluslararası veri aktarımına yönelik 9. maddede belirtilen dar kapsamlı lafzı ve uygulamadaki genel eğilimin yorumları, GDPR ve Avrupa Birliği hukuku içerisinde geliştirilen hiyerarşik, çok katmanlı, aktarımın amaç ve niteliğine göre hukuki himaye vasıtalarının niteliğini, uygulama şartlarını çeşitlendiren ve detaylandıran çağdaş yaklaşımın hayli gerisindedir.

- AB Hukuku ve GDPR'da düzenlenen uluslararası veri aktarımına yönelik hukuki şartların Türk Hukuku bakımından nasıl uygulanması gerektiği ve bu yönde hukuki yorum tekniğiyle bir değerlendirme yapılıp yapılamayacağı bu zamana kadar gündeme getirilmemiştir.

düzenlemesi açık rızanın niteliğine ilişkin açık ve spesifik olması, olası risklere karşı aydınlatılmış olması gibi daha detaylı düzenlemeler getirirken, KVKK açık rızanın niteliğini belirlemede aynı ayrıntıya girmemektedir.

[57] Söz konusu taahhütler GDPR düzenlemesindeki "Komisyon Tarafından Kabul Edilmiş Standart Veri Koruma Maddeleri" ve "Bir Denetleyici Otorite Tarafından Kabul Edilen ve Komisyon Tarafından Onaylanan Standart Veri Koruma Maddeleri" ile benzerlik göstermekle birlikte farklı bir mekanizma öngördüğünden ayrıca değerlendirilmiştir.

- Uluslararası veri aktarımında uygulamadaki genel eğilimin esas aldığı yegane kriter niteliğindeki "açık rıza ve Kurul izni" hukuki şartlarının mehaz düzenleme ve yorumlardaki bağlamlarından ve kapsamlarından koparılarak kullanılması zorunluluğu ortaya çıkmıştır.

- Uygulamadaki genel eğilim tarafından GDPR ve mehaz düzenlemedeki kapsam, bağlam ve yorumlarından kopuk bir şekilde uygulanmak zorunda bırakılan açık rıza ve Kurul izni hukuki şartları, uluslararası veri aktarımlarının bu hukuki şartlara dayalı olarak yapılmasını imkansız hale getirdiği gibi; bu hukuki şartların GDPR ve AB hukukundaki uygulamalarda görüldüğü üzere belirli kapsam ve şartlarda ifa etmesi gereken hukuki himayenin de gereği gibi uygulanamamasına neden olunmuştur.

- Uygulamadaki genel eğilim tarafından Türkiye'nin taraf olduğu ve iç hukuka aktardığı Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ve Avrupa Konseyi'nin "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol'ünün[58] ("**181 Sayılı Ek Protokol**") uluslararası veri aktarımlarına nasıl uygulanacağına dair bir hukuki değerlendirme ve uygulama ortaya konulmamıştır.

- Uluslararası veri aktarımlarını (aynı konuyu) düzenleyen KVKK'nın 9. maddesiyle; 108 Sayılı Konvansiyon'un ve 181 Sayılı Ek Protokol'ün uyumu olup olmadığına dair bir hukuki değerlendirme de uygulamadaki genel eğilim tarafından yapılmamıştır.

- Uluslararası veri aktarımına yönelik hükümler içeren 108 Sayılı Konvansiyon'un ve 181 Sayılı Ek Protokol'ün aynı konuyu düzenleyen KVKK arasında uyumsuzluk olduğu durumunda Anayasa'nın 90. maddesinin beşinci fıkrası gereğince nasıl bir uygulama ve hukuksal yorum çerçevesi geliştirilmesi gerektiğine dair bir açıklık getirilmemiştir.

- Yurt dışına veri aktarımlarını düzenleyen diğer kanunların neler olduğu ve bu kanunların KVKK ile nasıl uygulanması gerektiğine dair hukuki bir yaklaşım ortaya konulmamıştır.

- Uluslararası veri aktarımında "karşılıklılık" ilkesinin bağlamından koparılarak (özellikle uluslararası sözleşmelerle ile KVKK'nın çatıştığı durumda) hukuksal yorumlar yapıldığı görülmektedir.

[58] "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows," Council of Europe, 8 Kasım 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080626.

- "Yeterlilik" kararının verilmesi ve bu konudaki çalışmalar bakımından uygulamayı yönlendirici ve ilgili paydaşların kafasındaki soru işaretlerini giderici bir takvim ve çalışmaya rastlanmamıştır.

- GDPR ve AB hukukundaki uluslararası veri aktarımına yönelik hukuki kaynaklar, bu kaynakların şekillenmesine neden olan ihtiyaçlar, bu kaynakların ne şekilde uygulandığı, düzenlemelerin özünün (*ratio legis*) neye ulaşmaya hedeflediği, kaynaklar arasındaki sistematik ilişki bilimsel düzeyde ülkemizde detaylı olarak incelenmemiş ve yorumlanmamıştır.

- Uygulamadaki genel eğilim GDPR'da düzenlenen bazı güvenlik tedbirlerinin (örn. Bağlayıcı Şirket Kurulları) Kurul'un KVKK'daki yetkisine dayalı olarak uluslararası veri aktarımında dayanılacak hukuki şartlardan biri olarak konumlandırılmasını savunmaktadır. Bu şartlar ancak GDPR'da olduğu gibi sistematik, aktarım niteliği ve amacına uygun olarak dizayn edildiği ve uygulama alanlarının bu kapsamda sınırlandırıldığı noktada anlamlıdır. Aksi takdirde ülkemizdeki uluslararası veri aktarımındaki şu andaki kaotik durum uygulama alanı ve kapsamı sınırlı olan tek veya birden çok koruma tedbirinin ve istisnanın hukuken uygulamaya alınması ile çözülemeyecek; mevcut durumda Kurul izni ve açık rıza hukuki şartlarında olduğu gibi bu enstrümanların bağlamından koparılarak uygulanması tehlikesini ortaya çıkacaktır.

- Uluslararası veri aktarımı içerisinde yer alan diğer süjelerin (örn. veri işleyenlerin) ilgili kişilerin haklarını daha iyi himaye edebilmek ve bu çerçevede denetlenebilirdik, hesap verilebilirliği sağlayabilmek adına hangi hukuki şartlar çerçevesinde değerlendirilmesi gerekliliğine dair hukuki yorum ve yaklaşım geliştirilmemiştir.

- Ülkemizde uygulamadaki genel eğilimin uluslararası veri aktarımında uygulanması gerekliliğini ortaya koyduğu ana hukuki şart olan "açık rıza", GDPR ve AB hukuku uygulamasında "istisnalar" başlığı içerisinde ele alınıp tekrarlı, geniş kapsamlı ve yapısal olmayan veri aktarımıyla sınırlı olarak; "istisnalar" başlığı altında düzenlenen her hukuki şartta olduğu gibi diğer hukuki şartların olmadığı (yeterlilik veya güvenlik tedbirleri) koşulda uygulama alanı bulmaktadır. Bunun yanında GDPR ve AB uygulamasında uluslararası veri aktarımında aranan "açık rıza"nın GDPR'daki "açık rıza"ya göre daha ağır geçerlilik koşullarına tabi olduğu da unutulmamalıdır. Hal böyle iken Türkiye'de hakim yaklaşımın aktarımın niteliği, amacı, kapsamı ve açık rızanın taşıması gereken niteliklere göre değerlendirme/sınırlandırma yapmadan her neviden uluslararası veri aktarımının açık rızaya dayalı olarak yapılması gerekliliğini savunması, "açık rıza"ya dayalı olarak ilgili kişinin haklarının himaye edilmesi fonksiyonunu ortadan kaldırmakta, uygulanmaması gereken durumlarda açık rıza hukuki

şartına dayanılmasını da zorunlu kılarak hukuki şartın hukuki himaye amacının aksine kullanılmasına neden olunmaktadır.

- Ülkemizde uygulamadaki genel eğilimin uluslararası veri aktarımında uygulanması gerekliliğini ortaya koyduğu ana hukuki şartlardan biri olan veri sorumlularının taahhüdü ve Kurul izni, GDPR ve AB hukuku uygulamasında "koruma tedbirleri" başlığı içerisinde ele alınan "Sözleşme Hükümleri" başlıklı hukuki şarta benzemektedir. AB ve GDPR uygulanmasında otoritenin onayına sunulan sözleşme hükümleri, ilgili hukuki ilişkinin gerektirdiği ve bu hukuki ilişkiye özel olarak hazırlanan veri aktarımıyla ilgili olan kısımlarıyla sınırlıdır. Oysaki ülkemizdeki uygulamada Kurum'un yayınladığı genel nitelikli çerçeve sözleşme hükümleri veri sorumlusunun taahhüdünü yerine getirmekte kullanılacağı ve asgari olarak veri sorumlusunun taahhüdünde bulunması gereken koşullar olup, Kurul'un onayı GDPR'ın aksine sözleşmeye ilişkin değil ilgili veri aktarımına yöneliktir. Bunun yanında GDPR ve AB uygulamasında uluslararası veri aktarımında dayanılacak hukuki şartlardan biri olarak "koruma tedbirleri" başlığı içerisinde düzenlenen "Sözleşme Hükümleri"nin uygulama kapsamı sınırlı olup, AB hukuku ve GDPR uygulamasında bu şarta dayalı olarak otoritelerin onayladığı sözleşme hükümleri şu aşamada yoktur. Hal böyle iken Türkiye'de hakim yaklaşımın; aktarımın niteliği, amacı, kapsamı ve "sözleşme hükümleri" hukuki şartının taşıması gereken unsurlar ve bu çerçevedeki otoritenin yetkilerini değerlendirmeden/sınırlandırma yapmadan her neviden uluslararası veri aktarımının veri sorumlularının taahhüdü ve Kurul izni hukuki şartına dayalı olarak yapılması gerekliliğini savunması, bu hukuki şartın GDPR ve AB hukuku karşılaştırmalı bakıldığında ilgili kişinin haklarını himaye etme fonksiyonunu ortadan kaldırmakta, uygulanmaması gereken durumlarda da Kurul izni hukuki şartına dayanılmasını zorunlu kılarak bu hukuki şartın hukuki himaye amacının aksine kullanılmasına neden olunmaktadır.

- Hukuk politikası olarak, GDPR, AB Hukuku, mehaz düzenleme, Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 181 Sayılı Ek Protokol'ünde düzenlenen durumlar ile KVKK'nın 9. maddesi ve uygulamadaki genel eğilimin yorumlarının arasındaki fark ve bu farkın yarattığı uygulama güçlükleri tartışılmamıştır. Hukuk politikası olarak bu farklıkların ne şekilde çözülmesi gerekliliğine dair de gerek hukuki yorum tekniğiyle gerekse de hukuk politikaları araçları geliştirilmesi bakımından ne yapılması gerekliliğine ilişkin net bir çerçeve de ortaya konulmamıştır.

Bölüm 4 – Türk Hukukunun Mevcut Kaynaklarına Göre Yabancı Ülkelere Veri Aktarımında Amaca Uygun Hukuki Yorumla Ortaya Konacak Çözüm Önerisi

Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile İlgili Sözleşmenin Eki Olan 181 Sayılı Ek Protokol'ün Türk Hukuku Bakımından Değerlendirilmesi

Türkiye, Avrupa Konseyi'nin kişisel verilerin işlenmesi ve korunmasına yönelik 108 Sayılı Konvansiyon'u 02.05.2016 tarihi itibariyle iç hukuka aktarmış ve 01.09.2016 tarihi itibariyle de yürürlüğe koymuştur.[59] Türkiye aynı şekilde Avrupa Konseyi'nin 108 Sayılı Konvanisyon'u ve 181 sayılı Ek Protokol'ünü 11.07.2016 tarihinde iç hukuka aktarmış ve 01.11.2016 tarihi itibariyle de yürürlüğe koymuştur.[60]

Türkiye, 108 Sayılı Konvansiyon'un 13. maddesinin ikinci paragrafının (a) bendi gereğince sözleşmenin uygulanması için yetkili otoritenin (*competent authority*) Kişisel Verileri Koruma Kurulu olduğunu da resmi olarak 2 Mayıs 2016 tarihinde Avrupa Konseyi makamlarına deklare etmiştir.[61]

Kişisel verilerin korunması konusu Anayasa'mızın "Temel Hak ve Ödevler" başlıklı ikinci kısmının 20. maddesinin üçüncü fıkrasında düzenlenmiştir. Bu yaklaşımın bir neticesi olarak "kişisel verilerin korunması" konusunun Anayasa'mız içerisinde bireylerin "temel hak ve özgürlükleri" bağlamında düzenlendiği ve himaye edildiği söylenebilecektir.

Anayasa hukuku bakımından "kişisel verilerin korunması" huşunun, bireylerin "temel hak ve özgürlükleri" bağlamında himaye edildiği tespitinden sonra, Avrupa Konseyi'nin kişisel verilerin işlenmesi ve korunmasına yönelik 108 Sayılı Konvansiyon'u ile Avrupa Konseyi'nin 108 Sayılı Konvansiyon'unun 181 Sayılı Ek Protokol'ünün Anayasa'mızın 90. maddesinin beşinci fıkrasına göre kanun hükmünde olan "***usulüne göre yürürlüğe konulmuş milletlerarası andlaşma***" olup olmadığı değerlendirilmelidir. Bu anlaşmaların niteliği, hazırlayan makam, onayları, iç hukuka aktarma ve yürürlüğe konma prosedürlerine bakıldığında Anayasam'ızın 90. maddesin birinci fıkrasında aradığı "usule göre" yürürlüğe konduğu ve uluslararası anlaşma hüviyetinde olduğu hukuki tespiti yapılabilecektir.

---

[59] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 108-Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

[60] Taraf ülkeler listesi: "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=YP6ZdjNO.

[61] "Reservations and Declarations for Treaty No.108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/declarations?p_auth=YP6ZdjNO&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=TUR&_coeconventions_WAR_coeconventionsportlet_codeNature=3.

Son bir hukuki tespit olarak da Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile Avrupa Konseyi'nin Konvansiyon'unun 181 Sayılı Ek Protokol'ünün Anayasa'mızın 90. maddesinin beşinci fıkrasında belirtilen "***usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşma***" hüviyetinde olup olmadığının değerlendirilmesidir. Belirtildiği üzere kişisel verilerin korunması konusu Anayasa'mızın "Temel Hak ve Ödevler" başlıklı ikinci kısmının 20. maddesinin 3. fıkrasında düzenlenmektedir. Dolayısıyla "kişisel verilerin korunması" hususunun Anayasa kapsamında bireylerin "temel hak ve özgürlükleri" bağlamında düzenlendiği ve himaye edildiği görülmektedir. Bundan hareketle kişisel verilerin korunmasına ilişkin bu antlaşmaların Anayasa'mızın 90. maddesinin beşinci fıkrasında belirtilen "usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşma" hüviyetinde olduğu hukuken tespit edilecektir.

Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 108 Sayılı Konvansiyon'un 181 Sayılı Ek Protokol'ü Uluslararası Veri Aktarımını Nasıl Düzenlemektedir?

Çalışmamızın konusu olan kişisel verilerin uluslararası aktarımı konusu, 6698 Sayılı Yasa ile karşılaştırıldığında, Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 108 Sayılı Konvansiyon'un 181 Sayılı Ek Protokol'ünde konuları **farklı şekillerde** düzenlendiği görülmektedir. Şöyle ki;

Uluslararası veri aktarımı 108 Sayılı Konvanisyon'un 12. maddesinde düzenlenmiştir. İlgili madde uyarınca; taraf devletlerin **münhasıran kişisel verinin korunması amacıyla taraf devletlere yapılan kişisel veri aktarımlarını yasaklayamayacağına ya da özel izne tabii tutamayacağına** hükmedilmiştir. Bu hükme aşağıda yer alan istisnalar getirilmiştir:

- Taraf devletlerin iç hukukunun **belli kişisel veri kategorileri veya otomatik işleme tabi tutulmuş kişisel veri dosyaları için bu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler içermesi** ve diğer tarafın düzenlemelerinin eşdeğer bir koruma içermemesi durumunda,

- Bu aktarımın bir taraf devletin, bir diğer taraf devlet üzerinden taraf olmayan bir devletin ülkesine ilgili tarafın iç hukukundaki boşluktan yararlanmak üzere yapılması halinde; bu tür aktarımları engellemek amacıyla yapılması.

108 Sayılı Konvansiyon'un "Açıklayıcı Raporun"da, uluslararası veri aktarımı ve ilgili iç hukukların çatışması konusunda çok önemli değerlendirmeler yapılmıştır. Bu değerlendirmelere göre;

- Sözleşme dizayn edilmeden önce sözleşmeye taraf olan ülkeler arasında uluslararası uygulamanın nasıl olması gerektiğine yönelik yaklaşımlar tartışılmıştır. İlk yaklaşım

"karşılıklılık" ilkesine dayanan, ilgili iç hukukun aradığı standartların diğer ülkedeki tüm veri işleme faaliyetleri ve uluslararası veri aktarımlarında uygulanması yaklaşımı idi. Bu yaklaşım sözleşmeye taraf olan ülkelerde ilgili kişilerin aynı kapsam ve çerçevede haklarının himaye edilmesi, taraf ülkelerdeki uygulamalarda birlik sağlanması ve ilgili ülkeler arasında iş birliğinin tesis edilmesi amaçlarına ters düşeceği için tercih edilmemiş; onun yerine "kişisel verilerin yurt dışında işlenmesi ve sınır ötesi aktarılması süreçlerinde korunmasını" temin eden; tüm sözleşmeye taraf ülkelerde ortak olarak benimsenen ve uygulanan kişisel verilerin korunması ilkeleri özelinde dizayn edilen uluslararası sözleşmeyle bu uluslararası uygulamanın hayata geçirilmesine karar verilmiştir. 108 Sayılı Konvanisyon, bu ana amaç çerçevesinde hazırlanmış, yürürlüğe konmuş ve uygulanmıştır.[62]

- Uluslararası veri aktarımları için 108 Sayılı Konvanisyon'a taraf olan ülkelerin iç hukuklarda ayrı kontrol mekanizmaları ve sınırlandırmalar getirmesi, ilgili kişiler ve ülkeler için temel önemde bir değer olan verilerin sınır ötesi serbest dolaşımı ilkesini ihlal edebilmektedir. Bu nedenle uluslararası alanda kişisel verilerin korunmasına yönelik varılacak çözümün verilerin sınır ötesi serbest dolaşımı prensibini zayıflatmaması[63] ve uygulanmasını güçleştirmemesi gerekmektedir.[64]

- 108 Sayılı Konvanisyon'un ikinci bölümünde düzenlenen kişisel verilerin işlenmesine yönelik temel ilkelerin ("*common core*") tüm akit devletler tarafından benimsenmesi ve aynı şekilde uygulanması, akit devletler tarafından ilgili kişilere aynı düzeyde koruma sağlayacaktır. Bu yaklaşım aynı zamanda verilerin serbestçe dolaşımına ilkesinin herhangi bir "korumacılık" yaklaşımıyla sınırlandırılması tehlikesini; bu noktada ortaya çıkabilecek kanunlar ihtilafı ve yer bakımından uygulama tartışmaların da ortaya çıkmasını engelleyecektir.

- Akit devletler arasında veri aktarımları, "verilerin serbest dolaşımı" ilkesine bağlı olarak herhangi bir özel kontrole tabi kılınmamalıdır. Bu yaklaşım 108 Sayılı Konvanisyon'un ikinci bölümünde düzenlenen kişisel verilerin işlenmesine yönelik temel ilkelerin ("*common core*") aynı kurallarla hayata geçirilmesinin sağlanması konusuyla yakın ilişki içerisindedir. [65]

62 "Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," Council of Europe, son güncelleme 28 Ocak, 1981, Paragraf 10-13, https://rm.coe.int/16800ca434.
63 Bu prensibin kaynağı ilgili "Açıklayıcı Raporda" Avrupa İnsan Hakları Sözleşmesinin 10. Maddesine dayandırılmaktadır.
64 Council of Europe- Explanatory Report of 108, Paragraf 8-9.
65 Council of Europe- Explanatory Report of 108, Paragraf 20-21.

181 Sayılı Ek Protokol'ün 2. maddesi 108 Sayılı Konvanisyon'dan farklı olarak bu defa, **108 Sayılı Konvansiyon'a taraf olmayan ülkelere veya kurumlara** veri aktarımın ne şekilde yapılacağını hüküm altına almıştır.

181 Sayılı Ek Protokol'ün 2. maddesi göre; 108 Sayılı Konvansiyon'un tarafları, **108 Sayılı Konvanisyon'a taraf olmayan ülkelere ve kurumlara amaçlanan veri aktarımına yönelik** olarak ilgili ülkelerin veya kurumların **yeterli düzeyde korumayı sağlaması** durumunda aktarım gerçekleştirebilecektir.

Yeterli düzeyde korumanın 108 Sayılı Konvansiyon'a taraf olmayan ülke veya kurum tarafından ne şekilde sağlanacağına dair 181 Sayılı Ek Protokol'de bir açıklık getirilmemiştir. 181 Sayılı Ek Protokol'ün Açıklayıcı Raporunun[66] (*Explanatory Report*) 25 ila 30. paragrafları içerisinde bu konuda değerlendirmeler yapılmıştır. Bu değerlendirmelere göre;

- Yeterlilik düzeyi değerlendirmesi her bir aktarım özelinde, aktarımla ilgili tüm şartlar dikkate alınarak belirlenmelidir.

- Yeterlilik düzeyi değerlendirmesi her bir aktarıma konu olan olay özelinde aktarımın niteliği veya aktarılacak verilerin kategorilere göre yapılmalıdır. Bu çerçevede aktarıma ilişkin tüm koşullar özellikle de aşağıda belirtilen konular yeterlilik değerlendirmesinde dikkate alınmalıdır;

    - Aktarıma konu olan verilerin tipi

    - Aktarıma konu olan verilerin işlenme amaçları ve muhafaza edilme süreleri

    - Aktarımın yapıldığı ülke ve aktarılan ülke

    - Aktarımı yapılan ülkedeki veya organizasyonundaki uygulanan genel ve sektörel hukuk kuralları

    - İlgili veri aktarımı ve işleme faaliyetlerine uygulanacak profesyonel ve güvenlik kuralları ve bu kurallara göre alınan tedbirler.

[66] "Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows," Council of Europe, son güncelleme 8 Kasım, 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce56.

- Yeterlilik düzeyi değerlendirmesi ilgili tüm aktarımlar bakımından aktarılacak ülke veya organizasyon bakımından yapılarak bu ülke veya organizasyona yapılacak tüm aktarımlara izin verilmesi de gündeme gelebilir. Bu durumda yeterlilik değerlendirmesi ve bununla ilgili karar 108 Sayılı Konvanisyon'u uygulama bakımından görev verilen yetkili otorite tarafından yukarıda belirtilen şartlar da göz önüne alınarak gerçekleştirilir.

- Yeterlilik düzeyi değerlendirmesi, 108 Sayılı Konvansiyon ve 181 Sayılı Ek Protokol'deki "kişisel verilerin korunması konusundaki temel ilkeler" çerçevesinde aktarılan ülkenin veya organizasyonun bu prensiplere ne ölçüde uyduğu dikkate alınarak gerçekleştirilir. Aktarımın niteliği gerektiriyorsa ilgili kişinin kişisel verilerinin hukuken himaye edilen haklarına uyumsuz işlenmesi durumunda, ilgili kişinin haklarını ne şekilde ileri sürebileceği ve koruyacağı da yeterlilik düzeyi değerlendirilmesinde dikkate alınması önerilmektedir.

- 108 Sayılı Konvansiyon'un Danışma Komitesi, ilgili ülkenin veya organizasyonun yeterlilik değerlendirilmesi yapılırken taraf devletlere görüş sağlama noktasında, taraf devletin talebi üzerine destek olabilecektir.

Yeterli koruma düzeyinin amaçlanan aktarımla alakalı **108 Sayılı Konvansiyon'a taraf olmayan ülke veya kurum tarafından sağlanamaması** durumunda, **181 Sayılı Ek Protokol'ün 2. maddesinin ikinci fıkrasında** bu ülkelere veya kurumlara yapılacak kişisel veri aktarımlarının aşağıda belirtilen koşullara dayalı olarak gerçekleştirilebileceği hüküm altına alınmaktadır:

a) Eğer taraf devletin iç hukuku ilgili kişinin özel bir menfaatinin yerine getirilmesi veya ilgili kişinin özel menfaatini aşan üstün hukuki yararın yerine getirilmesi için (örneğin kamu yararı) bu aktarımın yapılmasına izin veriyorsa, ya da

b) İlgili veri aktarımından sorumlu olan veri sorumlusu tarafından sağlanan ve ilgili otorite tarafından iç hukukuna göre uygun bulunan **koruma tedbirleri** varsa (ki bu koruma tedbirleri aktarıma konu olan sözleşme hükümlerinin bir sonucu olarak ortaya çıkabilir).

Yukarıda belirtilen **181 Sayılı Ek Protokol'ün 2. Maddesinin ikinci fıkrasının "a" ve "b"** bentlerinin ne şekilde yorumlanması gerektiğine yönelik olarak, 181 Sayılı Ek Protokol'ün içerisinde açıklık olmamasına rağmen, 181 Sayılı Ek Prokol'ün gerekçelerinin belirtildiği "*Açıklayıcı Rapor*"un **31 ile 33. paragraflarında**[67] konu detaylandırılmaktadır. Şöyle ki;

[67] Council of Europe- Explanatory Report of 181.

Ek Protokolün 2. Maddesinin 2. Fıkrasının "a" bendi; taraf devletlerin "yeterli korumayı sağlamayan" ülke ve kurumlara veri aktarımı yapılması noktasında **istisna** getirebilmelerine yönelik takdir yetkisi bulunmaktadır. Bu istisnaları düzenleyen iç hukuk kurallarının 108 Sayılı Konvansiyon'un getirdiği prensiplerle uyumlu olması, sınırlı bir uygulama kapsamı olması, uygulama kapsamıyla sınırlı olarak yorumlanması ve uluslararası veri aktarımında "ana esas" olarak uygulanmaması gerekmektedir. 181 Sayılı Ek Protokol'ün 2. Maddesinin ikinci fıkrasının (a) bendinde belirtilen durumlar "istisna"ların hangi hukuki yararlara (**ilgili kişinin özel bir menfaatinin yerine getirilmesi veya ilgili kişinin özel menfaatini aşan üstün hukuki yararın yerine getirilmesi "kamu yararı"**) yönelik olacağına işaret etmektedir. İç hukukta belirtilecek "istisnalar" ilgili kişinin özel bir menfaatini korumasının yanında, bu özel menfaati aşan üstün hukuki yararın bir başka deyişle kamu yararının korunmasını amaçlayan şekilde de ortaya çıkabilir. Bu noktada "kamu yararını" korumayı hedefleyen istisnaların Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin ikinci fıkrası, 108 Sayılı Konvansiyon'un 9. maddesinin ikinci fıkrası içerisinde belirtilen hukuki yararları korumaya yönelik ve onlarla sınırlı olmalıdır. Bu paragrafta "kamu yararını" sağlamaya yönelik "istisnalara" örnek olarak **"hukuki talep ve iddialar**", "**kamuya açık sicillerden yapılan aktarımlar**" gösterilebilir. Bir diğer istisna konusu olan "ilgili kişinin özel bir menfaatinin korunması" istisnası içerisinde ise "**ilgili kişiyle birlikte veya ilgili kişi yararına bir sözleşmenin yerine getirilmesi**", "**ilgili kişinin yaşamsal çıkarlarının korunması**" veya "**aktarıma ilgili kişinin rıza vermesi**" sayılabilir. İlgili kişinin "rıza vermesi" hukuki şartına dayanılıyorsa, ilgili kişi amaçlanan veri aktarımıyla ilgili uygun bir yöntemle rızasına açıklamadan önce bilgilendirilmesi gerekmektedir.

181 Sayılı Ek Protokol'ün 2. maddesinin ikinci fıkrasının (b) bendi;

108 Sayılı Konvansiyon'a taraf olmayan ülkede veya "yeterli korumayı sağlamayan" ülke veya organizasyonlarda bulunan alıcıya veri aktarımlarında, bu veri aktarımından sorumlu olan tarafın uygun güvenlik tedbirlerini sağlaması durumunda bu aktarımlar gerçekleştirilebilecektir. Bu güvenlik tedbirlerinin ne olduğu ve uygunluğu iç hukuka göre bu güvenlik tedbirlerinin uygunluğuna karar verme yetkisine haiz olan yetkili otorite tarafından belirlenecektir. Bu güvenlik tedbirleri taraf ülkede yerleşik olan veri sorumlusundan taraf olmayan ülkedeki bir alıcıya veri aktarımını gerekli kılan sözleşmeye dayalı olarak ilgili tarafların taahhüt ettikleri sözleşme hükümleri neticesinde de ortaya konabilir.

İlgili tarafların veri aktarımını gerekli kılan sözleşme hükümleri mutlaka veri korunmasına yönelik koruyucu hükümler de içermelidir. Usul hükümleri bakımından ilgili aktarımdan sorumlu olan taraf nezdinde sözleşme hükümlerinin uyumluluğunu sağlayacak kişilerin de belirlenmesi önem arz etmektedir. İlgili kişinin veri sorumlusu nezdinde belirlenen bu kişiye herhangi bir zamanda ve

herhangi bir maliyet olmadan gerekli olan durumlarda başvurarak, kendi haklarının icrasıyla ilgili destek alınması da temin edilmelidir.

Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 108 Sayılı Konvansiyon'un 181 Sayılı Ek Protokol'ünün Uluslararası Veri Aktarımına İlişkin Hükümleri KVKK'nın 9. Maddesi Hükmüyle Çatıştığı Durumda Nasıl Bir Hukuki Yaklaşım Geliştirmelidir?

Yukarıdaki açıklamalardan da görüldüğü üzere; uluslararası veri aktarımı konusunda KVKK'nın 9. maddesi lafzı ve bu maddeyi ilişkin uygulamadaki genel yaklaşımın yorumları, Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 108 Sayılı Konvansiyon'un 181 Sayılı Ek Protokol'ü ile **farklıdır**. Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 108 Sayılı Konvansiyon'un 181 Sayılı Ek Protokol'ünün yukarıda yaptığımız açıklamalar ışığında Anayasa hukukumuzun bakımından "***usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşma***" hüviyetinde olduğu tespitinden hareketle, somut durumda Anayasamızın 90. maddesinin beşinci fıkrasında işaret edilen "***usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi***" ve buna dayalı olarak da "***bir uyuşmazlık***" durumunun var olduğu tespit edilebilir. Bu durumda hukuken nasıl hareket edilmesi gerekliliği de yine Anayasamızın 90. maddesinin beşinci fıkrasında işaret edilmiştir. Bu hükme göre;

"..***Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır***".

denilmektedir.

Bu durumda uluslararası veri aktarımı konusunda KVKK'nın 9. maddesi ve ilgili hükümleri Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ile 108 Sayılı Konvansiyon'un 181 Sayılı Ek Protokol'ü ile çatışmadığı ve ona uygun olarak yorumlanıp uygulandığı durumda uygulama alanı bulanacaktır. Bu noktada Türkiye'deki uluslararası veri aktarımlarında aşağıda belirtilen ana ilkeler kapsamında hareket edilmelidir.

- Türkiye'deki veri sorumluları veya ilgili kişiler, Avrupa Konseyi'nin 108 Sayılı Konvansiyon'unun 12. maddesine dayanarak akit devletlere ilgili sözleşme ve Avrupa İnsan hakları 108 Sayılı Konvansiyon'un 10. maddesine göre tanımlanmış olan verilerin serbest dolaşımı ilkesi gereğince veri aktarımında bulunabilir.

- Türkiye akit devletlere yapılan bu veri aktarımları 12. maddede belirtilen;

- Taraf devletlerin iç hukukunun **belli kişisel veri kategorileri veya otomatik işleme tabi tutulmuş kişisel veri dosyaları için bu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler içermesi** ve diğer tarafın düzenlemelerinin eşdeğer bir koruma içermemesi durumunda,

- Bu aktarımın bir taraf devletin, bir diğer taraf devlet üzerinden taraf olmayan bir devletin ülkesine ilgili tarafın iç hukukundaki boşluktan yararlanmak üzere yapılması halinde; bu tür aktarımları engellemek amacıyla yapılması

koşulları dışında engelleyemez veya sınırlandıramaz.

- Yeterlilik değerlendirmesi ancak 108 Sayılı Konvansiyon'a taraf olmayan devletler veya organizasyonlar için yapılabilir.

- Yeterlilik değerlendirmesinin akit olmayan devletler ve organizasyonlar için nasıl yapılacağı 108 Sayılı Konvansiyon ile 181 Sayılı Ek Protokol içerisindeki hükümler ve "açıklayıcı raporları" içerisindeki gerekçeler ışığında belirlenmelidir

- Sözleşmeye taraf olmayan ülkelere, yeterlilik değerlendirmesini haiz olmayan ülke veya kurumlara;

  - Eğer taraf devletin iç hukuku **ilgili kişinin özel bir menfaatinin yerine getirilmesi** veya **ilgili kişinin özel menfaatini aşan üstün hukuki yararın yerine getirilmesi** için (örneğin kamu yararı) bu aktarımın yapılmasına izin veriyorsa ("istisna" üst başlığı içerisinde düzenlenmektedir),

ya da

  - İlgili veri aktarımından sorumlu olan veri sorumlusu tarafından sağlanan ve ilgili otorite tarafından iç hukukuna göre uygun bulunan **koruma tedbirleri** varsa.

Bu hukuki şartlara dayalı olarak aktarım yapılabilecektir.

Yukarıdaki açıklamalarımızdan da görüldüğü üzere; 108 Sayılı Konvansiyon ve 181 sayılı Ek Protokol'ü, Avrupa Birliği'nin GDPR'ın uluslararası veri aktarımına yönelik getirdiği rejime benzer bir hukuki alt yapının ülkemizde de oluşturulması ve buna uygun hukuki enstrümanların geliştirilmesi için çok değerli bir hukuki dayanak sunmaktadır. Yeterlilik değerlendirmesi olmayan ülkelere veya kurumlara veri aktarımlarında dayanılabilecek hukuki şartlar olarak 108 Sayılı Konvansiyon'un 181

Sayılı Ek Protokol'ünün Açıklayıcı Raporunda içeriği detaylandırılan "güvenlik tedbirleri" ve "istisnalar", gerek müesseselerin kapsamı gerekse de ortaya konulacak hukuki enstrümanların tipleri bakımından neredeyse GDPR'ın 46-47 ve 49. maddelerinde düzenlenen hususlarla aynıdır. 181 Sayılı Ek Protokol'ün GDPR'da olduğu gibi uluslararası veri aktarımında ilgili kişinin rızasını "istisna"lar içerisinde düzenlemesi, daha nitelikli bir rıza olmasına vurgu yapması ve sınırlı bir uygulama kapsamı içerisinde işlevsellik tanıması ülkemizdeki genel uygulamanın aksine ayrıca anlamlıdır.

Hakkın özü itibariyle 108 Sayılı Konvansiyon'a taraf olan akit devletlere Türkiye'deki veri sorumluları tarafından gerçekleşen veri aktarımlarını yasaklanmamalı, 108 Sayılı Konvansiyon'a aykırı olarak sınırlandırılmamalı ve KVKK'nın 9. maddesine uygun değil gerekçesiyle de hukuka aykırı olarak değerlendirmemelidir. İlgili sözleşmeye dayalı olarak Türkiye'deki veri sorumluları tarafından akit devletlere yapılan uluslararası veri aktarımlarının KVKK'nın 9. maddesine uygun olmadığı gerekçesiyle hukuka aykırı saymak açıkça Anayasa'ya ve Türkiye'nin uluslararası hukuktaki taahhütlerine aykırıdır. 108 Sayılı Konvansiyon'un 12. maddesinde akit devletlere olan veri aktarımında yapılabilecek sınırlandırmalara ilişkin durumlar saklıdır. Ancak bu sınırlandırmalar 108 Sayılı Konvansiyon'un uygulanması konusunda, Türkiye'nin yetkili otorite olarak gösterdiği Kurul tarafından hukuken ortaya konulmadan, sırf bu durumların varlığı nedeniyle bahsi geçen aktarımları hukuka aykırı olarak nitelendirmeye neden olmayacaktır.

Aynı şekilde gerek 108 Sayılı Konvansiyon gerekse de 181 Sayılı Ek Protokol'ünde akit devletlerin otoriteleri arasındaki işbirliği, ilgili kişilerin aktarılan ülkedeki haklarının etkin şekilde korunması için ilgili otoriteler üzerinden işbirliği süreçlerini tanımlanmıştır. Bu sözleşmelerin uygulanması konusunda ülkemiz tarafından yetkili otorite olarak gösterilen Kurul, sözleşmelerdeki bu mekanizmaları etkin şekilde işleterek akit devletlere yapılan bu aktarımlarda ilgili kişilerin haklarının himaye edilmesini temin etmelidir.

GDPR uygulaması ile KVKK'nın uygulaması karşılaştırıldığında, "yeterlilik kararı" olmayan ülkelere veri aktarımında kullanılabilecek hukuki şartların sayısı, niteliği ve uygulama şartları bakımından ülkemizde hayli kısıtlayıcı bir çerçeve olduğu ortaya konulmuştur. Kurul, 108 Sayılı Konvansiyon ve 181 Sayılı Ek Protokol'deki yetkileri ile KVKK'nın 22. maddesinin birinci fıkrasının (a), (e), (f) ve (g) bendelerindeki yetkilerini birleştirerek GDPR'ın 46-47 ve 49. maddelerinde düzenlenen "koruma tedbirleri" ve "istinalar" başlığı altındaki hukuki şartları aynı şekilde "yeterli koruma"ya haiz olmayan ülkelere veri aktarımı için uygulanacak hukuki şartlar olarak ülkemizde düzenleyebilecektir. Bu yetkisi aynı zamanda 181 Sayılı Ek Protokol'ün Açıklayıcı Raporunda ve GDPR'ın 49. maddesinin birinci fıkrasının (a) bendinde belirtilen ilgili kişinin "rıza"sının bağlamına uygun kapsam ve şekilde uluslararası veri aktarımında bir hukuki şart olarak kullanılmasını da sağlayacaktır.

Son olarak Avrupa Birliği ülkelerinin 108 Sayılı Konvanisyon ve 181 sayılı Ek Protokol'e taraf olmasına rağmen, Türkiye'ye olan veri aktarımlarında 108 Sayılı Konvanisyon'un 12. maddesinin aksine 181 Sayılı Ek Protokol'de belirtilen ve "yeterlilik değerlendirmesi olmayan" ülke ve kurumlar için dayanılması gereken GDPR'da da 46-47 ve 49. maddelerinde düzenlenen "koruma tedbirleri" ve "istisnalar" hukuki şartlarına olarak veri aktarımı yapması hususuna değinmek gerekirse;

- Türkiye bu durumda uluslararası hukuktaki "karşılıklılık" ilkesinin kendisine verdiği hukuki hakka dayanarak, 108 Sayılı Konvansiyon'un 12. maddesine aykırı tutumda bulunan GDPR'ı uygulayan ülkelere aynı şekilde muamelede bulunmak adına GDPR'ın 46-47 ve 49. maddelerinde düzenlenen "koruma tedbirleri" ve "istisnalar" hukuki şartlarına dayalı olarak bu ülkelere veri aktarımı yapılmasına karar verebilir.

- Türkiye'nin uluslararası hukuktaki "karşılıklılık" ilkesine dayalı olarak 108 Sayılı Konvansiyon'un 12. maddesine dayalı veri aktarımlarına ek şart getirmesi ancak GDPR'ın 46-47 ve 49. maddelerinde belirtilen tüm "istisna" ve "koruma tedbirlerinin" Türk hukuku bakımından aynı şekilde düzenlenmesi ve ilgili ülkelere yapılacak veri aktarımlarında aynı şekilde uygulanması durumunda uluslararası hukuka uygun olabilecektir.

- Karşılıklılık ilkesinin Avrupa Birliği üyesi olmayan diğer akit devletlere ne şekilde uygulanacağı da bu akit devletlerin 108 Sayılı Konvansiyon'un 12. maddesini Türkiye bakımından ne şekilde uyguladıklarına göre de değişebilecektir.

- Karşılıklılık ilkesine dayalı olarak 108 Sayılı Konvansiyon'un 12. maddesine dayalı olarak akit devletlerde bulunan kişilere veri aktarımlarının sınırlandırılması, ek koşullara tabi kılınması ancak bu konuda Kurul tarafından "karşılıklılık ilkesine" uygun biçimde gerekli düzenlemeler yapıldığı durumda söz konusu olacak olup; bu gerekçeyle düzenlemeler yapılmadan "karşılıklılık" durumunun olmadığından bahisle akit devletlerde bulunan kişilere 108 Sayılı Konvansiyon'un 12. maddesi uyarınca Türkiye'deki veri sorumluları tarafından yapılan aktarımların hukuka aykırı olduğu ve gerekli şartları taşımadığı iddia edilemeyecektir.

Bölüm 5 – Hukuk Politikası Gereği Sürdürülebilir Bir Uluslararası Veri Aktarımı İçin Ülkemizde Atılması Gereken Adımlara Yönelik Öneriler

Yukarıdaki açıklamalardan görüleceği üzere; Türkiye'nin taraf olduğu Avrupa Konseyi'nin 108 Sayılı Konvansiyon'u ve 181 Sayılı Ek Protokol'ü, GDPR'da olduğu gibi Türkiye için sürdürülebilir, çok katmanlı, amaca uygun ve hukuki himayeyi en üst düzeye taşıyacak hukuki alt yapının ülkemizde oluşturulması için gerekli olan tüm imkanları ve hukuki dayanakları sunmaktadır. Bu imkanları

kullanmak ve buna uygun hukuksal yorumlar geliştirmek uluslararası veri aktarımı bakımından ülkemizde uygulanacak çağdaş hukuk politikasının bir gereği olduğu gibi, Anayasal da bir zorunluluktur.

108 Sayılı Konvansiyon'un 13. maddesi ve 181 Sayılı Ek Protokol'ün 1. maddesi akit devletler arasında işbirliği koşullarını düzenlemektedir. Kurul, bu işbirliği mekanizmalarını işleterek uluslararası veri aktarımında akit devletlerin maddi hukuk kuralları arasında yeknesaklık, uygulamaları – yorumları bakımından birlik ve ilgili kişilerin haklarını himaye yönünden de etkin ve uygulanabilir bir mekanizma yaratılmasına zemin hazırlayacaktır. 108 Sayılı Konvansiyon ve 181 Sayılı Ek Protokol içerisinde tanımlı olan akit devletler ve ilgili otoriteleri arasındaki işbirliği süreçlerinin ve mekanizmaların işletilmesi gerek ilgili sözleşmelerin doğru şekilde iç hukukumuzda uygulanması gerekse de KVKK kapsamında Türkiye'nin yeterli korumaya sahip ülkeleri belirlemesi konusunda yapacağı çalışmalara ışık tutacaktır. Bunun yanısıra; bu işbirliği ve diyalog mekanizmaları Türkiye'nin GDPR'a göre Konvansiyon tarafından "yeterli korumayı sağlayan ülke" olarak tanınması süreçlerinin daha yetkin ve süreç odaklı olarak yürütülmesi konusunda Kurul'a önemli bir avantaj ve destek sağlayacağı gibi, diğer ülkelerin otoritelerinin uygulama ve perspektiflerini yakından görmek, analiz etmek ve karşılıklı fikir alış verişinde bulunmak ülkemizde "kişisel verilerin korunması hukuku" konusunda oluşacak bilgi birikimine de katkı yapacaktır.

108 Sayılı Konvansiyon'un ve 181 Sayılı Ek Protokol'ün modernizasyonu çalışmaları uzun süredir Avrupa Konseyi nezdinde sürdürülmektedir. Konvansiyon 108+ olarak gündemde yer alan bu çalışmalar daha sonra 223 Sayılı Sözleşme ismiyle resmi bir formata bürünmüş, Konsey ülkeleri ve 108 Sayılı Konvansiyon'un akit devletlerinin imzasına açılmıştır. Konvansiyon 108+, uluslararası veri aktarımı ve GDPR'da belirtilen çağdaş veri koruması hukuku prensiplerini ve düzenlemelerini uluslararası sözleşme formatında bir metin içerisinde somutlaştırması bakımından anlamlıdır. Türkiye'nin Konvansiyon 108+'a taraf olarak iç hukukuna aktarması, Türkiye'de uygulanan veri koruması hukukuna ilişkin standartları yükselteceği gibi uluslararası işbirliği ve koruma mekanizmalarını da güçlendirecektir.

Türkiye'de maddi hukuk kaynakları bakımından güncel ihtiyaçlara cevap vermeyen KVKK'nın mevcut kapsamı, karışıklıklara, yanlış uygulamalara ve yorumlara zemin hazırlayan lafzı ve sistemi de değiştirilmelidir. Çalışmamızın konusu olan uluslararası veri aktarımına yönelik KVKK'nın 9. maddesi buna güzel bir örnektir. Bu çerçevede gerek Avrupa Konseyi'nin Konvansiyon 108+'ı gerekse de GDPR bu konuda geliştirilecek hukuk politikalarına, maddi hukuk kaynağı olarak kaynaklık etmek için çok değerli emsalleri oluşturmaktadır.

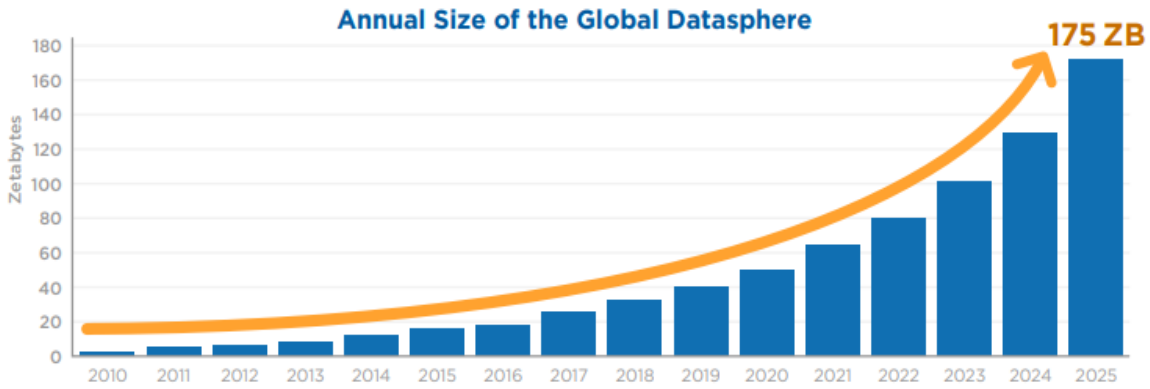
3. Veri Ekonomisine ve Aktarım Rejimlerine Genel Bakış

Son birkaç on yıllık periyot içerisinde teknolojik gelişmelerin hızla ilerlemesi, insanlık tarihinde görülmemiş bir hızla veri artışına sebep olmuş ve veriyi elde tutmak, verinin paylaşılması ve uygun alanlarda kullanılması ekonomilerin temeli haline gelmiştir. Hayatın ve ekonominin her alanında yer bulan veri; ekonomik büyüme, istihdam yaratma ve toplumsal gelişmenin vazgeçilmez bir kaynağı haline gelmiştir. Bu bağlamda veri analitiği sayesinde süreçlerin ve kararların optimize edilmesi sağlanmış, inovasyon tetiklenirken gelecek öngörülerinde kesinlik artmıştır. Bu küresel eğilim, sağlık, çevre, gıda güvenliği, iklim ve kaynak verimliğinden enerji, akıllı ulaşım ve akıllı şehirlere kadar birçok alanda uygulama imkanı bulmuş ve "veri ekonomisi" diye adlandırılan yepyeni bir ekosistemin ortaya çıkmasına neden olmuştur.

En temel özelliği üreticiler, araştırmacılar ve altyapı sağlayıcıları gibi birçok farklı pazar oyuncusunun verinin erişilebilir ve kullanılabilir olmasını sağlamak amacıyla iş birliği yapması olan veri ekonomisindeki bu iş birliği sayesinde günlük yaşamı iyileştiren birçok uygulamanın oluşturulması, verinin üretimi ve kullanılması ile sağlanmaktadır[68].

Nitekim, veri ekonomisinin son yıllarda global ölçekte yaratmış olduğu verinin büyüklüğü, araştırmalara da yansımış, Kasım 2018'de IDC tarafından yayımlanan "*The Digitization of the World From Edge to Core (Dünyanın Dijitalleşmesi- Kenardan Çekirdeğe)*[69]" isimli raporda ("**IDC Raporu**"), 2010 yılı itibariyle yıllık küresel veri dünyası büyüklüğünün 20 zettabayttan 2018 yılında 33 zettabayta çıktığı tespit edilmiş ve 2025 yılında ise 175 zettabyta çıkacağı öngörüsünde bulunulmuştur.

Yıllık Küresel Veri Dünyası Büyüklüğü



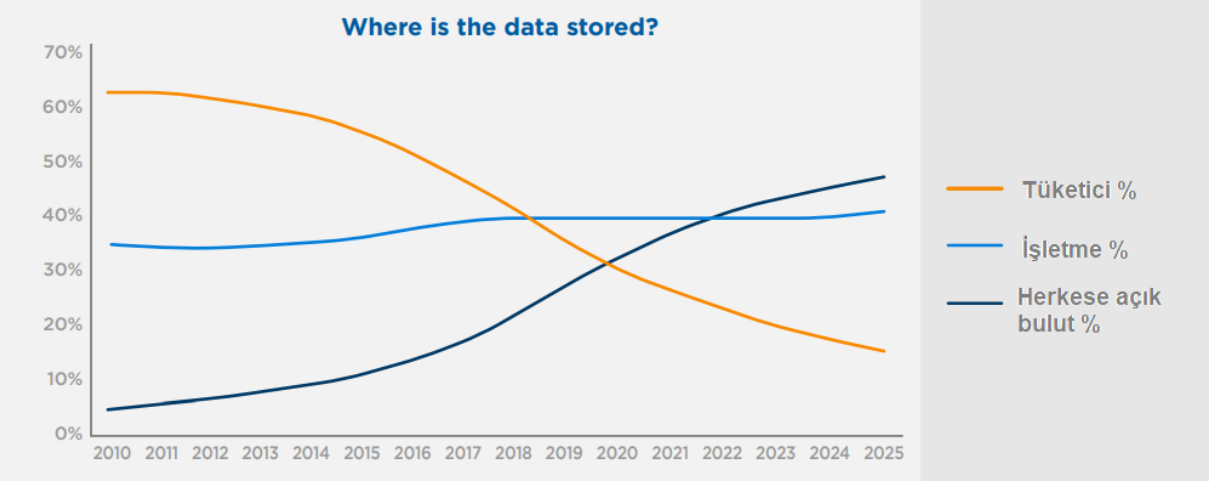
[68] "Communication on Building a European Data Economy," European Commission, son güncelleme 10 Ocak, 2017, https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy.
[69] "The Digitization of the World: From Edge to Core," IDC, son güncelleme Kasım, 2018, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

Benzer bir artış oranı, Şubat 2019'da yayımlanan "European Data Strategy (Avrupa Veri Stratejisi)[70]" nde de öngörülmüştür. IDC tarafından yayımlanan raporda olduğu gibi Avrupa Veri Stratejisi'nde de küresel veri hacminin %530 oranında artış göstereceği belirtilmiş olup AB üye devletleri veri ekonomisinin ise 2025 yılında, 2018 yılındaki 301 milyar Euro değere göre artış göstererek 829 milyara ulaşacağı öngörülmüştür. Avrupa Veri Stratejisi aynı zamanda nüfusun da dijitalleşme konusunda ilerleme kaydedeceğini öngörmüş ve nüfus içerisinde veri uzmanlarının sayısı ve temel dijital becerilere sahip kesimin oranına ilişkin çarpıcı rakamlar sunmuştur.

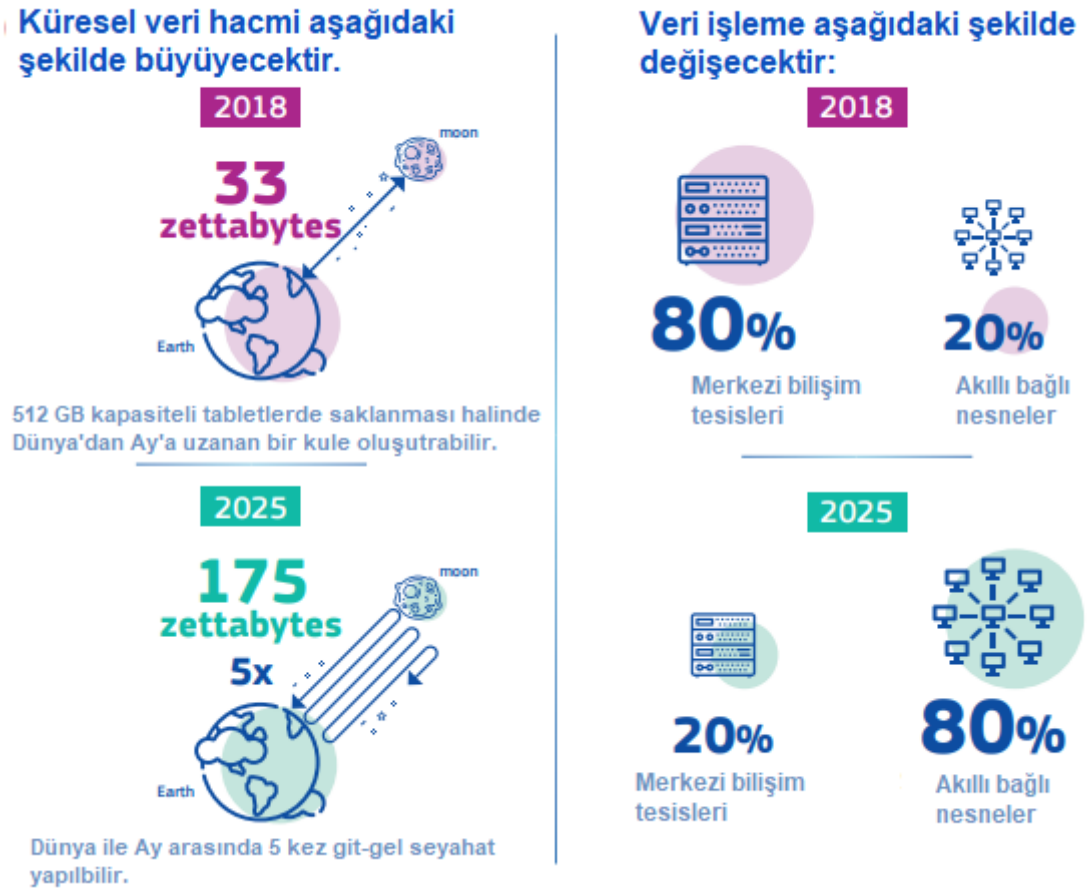
Veri ekonomisinin ve buna bağlı olarak üretilen ve kullanılan verinin büyüklüğünün artmasının yanı sıra, verilerin saklandığı yerler/kişiler ve verilerin işleyiş şekilleri de değişim göstermektedir. IDC Raporu'na göre, zaman içerisinde tüketicilere ait cihazlarda saklanan verilerin oranı düşüş trendi göstermekte ve 2020 yılında tüketicilerin elindeki cihazlarda saklanan verilerin oranı ile herkese açık bulutlarda saklanan verilerin oranın eşitlenmesi beklenmektedir. 2025 yılına gelindiğinde ise yaklaşık %50 ile herkese açık bulutta saklanan verilerin geleneksel veri saklama yöntemlerinin önüne geçmesi öngörülmektedir.

[70] "European Data Strategy," European Commission, son güncelleme 19 Şubat, 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

Veriler nerede saklanmaktadır?



Değişim yalnızca bunlarla sınırlı kalmamaktadır. Avrupa Veri Stratejisi, 2018 yılında %80 oranında merkezi bilişim tesislerinde yapılan veri işleme faaliyetlerinin 2025 yılına gelindiğinde tam tersi yönde bir değişim göstereceği ve veri işleme faaliyetlerinin geleneksel yollardan uzaklaşarak %80 oranında akıllı bağlı nesneler tarafından gerçekleşeceği öngörülmektedir.

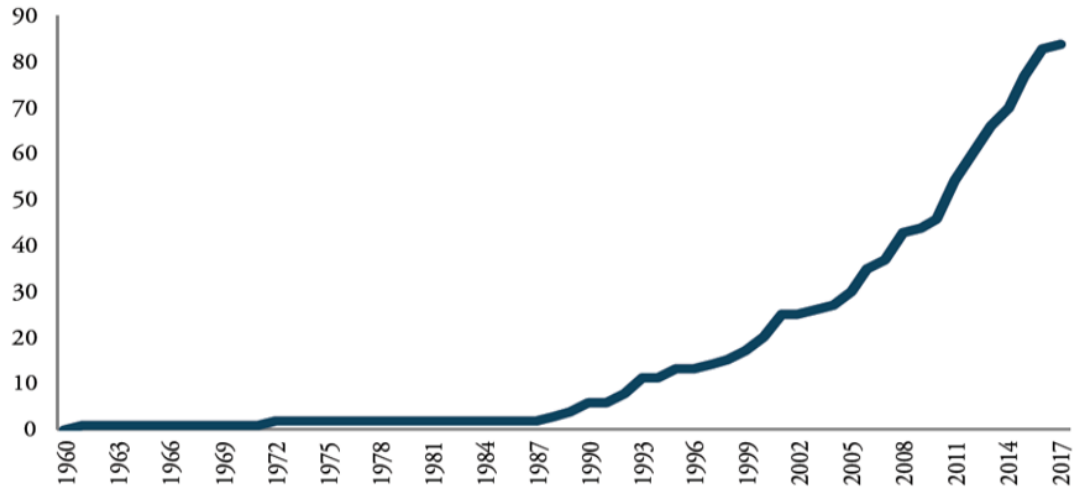


Veri ekosistemindeki tüm bu değişimler, verinin değerini artırmış, öte yandan geleneksel olarak belirli merkezlerde ve fiziksel mekanlarda tutulan verilerin yurt içinde ve sınır ötesi akışları, özellikle teknoloji kullanımı ile, hız kazanmıştır. İnternet ve bulut bilişim hizmetlerinin yaygınlaşması ile paralel olarak artan veri aktarımı, beraberinde birtakım endişeleri de getirmiştir. Verinin ekonomik varlık haline dönüşmesi ile rekabetçi gücü elinde bulundurmak ve fayda elde etmek isteyen ülkeler, 1970'li yıllar itibariyle sınır ötesi veri aktarımına ilişkin birtakım kısıtlamalar getirmeye başlamışlardır. Ayrıca, çevrimiçi ortamlarda oluşturulan bilgiler üzerinde ve bunlara erişimde kontrol sağlama, vatandaşlarını olası müdahale ve zararlardan korumak isteyen devletlerin, bu tür kısıtlamalar getirmesinde saikleri olmuştur. Özellikle verilerin aktarıldığı bazı ülkelerin yeterli koruma sağlamayacağının düşünülmesi, mahremiyet endişelerini doğurmuş, tüketiciyi koruma eğilimi ile de birleşince sınırlamaların artmasına sebep olmuştur[71]. Öte yandan, zaman içerisinde veri kaynaklı dış tehditlerin artması ile verilerin korunması milli güvenlik meselesi haline gelmiş, bunun neticesinde devletler, milli güvenlik, kamusal güvenlik, kamu yararı, siber güvenlik ve bilgi güvenliği gibi sebeplerle veri aktarımını sınırlama sebepleri olarak ortaya çıkmıştır. Bunların yanı sıra, denetim, yasaların uygulanması, ticari/müşteri sırlarının korunması gibi sebepler ile farklı ülkelerde farklı seviye korumaların öngörülmesi de sınır ötesi aktarımların kısıtlanması sonucunu doğurmuştur.

Avrupa Uluslararası Politik Ekonomi Merkezi (*ECIPE*) tarafından oluşturulan 2018 Dijital Ticaret Sınırlılık Endeksi (*Digital Tade Restrictiveness Index*) verilerinden oluşturulan aşağıdaki grafik de göstermektedir ki, her ne kadar sınır ötesi veri aktarımı sınırlamaları yeni bir olgu olmasa da, son on yıllık periyotta oldukça yaygınlaşmıştır. Sıkı mahremiyet rejimleri, yerel veri merkezlerinin kullanılması talepleri ve yurt dışına aktarımın doğrudan yasaklanması, ulusal ve bölgesel düzeyde kısıtlama getiren yakın zamanlı uygulamalara örnek teşkil etmektedir[72].

[71] "Data protection regulations and international data flows: Implications for trade and development," UNCTAD, son güncelleme 19 Nisan, 2016, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
[72] Martina F. Ferracane, *Restrictions on Cross-Border data flows: a taxonomy* (ECIPE: 1/2017), https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf.

Sınır Ötesi Veri Aktarımına Yönelik Getirilen Sınırlamaların Kümülatif Sayısı



Getirilen bu kısıtlamalar, her ülkede aynı şekilde yansıma bulmamış, veri aktarımını kısıtlayan çeşitli yapılar ortaya çıkmıştır. Öte yandan, rejimler farklılık göstermekle beraber hepsi, özel teşebbüsleri fiili olarak verileri lokalize etmeye zorlamakta veya yurt dışına verilerin aktarılması veya yurt dışında verilerin işlenmesi hususlarında daha yüksek maliyetler öngörmektedir. Ancak, bu sınırlamalar, sektörel veya veri tipi bazında farklılıklar gösterebilmektedir.

Bu çerçevede sınır ötesi veri aktarımlarına getirilen kısıtlamalar özel olarak veri lokalizasyonunu öngördüklerinde "katı", aktarım konusunda belirli koşulların yerine getirilmesini öngördüklerinde "koşullu" olarak sınıflandırılmaktadırlar. Bu şekilde sınıflandırma yapılmakla birlikte her iki tür rejim de veri aktarım maliyetlerini aktarmakta ve çeşitli derecelerde veri lokalizasyonu gerektirmektedir[73].

[73] Ferracane, "Restrictions on Cross-Border data flows".

Veri Aktarımına İlişkin Farklı Rejimler[74]

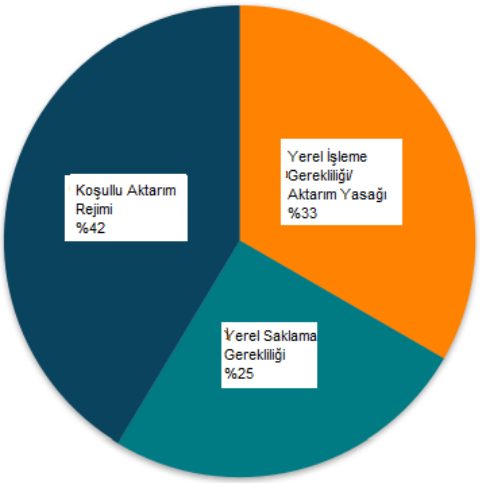
Bu çerçevede katı ve koşullu sınırlandırmalar, temel olarak şu şekilde sınıflandırılabilecektir:

1. Katı sınırlandırma rejimi
   a. Yerel saklama gerekliliği
   b. Yerel saklama ve işleme gerekliliği
   c. Veri aktarım yasağı (yerel saklama, işleme ve erişim gerekliliği)
2. Koşullu sınırlandırma rejimi
   a. Koşulların veri aktarılan ülkelere uygulandığı rejim
   b. Koşulların veri sorumlusu veya veri işleyene uygulandığı rejim[75]

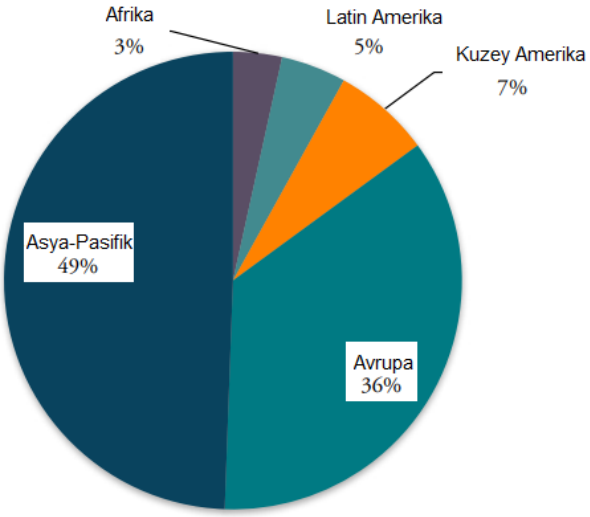
ECIPE veritabanından elde edilen verilerle 64 ekonomide yürürlükte olan veri aktarım kısıtlamaları farklı rejim türleri, bölge, sektör ve veri tipi açısından incelenmiştir.

Buna göre, 64 ülke tarafından getirilmiş olan 87 farklı önlem incelendiğinde, aktarım sınırlamalarının %42'sinin koşullu bir rejim öngördüğü, %33'ünün ise yerel işlemeyi gerektirdiği veya aktarım yasağı getirdiği görülmektedir.

[74] "Exploring International Data Flow Governance Platform for Shaping the Future of Trade and Global Economic Interdependence," World Economic Forum, son güncelleme 17 Aralık, 2019, http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.
[75] Ferracane, "Restrictions on Cross-Border data flows".

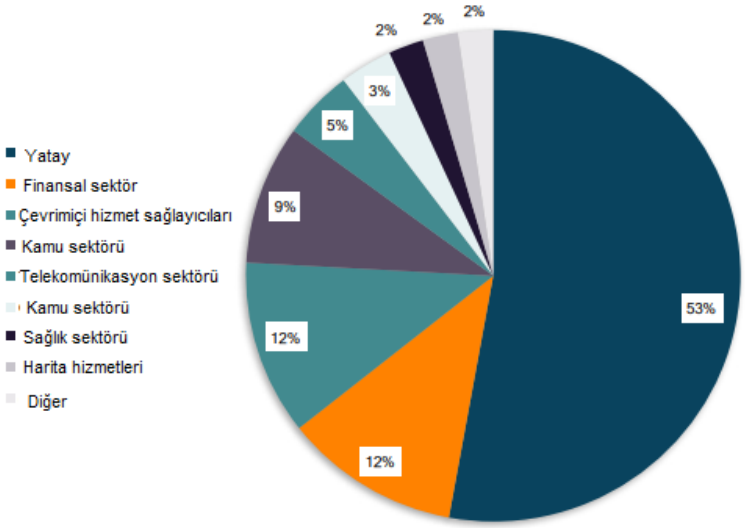


Bölgesel anlamda incelendiğinde ise sınırlamalarda %49 oranla Asya-Pasifik bölgesinin lider olduğu, bu bölgeyi ise %36 ile Avrupa'nın takip ettiği görülmektedir.

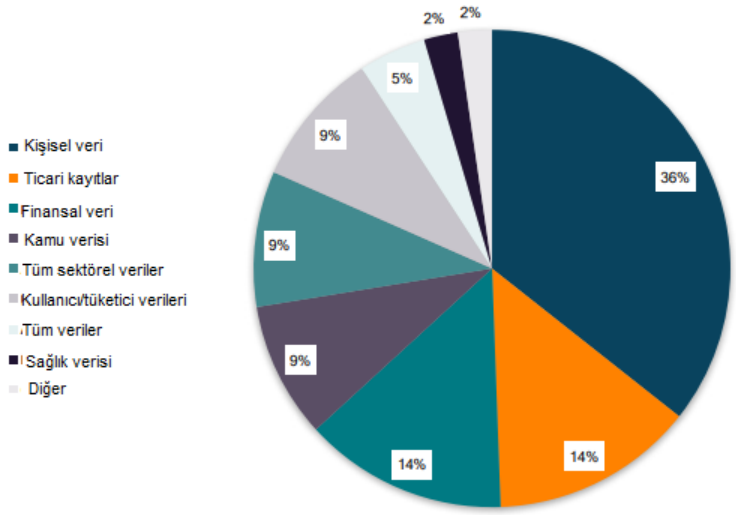


Veri aktarımına ilişkin kısıtlamalar sektörler açısından incelendiğinde ise %53 oranla kısıtlamaların sektör spesifik olmadığı, tüm sektörleri yatay olarak kesen genel düzenlemeler öngördüğü anlaşılmaktadır. Öte yandan araştırma, veri aktarım yasaklarının ve yerel saklama gerekliliklerinin sektör-spesifik olarak getirildiğini, koşullu aktarım rejimlerinin ise yatay düzenleme getirme eğiliminde olduğunu tespit etmiştir[76].

[76] Ferracane, "Restrictions on Cross-Border data flows".



Son olarak, veri tipleri açısından inceleme yapıldığında ise sınırlamaların %36'sının kişisel verilere ilişkin olduğu göze çarpmaktadır. Öte yandan, gelişen teknoloji nedeniyle kişisel verileri kişisel olmayan verilerden ayırmanın giderek zorlaşması ve maliyetlerin artması nedeniyle kişisel verilere ilişkin kısıtlamaların yatay bir etki doğurduğu ifade edilmektedir[77].



Veri temelli ekonomiye ve veri sirkülasyonuna ilişkin bu rakamlar genel resmi ortaya koymakla beraber işbu rapor bağlamında detaya inildiğinde, Avrupa Veri Stratejisi'nde veri koruma hukukuna ilişkin birtakım önemli açıklamalara yer verildiğini görmekteyiz. Veri akışına ilişkin yasal düzlem incelendiğinde ABD'de özel sektörün, Çin'de ise devlet gözetimi olmakla beraber yine büyük teknoloji şirketleri kontrolünde bir veri akışı görülmektedir. Veri koruma ve gizlilik perspektifinden bakıldığında ise karşımıza Avrupa Birliği'nin "veri akışı ve verinin geniş kapsamlı kullanımı" ile "gizlilik, güvenlik, koruma ve etik standartlar"ı birleştirdiği GDPR çıkmaktadır. Eklemek gerekir ki GDPR'ın

[77] Ferracane, "Restrictions on Cross-Border data flows".

güncellenecek versiyonunun bu anlamda daha elverişli araçlar getireceği düşünülmektedir. Bununla beraber Avrupa Veri Stratejisi veri konusunda sadece GDPR odaklı yaklaşmamakta, kişisel olmayan verilere[78], siber güvenliğe[79] ve açık veriye[80] ilişkin hukuki düzenlemeleri de dikkate almaktadır. Kişisel veri kapsamında olmakla beraber birtakım sektör-spesifik düzenlemelere de Avrupa Veri Stratejisi kapsamında yer verilmektedir; otomotiv[81], ödeme hizmetleri[82], akıllı sayaç bilgileri[83], elektrik ağı verisi[84], akıllı taşıma sistemleri[85].

Yasal düzenlemelere dikkat çeken Avrupa Veri Stratejisi, veri temelli uygulamalarda söz konusu güncel konuları değerlendirirken yine GDPR'ı göz önünde bulundurmuş ve şu hususlara değinmiştir; GDPR'ın 20. Maddesi veri taşınabilirliğine ilişkin olup yeni veri akışlarına imkan verebilecektir. Veri taşınabilirliğine ilişkin hakkın hem ilgili kişilerin kendi verileri üzerindeki kontrolünü artırıcı bir husus olduğu belirtilmekte (ve hatta "anahtar aksiyon" olarak sayılmıştır), hem de bu kapsamdaki veri aktarımlarının rekabete etkisine ilişkin çalışmalara atıf yapılmaktadır[86].

---

[78] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018, *Official Journal of the European Union* L 303/59, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN.

[79] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019, *Official Journal of the European Union* L 151/15, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

[80] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, 2019, *Official Journal of the European Union* L 172/56, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN.

[81] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, 2007 (amended in 2009), *Official Journal of the European Union* L 171/1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02007R0715-20121231&from=EN.

[82] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 2015, *Official Journal of the European Union* L 337/35, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

[83] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, 2019, *Official Journal of the European Union* L 158/125, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944&from=EN ve Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, 2009, *Official Journal of the European Union* L 211/94, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0094:0136:en:PDF.

[84] Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation, 2017, *Official Journal of the European Union* L 220/1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1485&from=EN ve Commission Regulation (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules, 2015, *Official Journal of the European Union* L 113/13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0703&from=EN.

[85] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, 2010, Official Journal of the European Union L 207/1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040&from=EN.

[86] "Unlocking digital competition: Report of the Digital Competition Expert Panel," Digital Competition Expert Panel, son güncelleme 13 Mart, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

Avrupa Veri Stratejisi ile getirilen strateji ise dört temel üzerinde kurgulanmıştır; (i) veriye erişim ve verinin kullanımı için sektörler arası yönetişim çerçevesinin oluşturulması ve bu kapsamda gerekli yasal enstrümanların oluşturulması ve dijital ekonomide verinin öneminin analiz edilmesi (ii) verinin barındırılması, işlenmesi ve kullanılması için mevcut kabiliyet ve altyapının güçlendirilmesi ve veriye yatırım yapılması, (iii) bireylerin güçlendirilmesi, yeteneklere ve genel veri okuryazarlığına yatırım yapılması, KOBİ'ler için kapasite oluşturulması (yukarıda bahsedilmiş olan veri taşınabilirliği üzerine çalışmalar bu kapsamdadır) ve (iv) stratejik sektörlerde ve kamu yararı olan alanlarda ortak strateji oluşturulması. Stratejiye ilişkin bu ana başlıklar altında getirilen açıklamaların ardından "açık ancak proaktif bir uluslararası yaklaşım" üzerinde durulmuştur. Bu kapsamda veri akışlarının ölçülmesi için bir çerçeve oluşturulması ve bu akışın ekonomik değerinin tahmin edilmesi aksiyonlarının 2021 yılında tamamlanması öngörülmüştür. Görüldüğü üzere Avrupa Birliği'nin öngördüğü stratejilerin temelinde mevcut durumun kavranması ve uluslararası bir perspektiften yatırımların ve yasal enstrümanların geliştirilmesi yatmaktadır.

4. Avrupa Birliği ve Türk Hukukunda Kişisel Veri Aktarım Mekanizmalarının Karşılaştırmalı Analizi

3.1 Avrupa Birliği'nde Uluslararası Veri Aktarımı

Avrupa Birliği mevzuatında GDPR, kişisel verilerin AEA içerisinde serbest akışını temel olarak düzenlemektedir. Bununla beraber AEA dışındaki üçüncü ülkelere ve uluslararası kuruluşlara veri aktarımlarına yönelik özel şartlar da içermektedir. GDPR söz konusu aktarımların önemini tanımakta, özellikle uluslararası ticaret ve iş birliği açısından dikkate almakta, ancak aynı zamanda kişisel verilere yönelik artan riski de göz önünde bulundurmaktadır. Dolayısıyla GDPR, üçüncü ülkelere aktarılan kişisel verilerin AEA içerisinde sahip olduğu koruma düzeyinin sunulmasını amaçlamaktadır (Bkz. GDPR Giriş Hükmü 101 ve 116).

Aynı zamanda belirtmek gerekir ki tüm Avrupa Birliği üye devletlerinin de taraf olduğu bir Avrupa Konseyi enstrümanı olan 108 Sayılı Konvansiyon, 1981 yılından itibaren hem kişisel verilerin korunması için temel prensipleri ortaya koymakta hem de kişisel verilerin aktarımına ilişkin paralel bir rejim oluşturmaktadır. Bu uluslararası anlaşma kişisel verilerin korunması alanında tek bağlayıcı uluslararası metin olup Türkiye dahil toplam 55 ülkenin taraf olduğu bir uluslararası hukuk enstrümandır. Dolayısıyla hem Avrupa Birliği hukukundaki hem de Türk hukukundaki etkileri dikkate alınarak bu belge de inceleme kapsamına alınmıştır. Avrupa Konseyi mevzuatında sınır ötesi veri akışları, kişisel verilerin yabancı bir yargı yetkisine tabi alıcılara aktarılması olarak tanımlanmaktadır. İlgili tarafın yargı yetkisine tabi olmayan alıcılara sınır ötesi veri akışına ilişkin rejim ise yine korumanın

sağlanması üzerinedir. Bu 108 Sayılı Konvansiyon'un dönemin ihtiyaçlarına cevap vermek üzere GDPR'a yakınsanan versiyonu Konvansiyon 108+ ise GDPR-benzeri bir veri korumanın uluslararası kişisel veri aktarımında da sağlanmasını temin edecek niteliktedir.

Hem Avrupa Konseyi hem de AB'nin üçüncü ülkelere veya uluslararası organizasyonlara veri akışına izin vermesine karşın farklı koşullar koymaktadırlar. Her iki koşullar dizini de ilgili kuruluşun farklı yapı ve amaçlarını göz önüne almaktadır. Aşağıda bu rejimler örnekler ve karşılaştırmalar ile özetlenmiştir.

3.1.1. Avrupa Genel Veri Koruma Regülasyonu

Avrupa Birliği mevzuatının temel kişisel veri koruma düzenlemesi olan GDPR, Mayıs 2018'de yürürlüğe girmiştir. GDPR, belirli prosedürleri standartlaştırmış, kişisel verileri işleyen tüzel ve gerçek kişilerden beklenenler için bir paradigma oluşturmuş ve kişilerin verilerinin toplanma ve kullanılma yöntemleri üzerinde kontrol icra etmelerini sağlamak amacıyla bireylerin haklarını geliştirmiştir. GDPR'ın esasen, AEA'da yer alan veri sorumluları ve veri işleyenler nezdinde hüküm ve sonuç doğurmaktadır ve bireyler, kişisel verilerinin AEA dışına çıkarılması halinde GDPR korumasını kaybetme tehlikesiyle karşı karşıya kalacaklardır. Bu sebeple GDPR, AB ve GDPR koruması dışına veri aktarımını, şahısların kişisel verilerinin korunmasına dair haklarının başka bir şekilde tesis edilmesi veya sınırlı sayıdaki birkaç istisnanın bulunması durumları haricinde kısıtlamıştır. Kişisel verilerin yurtdışına aktarımı GDPR 44 ve 50. maddeleri arasında düzenlenmekte olup bu düzenlemeler ile getirilen sistem aşağıda alt kırılımları ile ortaya konulmaktadır. Çalışmanın bu bölümünde ICO'nun GDPR rejimini izah ederken kullanmakta olduğu metodoloji benimsenmiş ve paralel bir şekilde kurallar açıklanmıştır[87].

GDPR uyarınca aşağıdaki durumlarda "sınırlandırılmış aktarım"ın (*restricted transfer*)[88] vuku bulacağı söylenebilecektir:

- Veri aktarımına konu olan veri işleme faaliyeti GDPR'a tabii olmalı,
- Verinin aktarılacağı ülke GDPR'a tabii olmamalı,
- Veri aktarımının alıcısı, göndericisinden farklı bir gerçek ya da tüzel kişi olmalı.

[87] ICO- "International Transfers."
[88] Bu raporda herhangi bir anlam karmaşasına yol açmamak amacıyla sınırlandırılmış aktarım ifadesi yerine "AEA dışına aktarım", "sınır ötesi aktarım" veya yalnızca "aktarım" ifadeleri kullanılmaktadır.

Bu tanım sayesinde belirli kriterlerin bir arada var olması halinde sınırlandırılmış aktarımdan bahsedilebilecektir ancak bu çalışmanın devamında incelenecek rejimin somutlaştırılabilmesi adına öncelikle AEA dışına aktarıma dair birtakım örnekler aşağıda ele alınmıştır.

AEA dışına aktarım konusunda ICO tarafından verilen temel örnek şu şekildedir; bir İngiliz şirketi, ABD'de ana şirketi tarafından sağlanan merkezi bir insan kaynakları hizmetini kullanmaktadır. İngiliz şirketi, çalışanları hakkındaki bilgileri insan kaynakları hizmeti ile bağlantılı olarak ana şirketine iletmektedir ve bu durum bir aktarım teşkil etmektedir.

Ancak belirtmek gerekir ki aktarım, transit geçiş ile aynı anlama gelmemektedir. Bu konuda ICO GDPR Rehberi'nde yer alan örnek ile transit geçiş somutlaştırılmıştır; kişisel veriler, Fransa'daki bir veri sorumlusu tarafından İrlanda'daki bir veri sorumlusuna (her iki ülke de AEA'ya dahil olmak üzere) Avustralya'daki bir sunucu üzerinden aktarılmaktadır. Kişisel verilere Avustralya'dayken erişilmesine veya işbu verilerin manipüle edilmesine dair bir niyet mevcut değildir. Bu nedenle, ilgili örnek kapsamında çıkarım yapıldığında, AEA dışına aktarımın yalnızca İrlanda'ya yapılmış olduğu görülecektir.

Kişilere dair bilgilerin düzenlenmemiş ve yapılandırılmamış bir biçimde kâğıda aktarılması ve akabinde bu kağıtların AEA dışındaki bir hizmet şirketine, (i) dijital forma sokulmak üzere; veya (ii) ilgili kişilere ilişkin yüksek derecede yapılandırılmış otomatik olmayan bir dosyalama sistemine eklenmek üzere gönderilmesi halinde de AEA dışına aktarımdan bahsedilebilecektir.

Bir diğer aktarım görünümü ise internet sitelerine kişisel verilerin eklenmesidir/konulmasıdır ve bu durum çoğunlukla AEA dışına bir aktarımla sonuçlanacaktır. AEA dışına aktarım, AEA dışındaki birinin bu kişisel verilere ilgili internet sitesi üzerinden eriştiği zaman gerçekleşmiş olacaktır.[89]

GDPR, ilgili veri aktarımlarını hukuka uygun hale getirecek üç adet mekanizma tanımlamış ve bu sistemleri detaylandırmıştır. Öncelik sıralarına göre bu mekanizmalar şu şekilde kategorize edilmektedir; (i) yeterlilik kararının varlığı, (ii) güvenlik tedbirlerinin varlığı ve (iii) istisnalardan birinin varlığı.

AEA dışına aktarım araçlarını belirlerken GDPR, aktarım mekanizmaları arasında açık bir hiyerarşi tesis etmiştir. GDPR, Komisyon tarafından belirlenen yeterli korumayı sağlayan ülkelere aktarımı önceliklendirmiştir. Bu şekilde hukuka uygun bir aktarımın gerçekleşmesi için Komisyon tarafından verinin aktarılacağı ülkenin yeterli korumayı haiz olduğunun deklare edilmesi gerekmektedir. Komisyon, veri koruma kurallarını temelde tek bir regülasyonda toplamış ve GDPR'ın ilgili konudaki

[89] ICO- "International Transfers."

yaklaşımına benzer bir yaklaşıma sahip ülkelere ayrıcalık tanıma eğilimindedir. Eğer yeterli korumanın sağlandığına yönünde bir karar mevcut değilse ikinci sırada güvenlik tedbirlerinin varlığının aranması gelmektedir. Bu aşamada güvenlik tedbirlerinin varlığından bahsedebilmek için aşağıdaki enstrümanlardan birinin sağlanmış olması gerekecektir;

- Kamu kurum veya kuruşları arasında oluşturulan yasal olarak bağlayıcı ve uygulanabilir bir araç,
- Bağlayıcı şirket kuralları,
- Komisyon tarafından kabul edilmiş standart veri koruma maddeleri,
- Bir denetleyici otorite tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma maddeleri,
- AEA dışındaki alıcının, bağlayıcı ve uygulanabilir taahhütleriyle birlikte onaylanmış davranış kuralları,
- AEA dışındaki alıcının bağlayıcı ve uygulanabilir taahhütleri ile onaylanmış bir sertifika mekanizması kapsamında sertifikalandırma,
- Denetleyici otorite tarafından onaylanmış sözleşme hükümleri,
- Kamu kurum veya kuruluşları arasında yapılan, kişisel verileri aktarılan şahıslara dair uygulanabilir ve etkili haklar içeren ve bir denetleyici otorite tarafından onaylanmış olan idari anlaşmalar.

Son olarak, güvenlik tedbirlerinin de var olmadığı durumlarda AEA dışına veri aktarımına izin verilen istisnai durumların varlığı halinde yine GDPR'a uygun bir veri aktarımından bahsedilebilecektir.

Aşağıda bu üç aktarım mekanizması hiyerarşik sıralarına uygun olarak ele alınmış ve detaylandırılmıştır.

3.1.1.1. Yeterlilik Kararı (Adequacy Decision)

Avrupa Birliği mevzuatında Komisyon, AEA üyesi olmayan ülkelerin kişisel verilere ilişkin "yeterli korumayı" sağlayıp sağlamadığına karar veren otorite olarak belirlenmiştir[90]. Komisyon ilgili ülkelerin

[90] Söz konusu yetki, Direktif'in 25. maddesinin altıncı fıkrası ve GDPR'ın 45. maddesi kapsamında verilmektedir.

yeterli korumayı sağlayıp sağlamadığına yönelik belirlemeyi "yeterlilik kararı" olarak anılan kararla gerçekleştirmektedir. Komisyon tarafından verilen bir yeterlilik kararı tüm AEA ülkeleri için bağlayıcı olup Komisyon'un yeterli olarak belirlediği ülkelere (istisnalar söz konusu olmakla beraber) sınırlandırılmamış bir şekilde veri aktarımı yapılmasına imkân verir. Zaman geçtikçe Komisyon'un vermiş olduğu yeterlilik kararları bir "beyaz liste" oluşturmuştur. Bu beyaz listede AB ile denk bir koruma sağladığı belirlenmiş olan ülkelere yer verilmiştir. Yeterlilik kararının alınması için;

- Komisyon tarafından bir teklif sunulması,
- EDPB'den görüş alınması, ve
- Kararın Avrupalı Komisyonerlerce kabul edilmesi gerekmektedir.

GDPR da AEA dışındaki ülkelere veri aktarımı yapılmasına imkân veren yeterlilik kararlarının verilmesinde Komisyon'un yetkili olacağını öngörmüştür. Hatta, GDPR, Komisyon'un yeterlilik kararı verme yetkisini genişletmiştir. GDPR uyarınca Komisyon'un AEA dışındaki ülkenin yeterli korumayı haiz olduğuna karar vermesine ek olarak Komisyon, üçüncü bir ülkenin *spesifik bir bölgesinin ya da sektörünün* yeterli korumayı haiz olduğuna dair de karar verebilmektedir.[91]İşbu durum, belirli bir ülkedeki çocukların gizlilik yasaları veya telekomünikasyon gizlilik yasaları gibi sektörel veri gizliliği mevzuatının yeterli olabileceği anlamına gelmektedir. Fakat bu durum sektörlerin sınırlarının belirlenmesi hususunda yapılacak yorumları güçleştirmektedir (sağlık sektörünün tam olarak neleri kapsadığının belirlenmesinin teşkil ettiği zorluk örnek verilebilecektir). Endüstrilerin ve sektör oyuncuları fazlasıyla iç içe olduğu için bu belirlemenin yapılabilmesi oldukça güç olacaktır.[92] Kısmi yeterlilik kararı (*partial adequacy decision*) olarak da anılan işbu duruma Kanada, Amerika Birleşik Devletleri (ABD) ve Japonya'nın haiz olduğu yeterlilik kararları örnek gösterilebilir.

Komisyon'un yeterlilik kararı verirken gözeteceği asgari unsurlar şu şekildedir:

- Temel veri koruma kavramlarının ve/veya ilkelerinin mevcut olması,
- Verinin hukuka uygun, adil ve meşru bir şekilde işlenmesi,
- Verinin belirli bir amaçla sınırlı olarak işlenmesi (*Amaçla Sınırlı Olma İlkesi*),

[91] Söz konusu yetki, GDPR'ın 45. maddesinin üçüncü fıkrasında verilmiştir.
[92] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."

- Verinin doğru ve güncel olması (*Veri Kalitesi İlkesi*),

- Verinin işleme amacıyla orantılı olması (*Orantılılık İlkesi*),

- Verinin işleme amacının gerçekleştirilmesi için yeterli olan süreden fazla saklanmaması (*Veri Saklama İlkesi*),

- Verinin güvenliği için teknik ve idari tedbirlerin alınması (*Güvenlik ve Mahremiyet İlkesi*),

- İlgili kişilerin verilerinin işlenmesi konusunda açık bir şekilde bilgilendirilmeleri (*Şeffaflık ilkesi*),

- İlgili kişinin erişim, düzeltme, silme ve itiraz haklarının bulunması,

- Veri aktarımının ilk alıcısı tarafından yapılacak aktarımlara, diğer alıcının, yeterli düzeyde koruma sağlayan kurallara tabi olması ve veri sorumlusu adına veri işlerken ilgili talimatları izlemesi durumlarında izin verilmesi *(İleride gerçekleştirilecek aktarımların kısıtlanması*),

- Aktarım yapılan ülkenin veri koruma, ulusal güvenlik ve ileriye dönük aktarımlar hakkındaki yasaları ve içtihatları ve bunların pratikte nasıl uygulandığı ve icra edildiği,

- Veri koruma yasalarına uyumu sağlayacak ve işbu yasaları icra edecek bağımsız denetleyici otoritelerin varlığı (ya da yokluğu),

- Aktarım yapılan ülkenin verilerin korunmasına ilişkin uluslararası taahhütleri.

Yeterlilik kararının alınmasının yanında GDPR'ın 45. maddesinin üçüncü fıkrasında, Komisyon kararlarının dinamik olmasını ve en az dört yılda bir gözden geçirilmesi gerektiği öngörülmektedir. Ayrıca, aynı maddenin beşinci fıkrası gereğince Komisyon'un beyaz listede yer alan ülkeleri "devam eden bir biçimde" yeterlilik kararını etkileyecek koşulların ortaya çıkıp çıkmadığı bahsiyle takip etmesi beklenmektedir. Yeterlilik kararının dinamik yapısı ve önemi nedeniyle Komisyon, ilgili ülke hakkında vermiş olduğu yeterlilik kararını ilgili ülkeye bildirimde bulunup cevap verme imkânı tanımasının akabinde herhangi bir zamanda iptal etme yetkisini de haizdir.

Eklemek gerekir ki GDPR, Direktif'in yürürlükte olduğu dönemde Komisyon tarafından alınan yeterlilik kararlarının değiştirilmemesine veya iptal edilene kadar geçerli olacağını öngörmektedir. Dolayısıyla yeterli koruma sağladığı belirtilen ülkelerin yer aldığı Komisyon'un beyaz listesi GDPR kapsamında geçerliliğini sürdürmeye devam etmektedir.

3.1.1.1.1. Gizlilik Kalkanı (EU-U.S. *Privacy Shield Framework*)[93]

GDPR kapsamında Amerika Birleşik Devletleri'ne yapılan veri aktarımı rejimini ayrı bir başlık altında değerlendirme uygun olacaktır zira Gizlilik Kalkanı isimli mekanizma kendine has özellikler barındırmaktadır. Gizlilik Kalkanı'ndan önce AB ile Avrupa Birleşik Devletleri arasındaki kişisel veri aktarımının hukuki kaynağı ise Güvenli Liman (*Safe Harbor*) veri aktarımı rejimi idi. Ancak 6 Ekim 2015'te Avrupa Birliği Adalet Divanı, "Schrems v (İrlanda) Veri Koruma Komisyoneri"[94] kararında Güvenli Liman'ın yeterli korumayı sağlamaması nedeniyle bu hukuki dayanağa ilişkin kararın geçersiz olduğuna ve Güvenli Liman'ın veri aktarımı için kullanılamayacağına hükmetmiştir. 12 Temmuz 2016'da ise Avrupa Komisyonu AB-ABD Gizlilik Kalkanı Çerçevesi'nin AB mevzuatı uyarınca veri aktarımı için yeterli olduğuna karar vermiştir[95].

Gizlilik Kalkanı, şirketlerce kendi kendilerine sertifika verilen bir sistem olup bu sertifika ile şirketler, "Gizlilik Kalkanı İlkeleri"ne uymayı taahhüt eder. Gizlilik Kalkanı İlkeleri şu şekilde listelenebilecektir: **i)** Bildirim, **ii)** Seçim, **iii)** Gelecek Aktarımlar için Hesap Verilebilirlik, **iv)** Güvenlik, **v)** Veri Bütünlüğü ve Amaçla Sınırlı Olma, **vi)** Erişim ve **vii)** Başvuru, Uygulama ve Sorumluk[96].

Gizlilik Kalkanı'na dair önemli hususlar aşağıdaki şekilde özetlenebilecektir[97];

- Bildirim: Şirketler, veri işleme faaliyetleri ve tüketicinin Gizlilik Kalkanı altındaki haklarıyla ilgili program kapsamında belirlenmiş on üç maddeyi[98] içeren, açık ve belirli gizlilik politikaları oluşturmalıdır. Uygulamada bu ilke; süreçlerin haritalandırmasını, açıkların değerlendirilmesini ve gizlilik bildirimlerindeki güncellemeleri gerektirmektedir.

- Seçim: Şirketlerin, verileri topladıkları amaçlardan "maddi olarak farklı" bir amaç için veri işlemeyi düşündükleri herhangi bir zamanda veri sahibine vazgeçme imkânı tanımaları ve yeni ve farklı amaçlarla hassas nitelikli veri işleyecekler ise bunun için ayrıca bir açık rıza almaları

[93] "Welcome to the Privacy Shield," The International Trade Administration (ITA)- U.S. Department of Commerce, erişim 18 Şubat, 2020, https://www.privacyshield.gov/welcome.
[94] "Maximillian Schrems v Data Protection Commissioner" kararının İngilizce metnine (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362) adresinden ulaşılabilir.
[95] Yeterlilik kararının tam metni: Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016, *Official Journal of the European Union* L 207/1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.
[96]"Privacy Shield Framework," The International Trade Administration (ITA)- U.S. Department of Commerce, erişim 18 Şubat, 2020, https://www.privacyshield.gov/EU-US-Framework.
[97] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[98] "Notice," The International Trade Administration (ITA)- U.S. Department of Commerce, Erişim 18 Şubat, 2020, https://www.privacyshield.gov/article?id=1-NOTICE.

gerekmektedir. Bu ilke, süreçlerin haritalandırılmasını, yetkili kullanıcıların belirlenmesini ve mevcut vazgeçme mekanizmalarının açıklarının değerlendirilmesini gerektirmektedir.

- İlgili Kişiler için İyileştirilmiş Çözümler: Gizlilik Kalkanı uyarınca, şirketlerin bir takım uyuşmazlık çözümü mekanizmaları ile uyumlu olmaları gerekmektedir:

  - İlgili kişiler, veri sorumlusu olan şirkete doğrudan şikâyette bulunabilirler. Şirket, 45 gün içerisinde bu şikâyeti cevaplandırmakla yükümlüdür.

  - Şirketler "bağımsız bir başvuru mekanizması" (temel olarak bir arabuluculuk) belirlemek ve iş birliği yapmakla yükümlüdür. Şirketler, arabuluculuk sağlayıcısının kim olduğunu tüketicilerine bildirmeli ve tüketicilerin şikâyette bulunmalarını (ve arabuluculuğa başvurmalarını) ücretsiz olarak sağlamalıdır.

  - AB vatandaşları yerel veri koruma otoriteleri aracılığıyla Gizlilik Kalkanı şirketlerine karşı şikâyette bulunabilmelidirler. Veri koruma otoriteleri ise bu şikayetleri ABD Ticaret Bakanlığı'na[99] (*U.S. Department of Commerce*) gönderecek olup bu şikayetler, ilgili kişiden ücret talep edilmeden incelenecektir.

  - Kişiler, yukarıda sayılan üç yönteme başvurmalarından sonra özel bir Gizlilik Kalkanı tahkim süreci başlatabilirler. Gizlilik Kalkanı şirketleri bu tahkimin sonucuyla bağlı olacaklardır.

  - Alternatif olarak, ABD şirketleri tüketici şikayetlerini çözmek için doğrudan Avrupa veri koruma otoriteleri ile çalışmayı seçebilmektedir.

- Veri Sorumlusundan Veri Sorumlusuna (C2C) İkincil Aktarım: Gizlilik Kalkanı, bir şirketin veri sorumlusu olarak başka bir şirkete veri aktarımı gerçekleştirilebilmesi için şu koşulları belirlemiştir;

  - Kişilerin aktarımın alıcısının "türü ya da kimliği" ve aktarımın amacı hakkında bilgilendirilmesi,

  - Kişilere aktarıma izin vermeme (*opt out*) imkanının verilmesi; ve

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

- Alıcının **i)** kişinin rıza göstermiş olduğu amaçlarla sınırlı olarak veriyi işleyeceğine ve **ii)** Gizlilik Kalkanı kapsamında gerekli görülen koruma düzeyi ile "eşdeğer bir koruma düzeyi" sağlayacağına dair aktarım alıcısı ile yazılı bir anlaşma yapılması.

- Veri Sorumlusunda Veri İşleyene (C2P) Aktarım ve Tedarikçi Yönetimi: Gizlilik Kalkanı, veri işleyenlerle olan tüm ilişkilerde temel teşkil edecek yazılı bir anlaşmanın varlığını aramaktadır. Dolayısıyla dış kaynak işleme faaliyetleri için bir sözleşme veya tedarikçi yönetim programı temin edilmesi gerekmektedir. Bu sözleşmesel ilişkinin yönetilmesi kapsamında tedarikçilerin denetlenmesi ve durum değerlendirmesine ilişkin *due diligence* süreçlerinin gerçekleştirilmesi de yer almaktadır. Gizlilik Kalkanı İlkeleri'nin tedarikçiler tarafından herhangi bir şekilde ihlal edilmesi durumunda ise Gizlilik Kalkanı şirketleri sorumlu tutulacaklardır.

- Doğrulama: Gizlilik Kalkanı uyarınca şirketler, her yıl Gizlilik Kalkanı İlkeleri'ne uyumlu olduklarını teyit etmeli ve gizlilik politikalarının gerçeği yansıttıklarını doğrulamalıdırlar. Doğrulama işlemi ilgili şirket tarafından bizzat ya da üçüncü kişi denetçilerce yapılabilmektedir. Eğer doğrulama işlemi şirketin kendisi tarafından gerçekleştirilecekse bir yetkili tarafından imzalı onayı gerekmekte olup bu onay ABD Federal Ticaret Komisyonu (*Federal Trade Commission- FTC*) ya da ABD Ulaştırma Bakanlığı (*Department of Transportation- DOT*) tarafından herhangi bir zamanda talep edilebilmektedir.

- Devam Eden Yükümlülükler: Gizlilik Kalkanı nezdinde kişisel veri elde eden herhangi bir şirket ilgili kişisel verileri elinde bulundurduğu sürece -şirket Gizlilik Kalkanı programından ayrılsa veya çıkarılsa dahi- Gizlilik Kalkanı İlkeleri'ni uygulamalıdır.

3.1.1.2. Güvenlik Tedbirlerinin Varlığı (Appropriate Safeguards)

İlgili kısıtlanmış veri aktarımı hakkında bir ülkeye, bölgeye veya sektöre dair alınmış bir yeterlilik kararı bulunmaması durumunda, GDPR'da sayılan "güvenlik tedbirleri"nin sağlanması ile bahsi geçen veri aktarımı gerçekleştirilmektedir. Bu güvenlik tedbirleri; hem alıcı hem de gönderici tarafından, ilgili kişilerin kişisel verileri kapsamındaki hak ve özgürlüklerinin korunmasını sağlamaktadır.

Bu çerçevede güvenlik tedbirlerinin ve GDPR'ın diğer hükümlerine uyumun sağlanmasının akabinde yurt dışına veri aktarımı gerçekleştirilebilecektir. Güvenlik tedbirleri GDPR'ın 46 ve 47. maddelerinde düzenlenmiş olup bu güvenlik tedbirleri sekiz ana enstrüman ile sağlanabilmektedir. Her bir güvenlik tedbirine ilişkin açıklamalar ve detaylara aşağıdaki ilgili başlıklarda yer verilmiştir.

3.1.1.2.1. Kamu Otoriteleri veya Organları Arasında Oluşturulan, Yasal Olarak Bağlayıcı ve İcra Edilebilir Enstrümanlar (*Legally Binding and Enforceable Instrument Between Public Authorities or Bodies*)

İki kamu otoritesi veya organı arasında oluşturulan, kişisel verileri aktarılan ilgili kişilerin hakları için "uygun güvenlik tedbirleri" sağlayan ve hukuken bağlayıcı ve icra edilebilir olan bir hukuki araç ile kısıtlı bir aktarım yapabilir. 'Uygun güvenlik tedbirleri', kişisel verileri aktarılan kişiler için uygulanabilir hakları ve etkili çözümleri içermelidir.

Yasal olarak bağlayıcı ve icra edilebilir bu araçlara katılma yetkisini haiz olmayan kamu kurum veya kuruluşları, uygulanabilir ve etkili bireysel haklar içeren bir idari düzenleme oluşturarak veri aktarımını gerçekleştirebilirler.

3.1.1.2.2. Bağlayıcı Şirket Kuralları (Binding Corporate Rules)

Bağlayıcı şirket kuralları, bir şirket grubundaki sınır ötesi aktarımlar dahil olmak üzere kişisel verilerin işlenmesi için geçerli ilkeleri ve kuralları belirleyen şirket içi davranış kurallarıdır.

GDPR, bağlayıcı şirket kurallarını şirket grupları içindeki kişisel verilerin aktarımı için yasal bir temel olarak açıkça kabul etmektedir. Ek olarak, ortak bir ekonomik faaliyette bulunan teşebbüs grupları da bağlayıcı şirket kuralları için başvurabilirler. GDPR, bahsi geçen bu teşebbüs gruplarını örneklendirmemiş olmakla birlikte, bir sadakat programı nezdinde iş birliği yapan havayolu şirketleri veya adi ortaklıklar bu kapsamda düşünülebileceklerdir[100]. GDPR, veri sorumlularının yanı sıra veri işleyenlere de kendi bağlayıcı şirket kurallarını oluşturma imkânı tanımaktadır.

Bağlayıcı şirket kurallarının değerlendirilmesi ise Komisyon'un yetkisi kapsamında düzenlenmemiştir. Özetle; şirketlerden birinin kurulu olduğu AB üye üyesinde yer alan AB denetleyici otoritesine onay için bağlayıcı şirket kurallarının iletilmesi gerekmektedir. GDPR kapsamında veri sorumluları ve veri işleyenlerin bağlayıcı şirket kuralları için baş denetleyici otoriteyi seçme ölçütlerine "Bağlayıcı Şirket Kurallarının Onaylanmasına İlişkin İş Birliği Prosedürü Hakkında Çalışma Belgesi"nde[101] yer verilmektedir.

[100] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[101] "Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors, WP 263 Rev.01," Article 29 Working Party, son güncelleme 16 Nisan, 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

Bağlayıcı şirket kuralları çerçevesinde kaç adet AB üye devletinde kısıtlı aktarımın gerçekleştirildiğine bağlı olarak bir veya iki denetleyici otorite, bağlayıcı şirket kurallarının gözden geçirilmesi ve onaylanmasında görev almaktadır. Bu otoriteler, ilgili bağlayıcı şirket kurallarına dahil olan diğer şirketlerin yer aldığı ülkenin denetleyici otoriteleri olacaklardır.

Kısıtlanmış aktarım gerçekleştirmek için yeterli güvenlik tedbirlerini sağlamak amacıyla bağlayıcı şirket kurallarının kullanılması kavramı, WP29 tarafından bir dizi çalışma belgelerinin oluşturulması ile geliştirilmiştir. Başvuru formları ve rehber de dahil olmak üzere tüm belgeler GDPR uyarınca gözden geçirilmiş ve güncellenmiştir.

Veri sorumlusu bağlayıcı şirket kuralları için WP29'un vurguladığı hususlar şunlardır[102]:

- Şikayette Bulunma Hakkı: İlgili kişilere, iddialarını yetkili bir veri koruma otoritesine veya AB üye devletlerinin yetkili mahkemesinin önüne getirme seçeneği verilmelidir;

- Şeffaflık: Tüm ilgili kişiler, hakları ve bu haklarını kullanma yolları konusunda yeterli bilgiye sahip olmalıdır;

- Uygulama Kapsamı: Bağlayıcı şirket kuralları, ortak bir ekonomik faaliyette bulunan teşebbüs grubunun veya şirketler grubunun ve üyelerinin her birinin yapısını ve iletişim bilgilerini belirtmelidir. Bağlayıcı şirket kuralları ayrıca, kişisel veri kategorileri, işleme türü ve amaçları, etkilenen veri sahibi türleri ve üçüncü ülkede ya da ülkelerdeki alıcıların kimlik bilgileri ya da ticari unvanları içeren maddi kapsamını da belirtmelidir.

- Veri Koruma İlkeleri: Bağlayıcı şirket kuralları şeffaflık, adil veri işleme, amaçla sınırlılık, veri kalitesi ve güvenlik ilkeleri ile, ayrıca GDPR'ın 47. maddesinin ikinci fıkrasının (d) bendinde belirtilen diğer ilkeleri de - örneğin, hukuka uygunluk ilkeleri, veri minimizasyonu, sınırlı saklama süreleri, özel nitelikli kişisel verilerin işlenmesine dair taahhütler, bağlayıcı şirket kurallarıyla bağlı olmayan kuruluşlara ileriye dönük aktarımlar ile ilgili şartlar- içermelidir.

- Hesap Verilebilirlik: Veri sorumlusu olarak hareket eden her kişi, bağlayıcı şirket kurallarına uyumlu hareket edildiğini göstermekle sorumludur ve uyumluluğu aktif olarak göstermelidir.

- Üçüncü Ülke Mevzuatı: Bağlayıcı şirket kuralları, bir şirketler grubu üyesinin bağlayıcı şirket kurallarının sağladığı garantiler üzerinde önemli bir olumsuz etkiye sahip olabilecek üçüncü ülke

[102] Article 29 Working Party- "Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors."

yasalarına tabi olması durumunda, bu durumun yetkili denetleyici otoriteye bildirileceğine dair taahhüde sahip olmalıdır (kişisel verilerin ifşa edilmesine ilişkin kolluk veya güvenlik güçlerinin yasal olarak bağlayıcı talepleri buna örnek verilebilecektir).

Veri işleyen bağlayıcı şirket kuraları için WP29'un vurguladığı hususlar *uygulama kapsamı* ve *şikâyette bulunma hakkı* bakımından yukarıda belirtilen şekildedir. Diğer hususlar ise şu şekilde yer almıştır:

- Üçüncü Taraf Lehtar Hakları: İlgili kişiler, bağlayıcı şirket kurallarını, söz konusu GDPR'a uygun gerekliliklerin özellikle veri işleyene yönelik olduğu durumlarda doğrudan veri işleyene karşı üçüncü taraf lehtarları olarak uygulattırabilmelidir.

- Veri Koruma İlkeleri: Bağlayıcı şirket kurallarında, şeffaflık, adil işleme, amaçla sınırlılık, veri kalitesi ve güvenlik ilkelerinden doğan yükümlülüklerinin yanı sıra ilgili kişilerin hakları, alt-işleme faaliyetleri ve bağlayıcı şirket kuralları ile bağlı olamayan kişilere yapılacak aktarım gibi diğer gereklilikler de açıklanmalıdır.

- Hesap Verilebilirlik: Veri işleyen, veri sorumlusunca ya da veri sorumlusunun görevlendirdiği kişilerce yapılan denetim ve incelemeler de dahil olmak üzere yükümlülüklerini yerine getirdiğini kanıtlamak için gerekli tüm bilgileri veri sorumlusuna iletme yükümlülüğü altındadır.

- Hizmet Sözleşmesi: Veri sorumlusu ve veri işleyen arasındaki hizmet sözleşmesi, GDPR'ın 28 inci maddesinde öngörülen tüm gerekli unsurları içermelidir.

3.1.1.2.3. Komisyon Tarafından Kabul Edilmiş Standart Veri Koruma Maddeleri (*Standard Contractual Clauses*)

Bu maddeler "standart sözleşme maddeleri" veya "model maddeler" olarak bilinmektedirler. Tüm bu hükümler, veri gönderen ve alanın sözleşmeden doğan yükümlülüklerini ve kişisel verileri aktarılan kişilerin haklarını içermektedir. İlgili kişiler bu haklarını, veri gönderen ve alandan doğrudan talep edebilmektedir.

Komisyon'un Direktif kapsamında kabul ettiği üç standart sözleşme bulunmaktadır. Veri sorumluları arasında gerçekleşen veri aktarımları için iki standart sözleşme[103], veri sorumlusu ile veri işleyen arasında gerçekleşen veri aktarımları için bir adet standart sözleşme[104] bulunmaktadır.

Komisyon, mevcut standart sözleşme maddelerini GDPR'a uygun bir şekilde geliştirmeyi planlamaktadır. Bu güncelleme gerçekleşene kadar ilgili taraflar, Direktif döneminde hazırlanmış olan bu standart sözleşmeleri kullanabilmektedirler. Komisyon, GDPR kapsamında yeni standart sözleşme maddelerini kabul etse dahi standart sözleşme maddelerini içeren mevcut sözleşmeler, kısıtlanmış veri aktarımları için kullanılmaya devam edilebilecek, geçersiz kılınmayacaktır.

Yeni bir sözleşmenin kurulması durumunda, standart sözleşme maddelerinin "bütünüyle ve değişiklik yapılmadan" kullanılması gerekmektedir. Standart sözleşmeye bağlı hükümlerle çelişmemek kaydıyla, iş ile ilgili konularda ek hükümler eklenebilmektedir. Ayrıca, standart sözleşme hükümlerine bağlı olmaları şartıyla başka taraflar da (ek veri gönderen ve alanlar) eklenebilmektedirler.

3.1.1.2.4. Bir Denetleyici Otorite Tarafından Kabul Edilen ve Komisyon Tarafından Onaylanan Standart Veri Koruma Maddeleri (*Standard Data Protection Clauses Adopted By a Supervisory Authority and Approved By The Commission*)

AB üyesi bir ülkenin veri koruma otoritesi tarafından kabul edilen standart veri koruma maddelerini içeren bir sözleşme yapılması durumunda, veri koruma otoritesinin bulunduğu ülkeden kısıtlanmış bir veri aktarımı gerçekleştirilebilir. Ancak belirtmek gerekir ki AB veri koruma otoriteleri henüz herhangi bir standart veri koruma maddesini kabul etmemişlerdir.

Bu kapsamda denetleyici otorite tarafından kabul edilen düzenlemelerin "Komisyon Tarafından Kabul Edilmiş Standart Veri Koruma Maddeleri (Standard Contractual Clauses)" başlığında belirtilen ve Komisyon tarafından kabul edilen hükümlere benzer olmaları muhtemeldir, ancak Komisyon tarafından kabul edilenlerden farklı olarak bu standart veri koruma maddeleri önce denetleyici otorite tarafından kabul edilip daha sonra Komisyon tarafından onaylanmaktadırlar.

3.1.1.2.5. Mesleki Davranış Kuralları (Code of Conduct)

GDPR, gereği gibi onaylanmış mesleki davranış kurallarının AEA dışına veri aktarılabilmesi için uygun güvenlik tedbirleri teşkil edebileceğini düzenlemiştir. Söz konusu mesleki davranış kuralları, ilgili iş sektörlerini temsil eden meslek birlikleri vb. organizasyonlar tarafından hazırlanan düzenleyici

[103] European Commission "Standard contractual clauses for the transfer of personal data to third countries."
[104] European Commission "Standard contractual clauses for the transfer of personal data to processors established in third countries."

enstrümanlardır. Bu kuralların GDPR kapsamında uygun güvenlik tedbirleri olarak kabul edilebilmeleri için GDPR'da öngörülen korumaya denk bir veri koruması sağlaması ve kurallara uymayı taahhüt eden şirketleri yasal olarak bağlayan bir mekanizmayı kurması aranmaktadır. Örneğin; AB'deki veri sorumlusu ile ABD'de bulunan veri işleyen arasındaki bir anlaşma ile onaylanmış meslek kurallarının uygulanacağı kararlaştırılabilecektir.[105]

GDPR'da ayrıca mesleki davranış kurallarının onaylanmış olması gerektiği de düzenlenmiştir. Buna göre aktarımın GDPR kapsamındaki yalnızca bir ülkeyi ilgilendirmesi halinde ilgili kişisel verilerin korunması otoritesi tarafından, birden çok ülkeyi ilgilendirmesi halinde ise EDPB tarafından mesleki davranış kurallarının uygun güvenlik tedbirleri sağladığına karar verilmesi gerekir.[106] Ancak henüz onaylanmış bir meslek davranış kuralları seti bulunmamaktadır.[107]

3.1.1.2.6. Sertifikasyon (Certifications)

GDPR'da düzenlenen uygun güvenlik tedbirlerinden bir diğeri de sertifikasyon yöntemidir. Buna göre AEA dışında bulunan bir şirket AEA verileri için yeterli korumayı sağladığını gösterir bir belge başvurusunda bulunabilmektedir.[108] Söz konusu işlemin uygun güvenlik tedbirleri kapsamında değerlendirilebilmesi (sertifikalandırılması) için başvurucunun belgedeki standartlara uyulacağına dair yasal olarak bağlayıcı bir taahhüttü ile bir arada olması gerekir.[109]

Sözü edilen belgeler, aktarımın yapılacağı ülkenin veri koruma otoritesi veya bu otorite tarafından yetkilendirilen "sertifikasyon kuruluşları" (*certification bodies*) tarafından hazırlanabilir. Ancak GDPR kapsamındaki birden çok ülkeyi ilgilendiren aktarımlar için sertifikasyon kuruluşları standartlarını belirleme yetkisi Avrupa Veri Koruma Kurulu tarafından kullanılacaktır.[110]

---

[105] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[106] Tess Blair et al., "Appropriate Safeguards in the GDPR- the Edata Guide to GDPR," son güncelleme 14 Şubat, 2019, https://www.morganlewis.com/pubs/appropriate-safeguards-in-the-gdpr.
[107] ICO- "International Transfers".
[108] ICO- "International Transfers".
[109] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[110] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."

Verilecek belgeler en çok üç yıl için geçerli olacak ve bu süre içerisinde şirketin taahhüdüne uygun hareket edip etmediği ilgili sertifikasyon kuruluşları tarafından takip edilecektir.[111] Bu çalışmanın hazırlandığı dönem itibariyle sertifikasyona ilişkin bir mekanizma henüz kurulmamıştır. [112]

3.1.1.2.7. Sözleşme Hükümleri (Contractual Clauses)

GDPR, veri aktaran ile veri aktarılan arasındaki sözleşmeye koyulacak hükümlerle de uygun güvenlik tedbirlerinin sağlanabileceğini düzenlemiştir. Söz konusu sözleşme hükümlerinin spesifik bir aktarıma ilişkin olması ve aktarımın yapılacağı AEA ülkesinin düzenleyici otoritesinin onayını içermesi gerekir. EDPB tarafından onayın hangi şartlar altında verileceğine dair bir rehber henüz yayınlanmamıştır ve bu doğrultuda hiçbir yerel veri koruma otoritesi bu kapsamda bir onay vermemiştir.[113]

3.1.1.2.8. İdari Düzenlemeler (Administrative Arrangements)

AEA dışına veri aktarımı iki kamu otoritesi arasında yapılacak idari düzenleme (mutabakat anlaşması gibi) ile de yapılabilir.[114] Bu kapsamda veri aktarımı yapılabilmesi için taraflardan en az birinin yasal olarak bağlayıcı anlaşma yapma salahiyetine sahip olmaması gerekir. Ayrıca söz konusu idari düzenleme, verisi aktarılacak kişilerin haklarının korunmasını sağlayacak uygun güvenlik tedbirleri içermeli, etkin ve icra edilebilir olmalıdır. Son olarak, idari düzenlemenin aktarımın yapılacağı AEA ülkesinin düzenleyici otoritesinin onayını içermesi gerekir. Aktarımın birden çok AEA ülkesinden yapılması halinde ayrıca EDPB'nin olumlu görüşü aranmaktadır.[115]

3.1.1.3. İstisnalar (Derogations)

3.1.1.3.1. Genel Açıklamalar

Özetlemek gerekirse yukarıdaki bölümde; GDPR kapsamında kişisel verilerin bir yeterlilik kararı veya uygun güvenlik tedbirleri olması halinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılabileceği ifade edilmiştir. Bununla birlikte, söz konusu veri aktarımı -belirli durumlarda kullanılabilecek- istisnalara da dayanabilmektedir.[116] Buna göre, AEA dışına veri aktarmak isteyen veri sorumlusu; aktarımın tekrarlı, çok geniş kapsamlı ve yapısal olmaması, ayrıca kullanılabilecek başka bir yasal yolun bulunmaması şartıyla GDPR'da düzenlenen istisnalardan birine dayanabilir.[117]

---

[111] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[112] ICO- "International Transfers".
[113] Tess Blair et al.- "Appropriate Safeguards in the GDPR."
[114] ICO- "International Transfers".
[115] Tess Blair et al.- "Appropriate Safeguards in the GDPR."
[116] European Commission- "Digital Single Market – Communication on Exchanging and Protecting Personal Data Q&A."
[117] EDPS- "International Transfers."

Sözü edilen istisnalar veri aktarımına ilişkin genel ilkeye istisna oluşturduğundan dar yorumlanmalı ve kural haline getirilmemelidir.[118] Veri sorumluları ilk olarak GDPR 45 ve 46. maddelerde yer alan mekanizmalardan birisiyle aktarımı gerçekleştirmek için çaba göstermeli, ancak bu imkanların yokluğunda 49. maddede belirtilen istisnaları kullanabilmektedir. Ayrıca 49. maddeyi uygularken, 44. madde uyarınca kişisel verilerin aktarılmasında GDPR'ın diğer hükümlerinde düzenlenen koşulların da yerine getirilmesi gerektiği unutulmamalıdır.[119] Son olarak, belirli kişisel veri kategorilerinin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarımının Avrupa Birliği veya AB üye devletleri hukukunda düzenlenen önemli kamu yararı sebepleri dolayısıyla sınırlandırılabileceği göz önünde bulundurulmalıdır.[120]

3.1.1.3.2. Açık Rıza (Explicit Consent)

GDPR'ın 49. maddesinin birinci fıkrasının (a) bendinde ilgili kişinin; bir yeterlilik kararı ve uygun güvenlik tedbirlerinin bulunmaması nedeniyle söz konusu aktarımın kendisine yönelik risklerinden haberdar edilmesinin ardından, önerilen aktarıma açık bir şekilde rıza gösterebileceği ve bu şekilde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir. Buradaki açık rızanın geçerli olarak kabul edilmesi için aranan genel şartlar GDPR'ın 4. maddesinin on birinci fıkrasında ve 7. maddesinde düzenlenmiştir. Buna ek olarak, WP29, açık rızada bulunması gereken genel şartlara ilişkin bir rehber[121] yayımlamıştır.[122] Buna göre, geçerli bir rıza hem belirli bir amaca özgü olmalı hem de veri sahibinin aktarıma ilişkin bilgilendirilmiş olmasına dayanmalıdır.[123] Rızanın belirli bir amaca özgü olması, veri sahibi tarafından aktarım üzerinde bir dereceye kadar kontrol sağlanmasına imkân tanımakta ve aktarımın içeriğine ilişkin şeffaflık sağlamaktadır. Rızanın belirli bir amaca özgü olması sebebiyle, bazı durumlarda gelecekteki bir aktarıma ilişkin (verilerin toplanması sırasında) rıza almanın mümkün olmayacağı açıktır. Bu gibi hallerde, veri sorumlusu, verilerin toplanmasından sonra gerçekleşse bile yapılacak aktarım için özel bir rıza alındığından emin olmalıdır.[124]

Veri sahibinin aktarıma ilişkin bilgilendirilmiş olması şartı ise GDPR'ın 4. maddesinin on birinci fıkrasında düzenlenen kişisel verilerin işlenmesi için rıza alınması gereken hallerde veri sahibinin bilgilendirilmesi gerektiği hükmüne dayanır. Bu genel bilgilendirme yükümlülüğünün yanı sıra 49. maddenin birinci fıkrasının (a) bendinde veri sahibinin, bir yeterlilik kararı ve uygun güvenlik

[118] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[119] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[120] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[121] Article 29 Working Party- "Guidelines on Consent under Regulation 2016/679, WP 259 Rev.01."
[122] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[123] ICO- "International Transfers".
[124] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".

tedbirlerinin bulunmaması nedeniyle söz konusu aktarımların kendisine yönelik risklerinden de haberdar edilmesi gerektiği düzenlenmiştir.[125] Söz konusu bilgilendirmenin yapılması veri konusunun gerekli açık rızayı verebilmesinin önemli bir şartı olduğundan yokluğunda bu istisna uygulama alanı bulamayacaktır.[126] Sonuç olarak, bir ilgili kişiye ilişkin kişisel veriler AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılırken veri sorumlusu aşağıdaki bilgilerin tamamını ilgili kişiye sağlamakla yükümlüdür:[127]

- Kişisel verilerin alıcıları veya alıcı kategorileri,
- Verilerin aktarılacağı ülke veya ülkeler,
- Aktarımın yapılmasını gerekli kılan sebepler,
- Aktarılacak veri türleri,
- Herhangi bir zamanda ilgili kişinin rızayı geri çekme hakkının varlığı,
- Kişisel veriler için yeterli koruma sağlamayan ve uygun başka güvenlik önlemlerinin alınmadığı bir ülkeye aktarım yapılmasının olası riskleri.

Yapılan açıklamalardan anlaşıldığı üzere GDPR, açık rızanın alınabilmesi için yüksek bir eşik belirlemiştir. Söz konusu yüksek eşik, ilgili kişi tarafından sağlanan rızanın herhangi bir zamanda geri çekilebilmesi imkanıyla birleştiğinde, açık rıza istisnasının üçüncü ülkelere yapılan aktarımlar için uygun bir uzun vadeli çözüm olamayacağı görülmektedir.[128]

3.1.1.3.3. Sözleşmenin İfası (Contract Performance)

GDPR'ın 49 uncu maddesinin birinci fıkrasının (b) bendinde aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin yürütülmesi veya ilgili kişinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması açısından gerekli olması hallerinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir. Giriş Hükmü 111 uyarınca, bu istisnaya dayanan veri aktarımları "söz konusu aktarım sözleşme için gerekli olduğunda ve sıklıkla gerçekleşmediğinde"

[125] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[126] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[127] ICO- "International Transfers".
[128] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."

devreye girebilecektir.[129] Gereklilik testi (*necessity test*), veri aktarımı ve sözleşmenin amaçları arasında yakın ve önemli bir bağlantı bulunmasını gerektirir. Veri aktarımının sıklıkla mı yoksa arada sırada mı gerçekleştiğine ise olay bazında karar verilecektir.[130]

49 uncu maddenin üçüncü fıkrasına göre, bu istisna, kamu yetkilerinin kullanımı kapsamında kamu kuruluşları tarafından gerçekleştirilen faaliyetlere uygulanmamaktadır.[131]

Bu istisnaya dayanılarak yapılan veri aktarımının klasik örneği; bir turizm şirketinin, AB vatandaşı müşterisinin verilerini rezervasyon yaptırmak amacıyla AEA dışındaki üçüncü bir ülkede bulunan otele aktarmasıdır. Bu noktada turizm şirketinin söz konusu otelle düzenli bir iş ilişkisi olmaması önem taşımaktadır. Bu istisna kapsamında ayrıca ilgili kişinin talebiyle alınan (sözleşme öncesi) tedbirlerin uygulanması amacıyla da veri aktarılabilmektedir. Bu kapsamda veri aktarılmasına örnek olarak ise Airbnb'nin rezervasyon yapılmasından önce AB vatandaşı müşteri verilerini AEA dışındaki üçüncü bir ülkede bulunan ev sahibine aktarması verilebilir.[132]

3.1.1.3.4. İlgili Kişi Yararına Üçüncü Taraf Sözleşmeleri (Third-Party Contracts in the Individual's Interest)

GDPR'ın 49 uncu maddesinin birinci fıkrasının (c) bendinde aktarımın, veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında ilgili kişi yararına yapılan bir sözleşmenin imzalanması veya yürütülmesi açısından gerekli olması hallerinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir. Giriş Hükmü 111 uyarınca, bu istisnaya dayanan veri aktarımlarında da söz konusu aktarımın sözleşme için gerekli olması ve sıklıkla gerçekleşmemesi şartları aranmaktadır.[133] Ayrıca bu istisna da kamu yetkilerinin kullanımı kapsamında kamu kuruluşları tarafından gerçekleştirilen faaliyetlere uygulanmaz.[134]

Sözleşme ilişkisi kurulmadan önce gerekli olan adımların atılması amacıyla yapılacak veri aktarımları için bu istisnaya dayanılması mümkün değildir. Bu özellik söz konusu istisnanın, (b) bendinde düzenlenen istisnadan en önemli farkını oluşturmaktadır.

[129] Recital 111 Metni'ne (http://www.privacy-regulation.eu/en/r111.htm) adresinden ulaşılabilir.
[130] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[131] ICO- "International Transfers".
[132] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[133] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[134] ICO- "International Transfers".

Yukarıda verilen örnekten devam edilirse; bir turizm şirketinin AB vatandaşı müşterisinin ailesine ilişkin verileri rezervasyon yaptırmak amacıyla AEA dışındaki üçüncü bir ülkede bulunan otele aktarması halinde bu istisna uygulama alanı bulur.[135]

3.1.1.3.5. Kamu Yararı (Public Interest)

GDPR'ın 49 uncu maddesinin birinci fıkrasının (d) bendinde aktarımın, kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması halinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir. Aynı maddenin 4 üncü fıkrasında atıfta bulunulan kamu yararının Birlik hukukunda veya aktarımı yapacak veri sorumlusunun tabi olduğu AB üye ülkesi hukukunda tanınan kamu yararı olduğu belirtilmiştir. Özellikle uluslararası iş birliğinde karşılıklılık kapsamında bu istisnaya dayanılması mümkündür.[136] Örneğin; belirli amaçları taşıyan ve uluslararası iş birliği sağlayan uluslararası bir anlaşma veya konvansiyon (AB'nin veya AB üye devletinin imzalamış olduğu) bu kapsamda değerlendirilebilir.[137]

Özel kuruluşlar tarafından da kullanılabilmekle birlikte, bu istisnadan esas olarak kamu makamlarınca yararlanılabileceği anlaşılmaktadır.[138]

3.1.1.3.6. Yasal Talepler (Legal Claims)

GDPR'ın 49 uncu maddesinin birinci fıkrasının (e) bendinde aktarımın, yasal taleplerde bulunulması, bu taleplerin uygulanması veya savunulması açısından gerekli olması halinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir. "Gereklilik testi", söz konusu veriler ile hukuki durumun belirli bir şekilde kurulması, kullanılması veya savunulması arasında yakın ve önemli bir bağlantının varlığını gerektirmektedir. Ayrıca bu istisna kapsamındaki veri aktarımlarının sıklıkla gerçekleşmemesi gerekir.[139]

Söz konusu yasal taleplerin hukuki bir dayanağı olması ve yasalarca düzenlenmiş resmi süreçleri ilgilendirmesi gerekmektedir. Ancak söz konusu süreçler adli veya idari yargı süreçleriyle sınırlı değildir. Bu kapsamda yasal talep kavramı geniş yorumlanmalıdır. Örneğin, söz konusu talepler aşağıda sayılan hususlara ilişkin olabilir:[140]

---

[135] ICO- "International Transfers".
[136] "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)," Article 29 Working Party, son güncelleme 22 Kasım, 2006, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.
[137] ICO- "International Transfers".
[138] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[139] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[140] ICO- "International Transfers".

- Özel hukuk ve ceza hukukuna ilişkin adli yargıdaki bütün yasal talepler. Bu kapsamda mahkeme işlemlerinin başlamış olmasına da gerek yoktur. Mahkeme dışı işlemler de (*out-of-court procedures*) istisna kapsamındadır.

- Finansal hizmetler düzenlemesi kapsamındaki bir soruşturmada savunma yapmak veya bir şirket birleşmesi için onay almak.

Son olarak veri sorumlularının, ulusal kanunların kişisel verilerin yabancı mahkemelere veya diğer yabancı organlara aktarımını yasaklayan veya sınırlandıran hükümler içerebileceğini göz önünde bulundurmaları gerekmektedir.[141]

3.1.1.3.7. Fiziksel veya Hukuki Engel (Physical or Legal Incapability)

GDPR'ın 49 uncu maddesinin birinci fıkrasının (f) bendinde aktarımın, ilgili kişi veya diğer kişilerin hayati menfaatlerinin korunması açısından gerekli olması ve ilgili kişinin fiziksel veya hukuki engeller sebebiyle rıza veremeyecek durumda olması halinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir. Söz konusu istisnanın özellikle tıbbi acil durumlarda uygulama alanı bulacağı açıktır. Örneğin, AEA dışındaki üçüncü bir ülkede acil bir tedaviye ihtiyaç duyan bilinci kapalı AB vatandaşının verilerinin AB üye devletindeki bir veri sorumlusundan aktarılması bu istisna kapsamında değerlendirilecektir. Bu gibi durumlarda ilgili kişinin karşı karşıya olduğu yakın ve ciddi zarar riskinin, onun kişisel verilerinin korunması kaygılarından daha ağır bastığı söylenebilir. Ancak ilgili kişinin geçerli bir karar verebilecek imkana sahip olduğu, bu kapsamda onun onayının alınmasının mümkün olduğu hallerde bu istisnanın uygulanamayacağı göz önünde bulundurulmalıdır. Örneğin, genel bir tıbbi muayene için bu istisnaya dayanılamayacaktır.[142]

İlgili kişinin fiziki ve ruhsal engeller yanında hukuki engeller sebebiyle de geçerli bir rıza veremeyecek durumda olması mümkündür. Acil bir tedaviye ihtiyaç duyan kişinin ergin olmayan çocuk olması hali bu duruma örnek olarak verilebilir.[143]

3.1.1.3.8. Avrupa Birliği Kamu Sicillerinden Yapılan Aktarımlar (Transfers from EU Public Registries)

GDPR'ın 49. maddesinin birinci fıkrasının (g) bendinde aktarımın, Avrupa Birliği veya AB üye ülkesi hukukuna göre kamuoyuna bilgi sağlanmasının amaçlandığı ve genel olarak kamuoyu veya meşru bir menfaati gösterebilen herhangi bir kişi tarafından erişime açık olan bir sicilden yapılması halinde AEA dışındaki üçüncü bir ülkeye veya uluslararası bir kuruluşa veri aktarılabileceği düzenlenmiştir.

[141] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[142] ICO- "International Transfers".
[143] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".

Bu kapsamda aktarımın, ancak Avrupa Birliği veya AB üye ülkesi hukuku çerçevesinde erişime yönelik olarak ortaya konan koşullar yerine getirildiği ölçüde yapılabileceği unutulmamalıdır.

Söz konusu siciller kamuya bilgi verme amaçlı olduğundan, özel kuruluşlara ait siciller bu istisnanın kapsamı dışındadır. Örneğin, ilgili kişinin kredibilitesini değerleyen özel sicillerden bu istisna kapsamında veri aktarımı yapılamaz.[144]

İstisna kapsamındaki siciller Avrupa Birliği veya AB üye ülkesi hukukuna göre kurulmuş ve:

- Genel olarak kamuoyuna; veya
- Meşru bir menfaati gösterebilen herhangi bir kişiye

açık olmalıdır. Şirket sicilleri, dernek sicilleri, adli sicil kayıtları, tapu sicil kayıtları vb. bu kapsamda değerlendirilebilecektir.

3.1.1.3.9. Veri Sorumlusunun Zorlayıcı Meşru Menfaatleri (Compelling Legitimate Interests of the Controller)

GDPR'ın 49. maddesinin ikinci fıkrası, daha önce Direktif'te yer almayan yeni bir istisna getirmiştir. Buna göre, bir dizi spesifik, açıkça sayılmış koşul altında, veri sorumlusunun zorlayıcı meşru menfaatlerinin de gerektirmesi halinde kişisel veriler AEA dışına aktarılabilmektedir. Bu istisna, GDPR 45 ve 46. maddeleri kapsamına girmeyen ve 49. maddede sayılan diğer istisnalara da sokulamayan veri aktarılmasını gerektiren durumlar için son çare olarak öngörülmüştür.[145] Açık rıza alınmasına ilişkin şartlara uyumun zorluğu ve diğer istisnaların dar kapsamı bu istisnayı veri sorumluları için çekici kılmaktadır.[146]

Sınır ötesi bir veri aktarımının bu istisna kapsamında değerlendirilebilmesi için şu şartlar aranmaktadır: [147]

- Bir yeterlilik kararı bulunmamalıdır.
- Uygun güvenlik tedbirlerine tabi olarak yapılan bir aktarım olmamalıdır.

[144] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[145] European Data Protection Board- "Guidelines 2/2018 on derogations of Article 49".
[146] Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US."
[147] ICO- "International Transfers".

- Diğer istisnalara dayanılarak bir aktarım yapılamamalıdır.

- Aktarım sürekli olmamalı, yinelenmemelidir. (Dolayısıyla bu istisna kapsamında aktarım birden fazla kez olabilmekle beraber devamlı/düzenli olmamalıdır.)

- Aktarım, yalnızca sınırlı sayıda ilgili kişiyi ilgilendirmelidir.

- Aktarım, veri sorumlusunun zorlayıcı meşru menfaatleri doğrultusunda gerekli olmalıdır. (Bir şirketin BT sistemlerini ani, ciddi bir zarardan korumak amacıyla veri aktarması örnek olarak verilebilir.)

- Veri sorumlusunun zorlayıcı meşru menfaatlerinin, ilgili kişinin menfaatleri, hakları ve özgürlükleri ile karşılaştırıldığında ağır basması gerekir.

- Veri sorumlusunun veri aktarımı ile ilgili tüm durumları değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olması gerekir. (Uygun güvenceler; gizlilik anlaşmaları, aktarımdan kısa bir süre sonra verinin silinmesinin gerekli kılınması veya verinin şifrelenerek aktarılması gibi güvenceler olabilir.)

- Veri sorumlusunun ilgili denetim makamını aktarım hususunda bilgilendirmesi gerekir.

- Veri sorumlusu, GDPR 13 ve 14. maddelerde atıfta bulunulan bilgilerin sağlanmasına ek olarak ilgili kişiyi aktarım ve gözetilen zorlayıcı meşru menfaatler hususunda bilgilendirmelidir.

3.1.2. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Konvansiyonu ve Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol)

Avrupa Konseyi tarafından 1970'li yıllardan itibaren gerçekleştirilen çalışmalar sonucunda 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan 108 Sayılı Konvansiyon, 1 Ekim 1985 tarihinde yürürlüğe girmiştir. 108 Sayılı Konvansiyon'u imzalayan ve onaylayan ülkelerin sayısı 55 olup tüm Avrupa Birliği üye devletleri 108 Sayılı Konvansiyon'a taraftır. 108 Sayılı Konvansiyon, kişisel verilerin işlenmesi ve ilgili kişilerin korunması alanında günümüzde uluslararası bağlayıcılığa sahip tek anlaşma olma özelliğini taşımaktadır. 108 Sayılı Konvansiyon'un Açıklayıcı Rapor'unda yurt dışına aktarıma ilişkin özetle şu ifadeler yer almaktadır; *Ulusal veri koruma yasalarının bireylerle ilgili veriler yurt dışına aktarıldığında ne ölçüde yeterli koruma sağladığı hususu akıllarda soru işareti yaratmaktadır.*

Bilgisayarlar, telekomünikasyon ile birlikte, veri işleme babında uluslararası ölçekte yeni olasılıklar yaratmakta, milletlerarası iletişimin kurulmasında karşılaşılan engellerden olan uzaklık, zaman, dil ve maliyet gibi engellerin aşılmasına yardımcı olmaktadırlar. Dağıtılmış işleme faaliyeti, veri sorumlularının bir bilgi sistemini veya veri tabanını birkaç ülkeye dağıtmalarına imkân vermektedir. Ağlar, kullanıcıların uzak ülkelerdeki bilgi sistemlerine erişmelerine veya bağlantı kurmalarına yardımcı olmaktadırlar. Birçok sektörde (örneğin bankacılık, seyahat, kredi kartları, vb.) bu tür aktarıcı veri işleme uygulamaları halihazırda yaygın olarak kullanılmaktadır. Prensip olarak, veri işleme operasyonlarının bir ülkede veya birkaç ülkede gerçekleşmesi veri sorumluları veya veri sahipleri için hiçbir fark yaratmamaktadır. Bununla birlikte, uygulamada, coğrafi alan genişletildikçe kişisel veriler daha az korunmaktadırlar. Ayrıca, veri sorumlularının operasyonlarını kısmen veya tamamen "veri cennetlerine", yani daha yumuşak veri koruma yasalarına sahip olan ya da bu alanda herhangi bir düzenlemeye sahip olmayan ülkelere taşıyarak veri koruma kontrollerinden kaçınmaya çalışabilecekleri yönünde endişeler ortaya çıkmıştır. Bu riskin bertaraf edilmesi için bazı ülkeler veri aktarımına dair izin alınması gibi özel kontrol mekanizmalarını ulusal yasalarına eklemişlerdir. Bununla birlikte, bu tür kontroller hem bireyler hem de uluslar için temel öneme sahip bir ilke olan verilerin uluslararası serbest dolaşımına müdahale edebilir. Dolayısıyla, uluslararası düzeyde veri korumanın bu ilkeye halel getirmediğinden emin olmak için bir formül bulunması gerekliliği ortaya çıkmıştır.

Veri aktarımı, 108 Sayılı Konvansiyon'un 12. Maddesinde düzenlenmiştir. İlgili madde uyarınca; taraf devletlerin münhasıran kişisel verinin korunması amacıyla taraf devletlere yapılan kişisel veri aktarımlarını yasaklayamayacağına ya da özel izne tabii tutamayacağına hükmedilmiştir. Bu hükme aşağıda yer alan istisnalar getirilmiştir:

- Tarafın iç mevzuatının belli kişisel veri kategorileri için bu verilerin doğasından kaynaklanan özel düzenlemeler içermesi, diğer tarafın düzenlemelerinin ise eşdeğer bir koruma içermemesi durumunda,

- Bu aktarımın bir taraf devletten, bir diğer taraf devlet üzerinden taraf olmayan bir devletin ülkesine yapılması durumunda, ilgili tarafın iç hukukunun boşluğundan yararlanmak üzere yapılması halinde bu tür aktarımları engellemek amacıyla.

Ek olarak, 108 Sayılı Konvansiyon'da, taraf olmayan bir devlete veri aktarımı yapılabilmesi için ilgili devletin yeterli koruma sağlaması gerektiği belirtilmiştir.

108 Sayılı Konvansiyon'un ayrılmaz parçası niteliğindeki ve 8 Kasım 2001'de imzaya açılmış olan 181 Sayılı Ek Protokol ise uluslararası veri aktarımı rejimine ek hükümler getirmektedir. Bu ek protokol

Türkiye tarafından 11 Temmuz 2016'da onaylanarak 1 Kasım 2016 tarihinde yürürlüğe girmiştir. 181 Sayılı Ek Protokol uyarınca; 108 Sayılı Konvansiyon'un tarafları, 108 Sayılı Konvansiyon'a taraf olmayan ve yeterli korumayı sağlamayan bir devletin / kuruluşun yetki alanına tabi olan bir alıcıya aktarım yapılmasına şu durumlarda izin verebilmektedirler:

c) İlgili kişinin belirli bir menfaati veya (özellikle önemli kamu menfaati olmak üzere) üstün gelen meşru menfaatler nedeniyle iç hukukun izin verdiği haller, ya da

d) İlgili veri aktarımından sorumlu olan veri sorumlusu tarafından sağlanan ve ilgili otorite tarafından iç hukukuna göre uygun bulunan koruma tedbirleri (ki bu koruma tedbirleri aktarıma konu olan sözleşme hükümlerinin bir sonucu olarak ortaya çıkabilir).

Dolayısıyla, 108 Sayılı Konvansiyon ve ek protokolü uyarınca (a) esasen taraf devletlere özel izin ya da yeterli korumanın bulunduğu ülkeler listesine ihtiyaç olmaksızın veri aktarımına izin verildiği, (b) taraf olmayan devletlere yapılan aktarımların izne tabii tutulabileceği ve haliyle (c) sadece 108 Sayılı Konvansiyon'a taraf olmayan devletlerin, veri koruma otoriteleri tarafından yayınlanan yeterli korumanın bulunduğu ülkeler listesine göre değerlendirilebileceği söylenebilecektir.

GDPR kapsamında uluslararası aktarımlara ilişkin 108 Sayılı Konvansiyon ile GDPR arasındaki somut bağlantı ise Giriş Hükmü 105 ile sağlanmıştır. Bu çerçevede AB üye devletleri dışındaki ülkeler arasından yeterli korumayı sağlayan ülkelere yönelik verilecek yeterlilik kararına ilişkin GDPR Giriş Hükmü 105'te, yeterlilik kararı verilirken dikkate alınan bir unsur olan (üçüncü taraf ülkelerin ve uluslararası organizasyonların) uluslararası taahhütlerin yanı sıra Avrupa Komisyonu'nun, üçüncü taraf ülkelerin ve uluslararası organizasyonların katıldığı çok taraflı veya bölgesel sistemlerden doğan yükümlülükleri de dikkate alması gerektiği ifade edilmiştir. Bu çerçevede GDPR özellikle üçüncü taraf ülkelerce 108 Sayılı Konvansiyon'a katılıma önem verilmesi gerektiğini belirtmektedir[148].

3.1.3. Modernize Edilmiş 108 Sayılı Konvansiyon (*Convention 108+*)

10 Ekim 2018 tarihinde imzaya açılan Konvansiyon 108+ , bu çalışmanın hazırlandığı tarih itibariyle 38 ülke tarafından imzalanmış ve 3 ülke tarafından onaylanmıştır. Belirtmek gerekir ki Avrupa Birliği (ve diğer uluslararası organizasyonlar) 108 Sayılı Konvansiyon'dan farklı olarak Konvansiyon 108+'e taraf olabileceklerdir.

Konvansiyon 108+, kişisel veriler konusunda daha iyi bir koruma düzeyi sağlamak amacıyla, taraf devletlerce uluslararası olarak uygulanacak güncellenmiş kurallar oluşturmak amacıyla

[148] Article 29 Working Party- "Working document on Adequacy Referential."

hazırlanmıştır. GDPR, Konvansiyon 108+ üzerinde önemli etkiye sahip olup bu etki "rıza" (GDPR benzeri nitelendirmeyle), profil oluşturma, yeni veri sahibi hakları, tasarıma göre gizlilik, gizlilik etki değerlendirmesi vb. gibi yeni kavramların sözleşmede yer almasıyla sonuçlanmıştır.

Konvansiyon 108+ de taraf devletlerin, münhasıran kişisel verinin korunması amacıyla taraf devletlerle yapılan kişisel veri aktarımlarını özel izne tabii tutamayacağına ve yasaklayamayacağına hükmetmiştir. Bu hükmün iki istisnası öngörülmüştür;

- Bir taraf devlet tarafından başka bir taraf devlete veya diğer bir taraf devlet üzerinden Konvansiyon 108+'e taraf olmayan bir devlete veri aktarımı yapılmasının, Konvansiyon 108+ hükümlerinin uygulanmamasına yol açacağı yönünde gerçek ve ciddi bir risk oluşturması,

- Bölgesel bir uluslararası organizasyonun taraf ülkelerince kabul edilen harmonize koruma kurallarına tabi olunması (Bu durumda ilgili veri koruma otoritesine bilgi verilmesi gerekmektedir.).

Sözleşmeye taraf olmayan devletlere yapılacak kişisel veri aktarımlarında eşdeğer koruma şartı Konvansiyon 108+'de de devam etmektedir. Bu tür bir koruma düzeyi, (i) uluslararası sözleşmeler dahil olmak üzere ilgili ülkenin iç hukukunca veya (ii) *ad hoc* (özel) uygulamalarla veya aktarım işlemine katılan kişiler tarafından kabul edilip uygulanan yasal olarak bağlayıcı ve uygulanabilir araçların sağladığı standart güvenlik tedbirleriyle güvence altına alınabilecektir. Sadece bahsedilen bu durumlarda veri koruma otoritelerinin bilgilendirilmesi aranmaktadır.

Yurt dışına veri aktarımına dair gerekliliklerin yerine getirilememesi durumunda dahi veri aktarımının gerçekleştirilebilmesi için taraf devletlerce aşağıdaki seçenekler sunulmuştur:

- İlgili kişinin, uygun güvencelerin yokluğunda söz konusu olabilecek risklere ilişkin bilgilendirildikten sonra verdiği açık, belirli ve özgür rızası

- Belirli durumlarda ilgili kişinin spesifik menfaatleri

- Önemli kamu menfaati gibi üstün gelen meşru menfaatler (Bu çerçevede kanunla öngörülme & demokratik bir toplumda gerekli ve orantılı olma şartları aranmaktadır.)

- Aktarımın, ifade özgürlüğü için demokratik bir toplumda gerekli ve orantılı olması

Bu seçeneklerin tercih edilmesi durumunda yine veri koruma otoritelerden izin alınmasına gerek bulunmamaktadır. Fakat belirli bir durumda ilgili kişinin spesifik menfaatinin veya üstün gelen meşru

menfaatlerin söz konusu olduğu hallerde talep edilmesi üzerine otoriteye bilgi verilmesi gerekebilecektir.

Konvansiyon 108+ uyarınca, veri koruma otoriteleri, kişisel veri aktarımı gerçekleştiren veri sorumlularından koruma tedbirlerinin etkinliğinin veya (söz konusu ise) üstün gelen meşru menfaatlerin ortaya konulmasını talep edebilecektir. Son olarak eklemek gerekir ki veri koruma otoriteleri, kişisel verilerin yurt dışında aktarımlarını ilgili kişilerin temel hak ve hürriyetlerini korumak amacıyla yasaklayabilir, askıya alabilir veya şarta bağlayabileceklerdir.

Konvansiyon 108+'ın Açıklayıcı Rapor'unda yurt dışına veri aktarımına ilişkin madde düzenlemesine dair açıklamalar şu şekildedir;

"*İşbu madde bilginin serbest akışının kolaylaştırılmasının kişisel verilerin yeterli düzeyde korunması şartıyla sağlanmasıdır. Uluslararası veri aktarımı, kişisel verilerin başka bir uluslararası organizasyonun veya devletin yetkisine tabi olan bir alıcıya erişilebilir kılındığı ya da açıklandığı hallerde gerçekleşmiş olmaktadır.*

Maddenin önem atfettiği nokta taraflardan birinin yetkisi dahilinde işlenen verilerin, Konvansiyon'un veri koruma ilkeleri tarafından her zaman korumasıdır. Ayrıca sağlanan koruma, veri sahiplerinin sahip oldukları insan haklarının globalleşmeden ve uluslararası veri aktarımından etkilenmemesini güvence altına alacak nitelikte olmalıdır.

Yalnızca kişisel verilerin korunması amacıyla veya özel izne tabi tutma yoluyla veri aktarımı kısıtlanamaz. Bununla birlikte, ulusal güvenlik, savunma, kamu güvenliği ve diğer kamu menfaatleri gibi başka amaçlarla veri aktarımının kısıtlanması Konvansiyon tarafından sınırlandırılmamaktadır.

İşbu maddede amaç Konvansiyon'da belirtilen veri koruma hükümlerinin kabul etmiş tarafların, verilerin özgür dolaşımına imkan tanıyan bir koruma düzeyi sunmasıdır. İşbu duruma istisna olarak getirilen hüküm dar yorumlanmalı ve taraflar, riskin farazi veya düşük olduğu hallerde bu hükme dayanamamalıdır. Bu nedenle, ilgili taraf işbu istisnayı ancak konvansiyon kapsamında verilere sağlanan korumaların önemli ölçüde olumsuz etkileyebileceği ve bu ihtimalin çok yüksek olduğu hususunda açık ve güvenilir bir delil olması durumunda ileri sürebilecektir. Ayrıca tarafların daha detaylı bir entegrasyon gözeten bölgesel ekonomik kuruluşlara dahil olan devletlerin paylaştığı uyumlaştırılmış veri koruma standartlarına tabi oldukları durumlar da uluslararası başka bir istisna olarak ortaya çıkmaktadır.

GDPR'da açıkça belirtildiği üzere, üçüncü bir ülkenin Konvansiyon 108'e ve onun uygulanmasına katılımı, AB'nin üçüncü ülkenin yeterli düzeyde korumayı sağlayıp sağlamadığı hususunu değerlendirmesinde önemli bir etmen olacaktır.

Bu madde kapsamında tarafların başta önemli kamu menfaatleri olmak üzere meşru menfaatlerini ileri sürerek uygun bir veri koruma düzeyi mevcut olmasa bile verileri aktarabileceklerine hükmedilmiştir. Her halükârda taraflar, Konvansiyon'a taraf olmayan ülke veya uluslararası organizasyonlara veri koruması amacıyla veya başka nedenlerle veri aktarımını sınırlandırmak hususunda Konvansiyon kapsamında özgürlerdir.

Uluslararası kişisel veri aktarımında, uygun bir koruma seviyesi garanti altına alınmalıdır. Alıcının Konvansiyon'a taraf olmadığı durumlarda uygun veri koruma seviyesin sağlanması amacıyla Konvansiyon kanuni güvenceler ile usulüne uygun olarak uygulanan geçici veya onaylanmış standartlaştırılmış güvenceler olmak üzere iki mekanizma kurar.

Kanuni güvenceler, işbu Konvansiyon'da belirtilen ilgili veri koruma unsurlarını içermeli, koruma seviyesi her aktarım veya aktarım kategorisi için değerlendirilmelidir.

Geçici veya onaylanmış standartlaştırılmış güvenceler de işbu Konvansiyon'da belirtilen ilgili veri koruma unsurlarını içermelidir. Ayrıca sözleşmesel hükümler, örneğin, ilgili kişiye, esasa ilişkin koruma standartlarına uyumu sağlamakla yükümlü olan ve veri aktarımından sorumlu olan bir irtibat kişi sağlanmasına imkan verir şekilde düzenlenebilir.

Koruma seviyesine dair değerlendirme yapılırken spesifik aktarımla ilgili olarak Konvansiyon ilkeleri ve ilgili kişinin düzenlemelere aykırılık durumunda menfaatlerini nasıl savunabildiği göz önünde bulundurulmalı ve bu durumların alıcı devlette veya organizasyonda ne ölçüde karşılandığına dikkat edilmelidir.

İlgili kişinin rızası veya özel çıkarları ile mevzuatın öngördüğü ve üstün gelen meşru menfaatin olması ve/veya aktarımın ifade özgürlüğü için demokratik bir toplumda gerekli ve orantılı bir önlem teşkil ettiği durumlarda taraflar uygun bir koruma seviyesi talep etme ilkesini uygulamayarak böyle bir koruma sağlamayan bir alıcıya veri aktarılmasına izin verebilmektedir. Bu istisnalar sınırlı sayıda olup gereklilik ve orantılılık ilkeleriyle uygun olmalıdır.

Gözetim otoritesi, alınan önlemlerin etkinliğini denetleme veya üstün gelen meşru menfaatlerin varlığının gösterilmesini talep etme ve ilgili kişilerin temel hak ve özgürlüklerini korumak için gerekli olması halinde aktarımı yasaklama, askıya alma veya koşullar oluşturma yetkileri ile donatılmalıdır."

Son olarak eklemek gerekir ki Konvansiyon 108+'ın yayınlanması ile birlikte hem Avrupa Birliği nezdinde devletlerin işbu sözleşmeye katılımı desteklenmiş, hem Birleşmiş Milletler yıllık raporunda tüm BM üye devletlerinin Konvansiyon 108+'ı onaylaması gerektiği belirtilmiştir[149].

3.2 Türk Mevzuatında Uluslararası Veri Aktarımı

3.2.1 Genel Mevzuat

Bilindiği üzere, kişisel verilerin yurt dışına aktarılması konusu mevzuatımızda KVKK'nın 9. maddesinde düzenlenmiş ve maddenin uygulamasına ilişkin olarak Kurul tarafından Kişisel Verilerin Yurtdışına Aktarılması Rehberi[150] yayınlanmıştır.

Buna göre kişisel verilerin yurt dışına aktarımı konusunda ilk şart, ilgili kişinin açık rızasının bulunmasıdır. İlgili kişinin açık rızası bulunması durumunda başka herhangi bir şart aranmadan söz konusu kişisel verilerin yurt dışına aktarılması mümkün olacaktır.

KVKK'nın 9.maddesinin ikinci fıkrası ise açık rıza aranmaksızın kişisel verilerin yurt dışına aktarılabileceği halleri düzenlemektedir. Açık rıza aranmaksızın yurt dışına kişisel verilerin aktarılabilmesi için;

- KVKK'nın 5. maddenin ikinci fıkrası (kişisel verilerin işlenme şartları) ile 6. maddenin üçüncü fıkrasında (özel nitelikli kişisel verilerin işlenme şartları) belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması, veya

- KVKK'nın 5. maddenin ikinci fıkrası ile 6.maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması gerekmektedir.

Dolayısıyla; açık rızanın bulunmadığı hallerde kişisel veriler açısından KVKK'nın 5. maddenin ikinci fıkrasında sayılan, özel nitelikli kişisel veriler açısından ise 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığının bulunup bulunmadığı öncelikle incelenecektir.

[149] "Right to privacy-Note by the Secretary-General," The Office of the High Commissioner for Human Rights, erişim 18 Şubat, 2020, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_73_45712.docx.
[150] Kişisel Verileri Koruma Kurumu- "Kişisel Verilerin Yurtdışına Aktarılması."

Buna göre, kişisel veriler için;

- Kanunlarda açıkça öngörülmesi

- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması

- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması

- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması

- İlgili kişinin kendisi tarafından alenileştirilmiş olması

- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması

- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Özel nitelikli kişisel veriler için;

- Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin kanunlarda öngörülen hâllerde aktarılması

- Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından aktarılması

şartlarından birinin sağlanması gerekmektedir. Bu şartlardan birinin sağlanmamış olması durumunda kişisel verilerin yurt dışına aktarılması mümkün olmayacaktır.

Öte yandan, yukarıda belirtilen şartlardan birinin sağlandığı hallerde dahi, verilerin yurt dışına aktarılması için aktarım yapılan ülkenin, Kurul tarafından yeterli korumanın bulunduğunun ilan edildiği

bir güvenli ülke olması gerekmektedir. Bu iki şartın sağlanması halinde açık rıza olmaksızın kişisel verilerin yurt dışına aktarımı gerçekleşebilecektir.

KVKK'nın 5. maddenin ikinci fıkrası ile 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin mevcut olması ancak veri aktarılacak ülkenin Kurul tarafından kabul edilen güvenli ülke listesinde bulunmaması halinde ise, KVKK, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri[151] ve Kurul'un izninin bulunması durumunda kişisel verilerin yurt dışına aktarımına olanak sağlamaktadır.

Yukarıda sayılan sürecin yanı sıra, ayrıca, KVKK'nın 9. maddesinin beşinci fıkrası, kişisel verilerin uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurul'un izniyle yurt dışına aktarılabileceğini düzenlemektedir. Söz konusu fıkra, bir yandan Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlara ilişkin olarak Kurul'un izni şartını getirerek ek bir yükümlülük getirmekte, öte yandan uluslararası sözleşmelere ilişkin olarak düzenleme sunmaktadır. Buna göre, uluslararası bir sözleşmenin mevcudiyeti halinde yukarıda anlatılan süreçten bağımsız olarak yurt dışına kişisel veri aktarımı, bu sözleşmenin hükümleri kapsamında gerçekleştirilebilecektir.

Son olarak, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklı tutulmuştur. Bir diğer ifade ile, yerel mevzuatta yurt dışına veri aktarılmasının öngörüldüğü hallerde, ilgili kişinin açık rızası ya da Kurul'un vereceği herhangi bir karar olmaksızın veri aktarımı gerçekleşebilecektir.

Bilindiği üzere, KVKK'nın 9. maddesinin dördüncü fıkrasında Kurul'un yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine dair karar verirken başvuracağı esaslar belirtilmekle birlikte, bu çalışmanın hazırlandığı tarihte henüz güvenli ülke listesi açıklanmamış ve herhangi bir münferit izin de verilmemiştir. Öte yandan Kurul tarafından yayınlanan Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü[152] isimli dokümanda, henüz Kurul tarafından güvenli ülkelere

[151] Kişisel Verileri Koruma Kurumu tarafından sağlanan ve yurtdışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurları içeren taahhütname örnekleri için: "6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi kapsamında, yurtdışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlar," Kişisel Verileri Koruma Kurumu, son güncelleme 16 Mayıs, 2018, https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler.

[152] "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü," Kişisel Verileri Koruma Kurumu, erişim 18 Şubat, 2020, https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu.

ilişkin belirleme yapılmadığından, gerçekleştirilecek aktarımlarda tüm ülkelerin yeterli korumanın bulunmadığı ülke statüsünde olduğu ifade edilmiştir.

3.2.2 Uluslararası Veri Aktarımını Düzenleyen Diğer Kanunlar

KVKK'nın 9. maddesinin son fıkrası, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğunu düzenlemiştir. Buna göre çeşitli kanunlarda ilgili kurum ve kuruluşlara yurt dışına veri aktarımı konusunda yetki verilmiştir. Söz konusu düzenlemelerim süreçleri KVKK'da öngörülen süreçten bağımsız olup, veri aktarımı konusunda yetkilendirilmiş kurum ve kuruluşların dışında ayrıca Kurul'un izni gerekmemektedir.

Aşağıda uluslararası veri aktarımını düzenleyen temel yerel kanunlar yer almaktadır.

3.2.2.1. Bankacılık Kanunu[153]

Bankacılık Kanunu'nun *Müşteri Sırrı* başlıklı 73. maddesinin son fıkrasında; kurumun gözetim ve denetimine tabi kuruluşların, bunların ortaklarına, bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıklarının faaliyetlerine veya müşterilerine ilişkin yabancı ülke kanunlarına göre denetime yetkili ve Kurum (Bankacılık Düzenleme ve Denetleme Kurumu; "**BDDK**") muadili mercilerin taleplerinin BDDK tarafından karşılanmasının sır saklama yükümlülüğü dışında değerlendirileceği düzenlenmiştir. Söz konusu madde BDDK'ya yabancı ülke kanunlarına göre denetime yetkili ve Kurum muadili mercilerin taleplerinin karşılanması çerçevesinde veri aktarımı hususunda yetki verdiğinden, yurt dışına BDDK tarafından kişisel veri aktarılabileceği sonucuna ulaşılabilmektedir.

Bununla beraber aynı maddenin sonuncu fıkrası aşağıdaki gibi olup, ilgili veri sorumluları nezdinde düzenleme kapsamındaki yurt dışına kişisel veri aktarımı için hukuki bir dayanak teşkil etmektedir;

"*Kurumun gözetim ve denetimine tabi kuruluşların, bunların ortaklarına, bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıklarının faaliyetlerine veya müşterilerine ilişkin yabancı ülke kanunlarına göre denetime yetkili ve Kurum muadili mercilerin taleplerinin Kurumca karşılanması, gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla bankaların ve finansal kuruluşların, kendi aralarında doğrudan doğruya ya da risk merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişinin yanı sıra doğrudan veya dolaylı pay sahipliği yoluyla sermayelerinin yüzde onunu ve daha fazlasını temsil eden paylarının satışı amacıyla muhtemel alıcıların yapacakları değerleme*

[153] Bankacılık Kanunu, *Resmi Gazete* 01.11.2005– 25983 (Mük), Erişim 21 Şubat, 2020, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf.

çalışmalarında ya da sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıkların konsolide finansal tablo hazırlama çalışmalarında, risk yönetimi ve iç denetim uygulamalarında veya kredileri de dâhil varlıklarının ya da bunlara dayalı menkul kıymetlerin satışı amacıyla yapılacak değerleme çalışmalarında ya da değerleme, derecelendirme veya destek hizmeti alınması ile bağımsız denetim faaliyetlerinde ve gerekli tedbirlerin alınması kaydıyla hizmet alımlarına yönelik işlemlerde kullanılmak üzere bilgi ve belge taleplerinin karşılanması sırasında banka ya da müşteri sırrı niteliğindeki bilgilerin öğrenilmesi sır saklama yükümlülüğü dışındadır."

3.2.2.2. Tebligat Kanunu[154]

Kişisel veri niteliğinde bilgileri de içerebilecek bilgi ve belgelerin yabancı ülkelere tebliğini[155] düzenleyen Tebligat Kanunu, bu belgelerin T.C. Dışişleri Bakanlığı aracılığıyla yabancı ülkedeki salahiyetli makama, buradan da ilgili yerlere tebliğ edilmesini düzenlemekte ve bu şekilde yurt dışına kişisel verilerin aktarımı konusunda yerel mevzuatta bir yükümlülük oluşturmaktadır. Bunun yanı sıra Tebligat Kanunu'nun ilgili maddeleri tebliğ olunacak kişinin yabancı ülkede bulunan Türk vatandaşı olması durumunda siyasi temsilciliklere[156], askeri şahıslara yapılacak tebligatta bağlı bulundukları Kara, Deniz, Hava Kuvvetleri Kumandanlıkları ile Jandarma Genel Komutanlığı'na[157] yurt dışına veri aktarımı konusunda yetki vermektedir.

3.2.2.3. Cezaî Konularda Uluslararası Adlî İş Birliği Kanunu[158]

Cezaî konularda uluslararası adlî iş birliğinin usul ve esaslarını düzenleyen Cezaî Konularda Uluslararası Adlî İş Birliği Kanunu, Türkiye'nin taraf olduğu adlî iş birliğine ilişkin milletlerarası antlaşmalar saklı kalmak üzere, Merkezi Makama[159] adlî iş birliği kapsamında ülkelerce talep edilen bilgi ve belgelerin kullanılmasına muvafakat vermek, bunların kullanılmasını sınırlandırmak, teminat veya şarta bağlamak görev ve yetkisini getirmektedir.

Yabancı ülkelerin adlî iş birliği taleplerinin reddedilmesi ancak (i) Türkiye'nin egemenlik hakları, millî güvenliği, kamu düzeni veya diğer temel çıkarlarının ihlal edilmesi, (ii) talebe konu fiilin sırf askerî suç, düşünce suçu, siyasî suç veya siyasî suçla bağlantılı bir suç olması, (iii) talebe konu kişinin ırkı, etnik kökeni, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasî görüşleri nedeniyle bir

---

[154] Tebligat Kanunu, *Resmi Gazete* 11.02.1959– 10139, Erişim 21 Şubat, 2020, https://www.mevzuat.gov.tr/MevzuatMetin/1.3.7201.pdf.
[155] Tebligat Kanunu Madde 25
[156] Tebligat Kanunu Madde 25/a
[157] Tebligat Kanunu Madde 27
[158] Cezai Konularda Uluslararası Adli İş Birliği Kanunu, *Resmi Gazete* 23.04.2016– 29703, erişim 21 Şubat, 2020, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6706.pdf.
[159] Türkiye açısından Merkezi Makam olarak Adalet Bakanlığı tayin edilmiştir.

soruşturma veya kovuşturmaya maruz bırakılacağına veya cezalandırılacağına ya da işkence veya kötü muameleye maruz kalacağına dair inandırıcı nedenlerin bulunması ve (iv) talepte bulunan ülkeye savunma hakkına ilişkin temel güvencelerin bulunmaması hallerinde mümkün kılınmıştır.

Kanun, adlî yardımlaşmaya ilişkin taleplerin yanı sıra iade, soruşturma veya kovuşturmanın devri, infazın devri, hükümlü nakli gibi konularda da uluslararası iş birliğini düzenlemekte ve bu şekilde Merkezi Makama bilgi paylaşımı yükümlülüğü getirerek, yurt dışına veri aktarımı konusunu düzenleyen ulusal mevzuattan biri olma niteliğini taşımaktadır.

3.2.2.4. Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun[160]

Suç gelirlerinin aklanmasının önlenmesine ilişkin usul ve esasları belirleyen Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un 22. maddesi, yabancı ülkelerdeki muadil kuruluşlara Malî Suçları Araştırma Kurulu Başkanlığınca bilgi verilmesinin, görevlilerin kişilerin ve bu kişilerle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına işlerine, işletmelerine, servetlerine ve mesleklerine ilişkin olarak öğrendikleri sırların ifşaı sayılmayacağını belirterek, kişisel verilerin yurt dışına aktarımına ilişkin olarak yasal dayanak oluşturmaktadır.

3.2.2.5. Türk Sivil Havacılık Kanunu[161]

Türk Sivil Havacılık Kanunu'nun *Milli Sivil Havacılık Güvenlik Kurulu ve havacılık güvenliği* başlıklı 40. maddesi; havayolu ile seyahat edecek kişilerin bilgilerinin kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla toplanabileceğini ve talep halinde yolcu bilgilerinin havayolu işletmeleri veya kurumlar tarafından üçüncü ülkelerle İçişleri Bakanlığının uygun görüşü ile paylaşılabileceğini düzenlemiştir. Bu şekilde, kişisel verilerin yurt dışına aktarılmasına ilişkin olarak yasal dayanak sağlanmış ve konuya ilişkin kararda etkili olan kamu kurumu olarak İçişleri Bakanlığı belirlenmiştir.

3.2.3 Uluslararası Veri Aktarımını Düzenleyen Uluslararası Sözleşmeler

Türkiye Cumhuriyeti Anayasası'nın 90. maddesinin son fıkrasına göre usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir ve temel hak ve özgürlüklere ilişkin

[160] Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun, *Resmi Gazete* 18.09.2006– 26323, erişim 21 Şubat, 2020, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5549.pdf.
[161] Türk Sivil Havacılık Kanunu. *Resmi Gazete* 14.09.1983- 18196. Erişim 21 Şubat, 2020. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2920.pdf.

milletlerarası antlaşmalar ile kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınacaktır.

Her ne kadar kişisel verilerin aktarılmasını öngören birçok uluslararası anlaşma (kara para aklama, terörizm, vb. konulara ilişkin) mevcut olsa da yurt dışına kişisel veri aktarımını düzenleyen temel uluslararası sözleşme, yukarıda da detaylı olarak açıklandığı üzere, 108 Sayılı Konvansiyon'dur. 108 sayılı Konvansiyon ve 181 sayılı Ek Protokol usulüne uygun olarak imzalanıp Türk mevzuatına aktarıldığından ve temel hak ve özgürlüklere ilişkin olduğundan, bu belgelerde yer alan yurt dışına veri aktarımına ilişkin hükümler öncelikli olarak uygulanacaktır. Benzer şekilde, bu husus, hukuki dayanak olarak ileri sürülebilecektir ve çıkacak uyuşmazlıklarda söz konusu hükümler esas olarak alınmalıdır.

Yukarıdaki açıklamalarımıza ek olarak belirtmek gerekir ki Türkiye, 108 Sayılı Konvansiyon'un taraflarına ilişkin olarak "… 108 Sayılı Konvansiyon'un onaylanmasının geçerliliği bulunmayan "*Kıbrıs Cumhuriyeti"nin anılan sözleşmeye taraf olan Güney Kıbrıs Rum Yönetimi tarafından temsil edildiği iddiasının herhangi bir biçimde kabulü anlamına gelmeyeceğini ve Türkiye'de sözde Kıbrıs Cumhuriyeti ile işbu Sözleşme kapsamında herhangi bir temasta bulunma yükümlülüğü getirmeyeceğini*" beyan etmiştir. Bu beyan haricinde Türkiye'nin herhangi bir çekincesi olmaması, Güney Kıbrıs Rum Yönetimi haricindeki her bir tarafa yönelik olarak uluslararası taahhütleri olduğunu göstermekte, dolayısıyla 108 Sayılı Konvansiyon'un uygulama alanını da netleştirmektedir.

Kanun hükmünde olan 108 Sayılı Konvansiyon'un III üncü bölümü "Sınır Ötesi Veri Akışları" başlığı altında serbest aktarım ilkelerini benimseyen ilgili madde uyarınca 108 Sayılı Konvansiyon'un taraf devletlerinin münhasıran özel yaşamın korunması amacıyla kişisel verilerin diğer bir Tarafa sınır ötesi akışının engellenmesi veya özel müsaadeye tabi tutulması yasaklanması ve sadece belirtilen iki durumda (özel düzenlemeye ilişkin karşı tarafça eşdeğer bir koruma sağlanmaması ve mevzuatın boşluğundan faydalanma hallerinde) sınırlama getirilebilmesi birtakım sonuçlar doğurmaktadır.

Bu kapsamda, 108 Sayılı Konvansiyon'un 12. maddesi uyarınca 108 sayılı Konvansiyon'un taraflarına gerçekleştirilecek kişisel veri aktarımlarının yukarıda yer alan (a) veya (b) bentlerinde sıralanan istisnalardan biri sağlanmadan yasaklanmaması veya özel izne tabi tutulmaması 108 Sayılı Konvansiyon'un getirdiği açık kurallardan bir tanesidir.

Türkiye tarafından gerçekleştirilmiş 108 Sayılı Konvansiyon'un öngördüğü ve yukarıda belirtilen iki istisnasına dayanılan herhangi bir sınırlandırma veya özel izne tabi tutulmaya ilişkin şu zamana kadar herhangi bir işlem bulunmamaktadır. Bu kapsamda, KVKK'nın 9. Maddesinin beşinci ve altıncı fıkraları da dikkate alındığında, 108 Sayılı Konvansiyon'un 12. maddesine dayanılarak 108 Sayılı

Konvansiyon'un Taraflarına veri aktarımı yapılmasına ilişkin herhangi bir hukuki sınırlandırma ve/veya engel bulunmamaktadır.

Diğer bir taraftan, 181 Sayılı Ek Protokol'ün 2. maddesinin birinci fıkrasında, sınır aşan kişisel veri aktarımlarına ilişkin olarak taraf olmayanlara yapılacak aktarımlarda *yeterli koruma sağlanıp sağlanmadığının* değerlendirmesinin yapılacağı düzenlenmiştir. Bu doğrultuda, ilgili maddenin mefhumu muhalifinden taraf olanlara yönelik yeterli koruma değerlendirilmesinin yapılamayacağı anlaşılmaktadır. Eklemek gerekir ki, 181 Sayılı Ek Protokol'ün 2. maddesinin ikinci fıkrasında ise, birinci fıkraya hangi koşullarda çekince getirilebileceği düzenlenmiştir. Buna karşın, ülkemiz ilgili düzenleme hakkında herhangi bir beyanda bulunmamıştır.

Tüm bu açıklamalar ışığında görülmektedir ki Türkiye'den 108 Sayılı Konvansiyon'un tarafı olan diğer 54 ülkeye yapılacak kişisel veri aktarımları için 108 Sayılı Konvansiyon'un (kanunlardan da önce uygulanması gereken) hükümleri hukuki dayanak teşkil edebilecektir. Yine belirtildiği üzere, bu uluslararası sözleşmenin insan haklarını ilgilendirmesi sebebiyle bu çerçevede bir mütekabiliyet şartı koşulması da mümkün olmayacaktır. Bu rejimde sağlanan koruma, Avrupa Konseyi'nin temel enstrümanlarından birine ve bununla bağlı olma iradesini gösteren 54 ülkenin uluslararası koruma yükümlülüğüne dayanmaktadır.

Aşağıda uluslararası veri aktarımını düzenleyen uluslararası sözleşmelerden temel olanları detaylandırılmıştır:

3.2.3.1. Vergi Konularında Karşılıklı İdari Yardımlaşma Sözleşmesi[162]

Avrupa Konseyi üye ülkeleri ile Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD) üye devletlerinin imzacı olduğu Vergi Konularında Karşılıklı İdari Yardımlaşma Sözleşmesi, söz konusu ülkeler arasında vergi konularında idari yardım sağlanmasını düzenlemektedir. Bilgi değişimi ve belgelerin tebliğ edilmesi hususlarını da düzenleyen sözleşme kapsamında taraflar, sözleşmeden etkilenen kişi ister taraflardan birinin isterse başka bir ülkenin mukimi veya vatandaşı olsun, öngörülen idari yardımı sağlamakla yükümlüdürler. Madde kapsamında vatandaş kavramı, gerçek kişilerin yanı sıra tüzel kişileri, ortaklıkları, kurumları ve statülerini taraf devletin yürürlükteki mevzuatına göre elde eden diğer

[162] İlgili sözleşme için: (Vergi Konularında Karşılıklı İdari Yardımlaşma Sözleşmesi, Son değişiklik 30 Ekim 2017, https://www.resmigazete.gov.tr/eskiler/2017/11/20171126-12.pdf.)
Taraf ülkeler listesi için: (Organization for Economic Co-operation and Development, Convention on Mutual Administrative Assistance in Tax Matters, son değişiklik 30 Ocak 2020, https://www.oecd.org/ctp/exchange-of-tax-information/convention-on-mutual-administrative-assistance-in-tax-matters.htm.)

kuruluşları da kapsamaktadır. Sözleşme kapsamında yetkili makamlar ise Maliye Bakanı[163] veya onun yetkili temsilcisi olarak belirlenmiştir.

Yardımlaşma şekilleri arasında sayılan bilgi değişimi, (i) talep üzerine bilgi değişimi, (ii) otomatik bilgi değişimi ve (iii) kendiliğinden bilgi değişimi olmak üzere üç ayrı şekilde düzenlenmiştir. Buna göre, talep üzerine değişimde, başvuran devletin talebi üzerine, talepte bulunulan devletin başvuran devlete bu sözleşmeni kapsamına giren vergilere ilişkin iç mevzuat hükümlerinin yürütülmesi veya uygulanması ile ilgili olduğu öngörülen her türlü bilgiyi sağlama yükümlülüğü bulunmaktadır. Otomatik bilgi değişiminde ise söz konusu her türlü bilginin iki veya daha fazla tarafın karşılıklı anlaşması ile otomatik olarak sağlanması sonucu doğmaktadır. Kendiliğinden bilgi değişimi ise sözleşmede belirtilen vergi kaybı, vergi istisnası elde etme, vergi tasarrufu sonucu doğurma, vergi yükümlülüğü doğurma hallerinde, bir tarafın diğer bir tarafa talep olmaksızın bu bilgileri sağlaması durumudur.

Öte yandan, sözleşmenin bilgi değişimini düzenleyen genel hükmü, talep üzerine ve kendiliğinden bilgi değişimi hallerinde, tarafların kendi mukimi veya vatandaşına ilişkin bilgileri iletmeden önce, yetkililerin, iç mevzuatları uyarınca bu kişileri durumdan haberdar edebilecekleri hususunda depozitörlerden birine beyanda bulunma imkanı tanımaktadır.

Sözleşmede ayrıca gerekli görüldüğü takdirde yardım talebinde (i) yetkili makam tarafından yapılan talebi başlatan makam ya da kurum, (ii) hakkında talepte bulunulan kişinin adı, adresi veya bu kişinin kinliğinin belirlenmesine yarayacak diğer hususlar, (iii) bilgi talep edilmesi durumunda, başvuran devletin, ihtiyaçlarının karşılanması için bilgiyi ne şekilde istediği belirtilecektir. Ayrıca, bu sözleşmedeki hiçbir hükmün, talepte bulunulan devletin mevzuatı veya idari uygulamaları ile kişilere sağlanmış olan hak ve güvenceleri etkilemeyeceği düzenlenmiş ancak bu sınırlamaların hiçbir surette talepte bulunulan devlete, sadece ulusal menfaati olmadığı gerekçesiyle bilgi sağlamayı reddetme hakkı verecek şekilde yorumlanamayacağı da ifade edilmiştir.

Son olarak, bir tarafın bu sözleşme kapsamında elde ettiği herhangi bir bilginin gizli tutulacağı ve bilgiyi sağlayan tarafın iç mevzuatında öngörülen koruma tedbirleri ile uyumlu olarak, kişisel bilgilerin korunmasında gerekli görülen düzeyde, bilgiyi alan tarafın kendi iç mevzuatı kapsamında elde ettiği bilgiler gibi korunacağı düzenlenmiştir. Ayrıca, bu bilgilerin, yalnızca vergilerin tahakkuku, tahsilatı ve cebri icra ya da kovuşturmasıyla veya bu hususlardaki itirazlara bakmakla görevli kişi veya makamlara, adli makamlar ile idari makamlar dahil, veya bunları denetlemekle görevli olan kişilere verilebileceği hükme bağlanmıştır.

[163] Güncel teşkilatlanmamıza göre yetkili makamın Hazine ve Maliye Bakanlığı olduğu söylenebilecektir.

3.2.3.2. Türkiye Cumhuriyeti Hükümeti ile Amerika Birleşik Devletleri Hükümeti Arasında Genişletilmiş Bilgi Değişimi Yoluyla Uluslararası Vergi Uyumunun Artırılması Anlaşması[164]

ABD vatandaşı ve/veya ABD vergi mükellefi olan gerçek ve tüzel kişilerin, ABD tarafından gelirleri ve varlıkları üzerinde bir vergilendirme işlemi yapılmaması amacıyla vergi kaçırma yoluna gitmelerini engelleme gayretiyle çıkarıyla ABD'nin Yabancı Hesapların Vergi Uyumu Yasası (*The Foreign Account Tax Compliance Act- FATCA*) kapsamında, OECD ve AB üye devletler ile G-20 ülkelerinin tamamına yakınının da bulunduğu, 100'den fazla ülke, ABD ile otomatik bilgi değişimi konusunda uluslararası anlaşma imzalamıştır.[165] Türkiye de Türkiye Cumhuriyeti Hükümeti[166] ile Amerika Birleşik Devletleri Hükümeti Arasında Genişletilmiş Bilgi Değişimi Yoluyla Uluslararası Vergi Uyumunun Artırılması Anlaşması'nı imzalayarak, Türk finansal kuruluşlarındaki ABD'li hesap sahiplerine ilişkin belirli bilgileri ABD'ye sağlama yükümlülüğü altına girmiştir.[167] Bu şekilde ABD'li hesap sahiplerine ilişkin kişisel veri niteliğindeki kimlik ve finansal bilgilerin yurt dışına aktarımı sözleşme gereği zorunluluk kazanmıştır.

3.2.3.3. 18 Mart 1970 Tarihli Hukukî ve Ticarî Konularda Yabancı Ülkelerde Delil Sağlanmasına Hakkında Sözleşme[168]

18 Mart 1970 Tarihli Hukukî ve Ticarî Konularda Yabancı Ülkelerde Delil Sağlanmasına Hakkında Sözleşme, istinabe taleplerinin iletilmesi ve yerine getirilmesi istemlerini kolaylaştırmak ve bu amaçta kullanılan faklı yöntemlerin uygunlaştırılmasını sağlamak ile hukuki ve ticari konularda karşılıklı adli iş birliğinin güçlendirilmesi amacıyla taraf devletler tarafından hazırlanmıştır. Bu sözleşmeye göre hukuki veya ticari konularda bir taraf devletin adli makamı, kendi devletinin kanun hükümleri gereğince istinabe yolu ile, diğer taraf devletin yetkili makamından delil sağlanmasını veya diğer adlî bir işlemin yerine getirilmesini talep edebilmektedir. Sözleşme delil teminine ilişkin olarak esas itibariyle iki farklı yol öngörmekte olup bunlardan ilki istinabe usulüdür ve taleplerin yürütülmesi amacıyla taraflar

---

[164] "Türkiye Cumhuriyeti Hükümeti ile Amerika Birleşik Devletleri Hükümeti Arasında Genişletilmiş Bilgi Değişimi Yoluyla Uluslararası Vergi Uyumunun Artırılması Anlaşması," Gelir İdaresi Başkanlığı, erişim 21 Şubat, 2020, https://www.gib.gov.tr/sites/default/files/fileadmin/haberler/FATCA/FATCA_Turkce.pdf.

[165] "FATCA Anlaşmasıyla İlgili Sıkça Sorulan Sorular," Gelir İdaresi Başkanlığı, erişim 12 Kasım, 2019, https://www.gib.gov.tr/uluslararasi_mevzuat/fatca-sorular.

[166] Türkiye açısından yetkili makam olarak Maliye Bakanı veya yetkili temsilcisi tayin edilmiştir. Güncel teşkilatlanmamıza göre yetkili makamın Hazine ve Maliye Bakanlığı olduğu söylenebilecektir.

[167] "Türkiye Cumhuriyeti Hükümeti ile Amerika Birleşik Devletleri Hükümeti Arasında Genişletilmiş Bilgi Değişimi Yoluyla Uluslararası Vergi Uyumunun Artırılması Anlaşması" Ankara'da İmzalandı," Gelir İdaresi Başkanlığı, erişim 12 Kasım, 2019, https://www.gib.gov.tr/node/102002.

[168] Hukuki veya Ticari Konularda Yabancı Ülkelerde Delil Sağlanması Hakkında Sözleşme, son güncelleme 15 Haziran 2004, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/lahey/turkce_lah20.pdf.
Taraf ülkeler listesine (https://www.hcch.net/en/instruments/conventions/status-table/?cid=82) adresinden ulaşılabilir.

devletler tarafından bir merkezi makam[169] tayin edilmiş olmasını öngörmektedir. Bu şekilde iletilecek olan istinabe talebinin içeriği sözleşmede belirtilmiş olup; davayla ilgili tarafların ve eğer mevcutsa temsilcilerinin isim ve adresleri, ifadelerine başvurulacak kişilerin isimleri ve adresleri, incelenmesi istenen belgeler veya kişisel ya da gayrimenkul diğer mal varlığı gibi kişisel veri niteliğinde bilgiler talepte yer almaktadır. Öte yandan ikinci usulde ise taraf devletin konsolosluk görevlisi veya diplomatik memuru ile özel memurlara bizzat delil toplamaya ilişkin hususlar düzenlenmiştir.

Bu noktada dikkat edilmelidir ki yurt dışından istinabe yoluyla delil talep edilmesi durumunda, bu talebin taraf devletin adli makamları tarafından talep edilmesi bir zorunluluktur. Sözleşme kapsamında bu talebin yerine getirilmesi zorunludur ve ancak sözleşmede belirtilen (i) uygulayıcı devlette, istinabenin yerine getirilmesi adli makamların yetkisine girmemesi ve (ii) istinabenin yerine getirileceği muhatap devlet, bunun egemenliğine veya güvenliğine zarar verebilecek nitelikte olduğu kanısını taşımaması hallerinde reddedilebilecektir. Ancak egemenliğe veya güvenliğe zarar verebilecek durumların sınırlı uygulanması gerektiği savunulmaktadır.[170]

3.2.3.4. 1965 Tarihli Hukuki veya Ticari Konularda Adli veya Gayriadli Belgelerin Yabancı Memleketlerde Tebliğine Dair Sözleşme[171]

Yabancı ülkelere tebliğ edilecek adli ve gayri adli belgelerin muhatabına vaktinde tebliğini sağlamak ve usulleri basitleştirerek ve hızlandırarak karşılıklı adlî yardımlaşmayı düzenlemek üzere imzalanan 1965 Tarihli Hukuki veya Ticari Konularda Adli veya Gayriadli Belgelerin Yabancı Memleketlerde Tebliğine Dair Sözleşme, ticarî veya hukukî, adlî veya adli olmayan belgeler gönderilmesi söz konusu olan bütün hallerde uygulanmaktadır. Söz konusu belgelerin kapsamı çok geniş tutulduğundan, içeriğinde kişisel veri niteliğinde bilgilerin de bulunduğu belgelerin tebliğ konusu olması yüksek olasılık olup, bu sözleşme, yurt dışına veri aktarımı noktasında yükümlülük getiren bir sözleşme olarak karşımıza çıkmaktadır. Zira, talep edilen devlet, bilgi ve belge tebliği taleplerinin merkezi makamlar[172]

[169] Türkiye açısından Merkezi Makam olarak Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü tayin edilmiştir.
[170] Cemal Şanlı, Emre Esen, ve İnci Ataman-Figanmeşe, *Milletlerarası Özel Hukuk* (İstanbul: Vedat Kitapçılık Basım Yayım Dağıtım Ltd. Şti., 2018), 474.
[171] İlgili sözleşme için: 172. Hukuki veya Ticari Konularda Adli ve Gayri Adli Belgelerin Yabancı Memleketlerde Tebliğine Dair Sözleşmenin Onaylanması Hakkında Bakanlar Kurulu Kararı, *Resmi Gazete* 17.06.1972- 14218. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/lahey/turkce_lah14.pdf.
Taraf ülkeler listesi için: Hague Conference on Private International Law. Status Table 14: Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, son güncelleme 22.11.2019, https://www.hcch.net/en/instruments/conventions/status-table/?cid=17.
[172] Türkiye açısından Merkezi Makam olarak Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü tayin edilmiştir.

aracılığıyla yürütüldüğü işbu Sözleşmeye uygun olarak yapılan bir tebliğ isteğinin yerine getirilmesini, ancak egemenlik veya güvenliği zedeleyici bulduğu takdirde reddedebilmektedir.

3.2.3.5. Cezai Konularda Adli İş Birliği Sözleşmeleri[173]

Cezai konularda adli iş birliği kapsamında uluslararası veri aktarımı düzenleyen birçok sözleşme bulunmaktadır. Bu sözleşmeler gereğince adli sicil, suçluların iadesi ve nakli, yargılama esnasında gerekli bilgi ve belgeler; sözleşmelerde belirtilen ve dar kapsamlı istisnalar dışında yetkili makamlarca yabancı yetkili makamlara aktarılacaktır. Yetkili makam olarak adli makamların veya Adalet Bakanlığı'nın tayin edildiği bu sözleşmelerde kimi durumlarda yardımlaşmanın Interpol aracılığıyla gerçekleştirilebileceği düzenlenmiştir.

Söz konusu sözleşmelerden Ceza İşlerinde Karşılıklı Adli Yardımlaşma Avrupa Sözleşmesi[174] ve Ek Protokolü[175], Suçluların İadesine Dair Avrupa Sözleşmesi[176] ve Ek Protokolü[177], Hükümlülerin Nakline Dair Avrupa Sözleşmesi[178], Ceza Yargılarının Milletlerarası Değeri Konusunda Avrupa Sözleşmesi[179] ve Ceza Kovuşturmalarının Aktarılmasına Dair Avrupa Sözleşmesi[180], münhasır olarak adli yardımlaşma sözleşmeleridir ve bu kapsamda genel anlamda kişilere ait ceza mahkumiyetine ilişkin bilgileri de içeren özel nitelikli bazı kişisel verilerin yurt dışına katarımı düzenlemektedirler. Öte

[173] Konuya ilişkin Türkiye'nin taraf olduğu sözleşme listesi için: "Cezai Konularda Adli İşbirliği Sözleşmeleri," Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, erişim 12 Kasım, 2019, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/munhasir_adli_yardimlasma.html.

[174] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 030-European Convention on Mutual Assistance in Criminal Matters," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030/signatures?p_auth=2XhBRoO6.

[175] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 099-Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/099/signatures?p_auth=2XhBRoO6.

[176] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 024-European Convention on Extradition," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024/signatures?p_auth=2XhBRoO6.

[177] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 098-Second Additional Protocol to the European Convention on Extradition," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/098/signatures?p_auth=2XhBRoO6.

[178] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 112-Convention on the Transfer of Sentenced Persons," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/112/signatures?p_auth=2XhBRoO6.

[179] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 070-European Convention on the International Validity of Criminal Judgments," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/070/signatures?p_auth=2XhBRoO6.

[180] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 073-European Convention on the Transfer of Proceedings in Criminal Matters," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/073/signatures?p_auth=2XhBRoO6.

yandan; terörizmin önlenmesi[181], uyuşturucu maddelerin kaçakçılığının önlenmesi[182], yolsuzlukla mücadele[183], hava ve deniz ulaşımında güvenliğin sağlanması[184], kara para aklamanın önlenmesi[185] gibi muhtelif konulara ilişkin uluslararası sözleşmelerde de uluslararası veri aktarımı düzenlenmiştir.

3.2.3.6. Gümrük Birliği Kararı[186]

Türkiye ile Avrupa Ekonomik Topluluğu arasında gümrük birliği tesis edilmesi amacıyla Gümrük Birliği'nin son döneminin uygulamaya konulmasına ilişkin koşulları belirleyen Gümrük Birliği Kararı'nın 7 numaralı "Gümrük Konularında İdari Merciler Arasında Yardımlaşma" isimli ekinde, taraflara, gümrük mevzuatına aykırı olan veya aykırı düşebilecek nitelik taşıyan işlemlerle ilgili bilgiler dahil olmak üzere bu mevzuatın gerektiği biçimde uygulanmasını sağlayabilecek her türlü bilgiyi talep üzerine ya da ihtiyari yardım kapsamında sağlama yükümlülüğü getirmektedir. Söz konusu bilgi taleplerinin reddedilmesi ancak (i) yardımın Türkiye veya Avrupa Ekonomik Topluluğu üyesi bir devletin egemenlik haklarını zedeleyebilecek olması, (ii) kamu güvenliği, kamu düzeni ve diğer temel çıkarları zedeleyebilecek olması, (iii) gümrük vergilerine ilişkin düzenlemelerin dışında kambiyo veya vergi düzenlemeleriyle ilgili olması veya (iv) sınai, ticari veya mesleki sırları ihlal etmesi durumlarında mümkün olmaktadır.

---

[181] Söz konusu sözleşmeler için:
Terörizmin Önlenmesine Dair Avrupa Sözleşmesi. 1977. TBMM İnsan Hakları İnceleme Komisyonu. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/ak/turkce/090_tur.pdf.
Council of Europe. Protocol Amending the European Convention on the Suppression of Terrorism. 2003. Council of Europe. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/ak/ingilizce/190_ing.pdf.
Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesi. 2005. Avrupa Konseyi. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/diger/196ETS.pdf.
Terörist Bombalamalarının Önlenmesine İlişkin Uluslararası Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanun. *Resmi Gazete* 11.01.2002 – 24637. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/diger/196ETS.pdf.
Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşmenin Onaylanmasının Uygun Bulunduğu Hakkında Kanun. *Resmi Gazete* 10.01.2002 – 24636. Erişim 21 Şubat 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/diger/11-%20TER%C3%96R%C4%B0ZM%C4%B0N%20F%C4%B0NANSMANININ%20%C3%96NLENMES%C4%B0NE%20DA%C4%B0R%20ULUSLARARASI.doc.

[182] Söz konusu sözleşmeler için:
Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesinin 17. Maddesinin Uygulanmasına İlişkin Deniz Yoluyla Yapılan Kaçakçılıkla Mücadele Anlaşması. 1988. Birleşmiş Milletler. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/ak/turkce/156_tur.pdf.
Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi. 1988. Birleşmiş Milletler. Erişim 21 Şubat, 2020. http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/diger/bm_uyusturucu_psikotrop.pdf.

[183] Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi. *Resmi Gazete* 2.10.2006- 26307, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/diger/13%20-%20bm-yolsuzlukla%20m%C3%BCcadele%20s%C3%B6zle%C5%9Fmesi.pdf.

[184] Sivil Havacılığın Güvenliğine Karşı Kanun Dışı Eylemlerin Önlenmesine İlişkin Sözleşme, son değişiklik 29 Kasım 1975, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/diger/bm_sivil_havacilik.pdf.

[185] Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve El Konulmasına İlişkin Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanun, *Resmi Gazete*, 22.06.2004- 25500, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/ak/turkce/141_tur.pdf.

[186] 1/95 Sayılı Ortaklık Konseyi Kararı (Gümrük Birliği Kararı), AT- Türkiye Ortaklık Konseyi, son güncelleme 22 Aralık, 1995, http://www.mfa.gov.tr/1-95-sayili-ortaklik-konseyi-karari-gumruk-birligi-karari.tr.mfa.

Öte yandan, kişisel bilgilerin ancak tarafların mevzuatındaki kişisel bilgilerin korunma düzeyinin aynı olması şartıyla iletilebileceği ve tarafların 108 sayılı Konvansiyon ilkelerine en azından denk düzeyde koruma sağlamakla yükümlü olduğu belirtilmiştir.

3.2.4 Avrupa Genel Veri Koruma Regülasyonu ile Karşılaştırma

Yukarıdaki bölümlerde yapılan açıklamalardan GDPR kapsamında AEA dışına yapılan aktarımlar ile KVKK kapsamında yurt dışına yapılan aktarımların birbirinden oldukça farklı formüle edildiği görülebilmektedir. İki rejim arasındaki bu farklılığın en önemli sebebinin, yasa koyucuların sınır ötesine yapılacak kişisel veri aktarımlarına karşı yaklaşımlarındaki tezatlık olduğu söylenebilecektir. Bu çerçevede GDPR, sınır ötesi veri aktarımına daha çok imkan tanıyarak verilerin aktarımını kolaylaştıracak çok alternatifli bir mekanizma kurmuştur. KVKK düzeninde ise kişisel verilerin ilgili kişinin açık rıza ile aktarılmadığı hallerde daha kontrollü ve otorite merkezli bir yapı karşımıza çıkmaktadır.

İki düzenlemenin sınır ötesi veri aktarımına ilişkin farklı yaklaşımlar aktarım rejiminin ilk aşamasında karşımıza çıkmaktadır. Buna göre, KVKK kapsamındaki yurt dışı veri aktarımlarında öncelikle veri sahibinin açık rızasının arandığı görülmektedir. Oysaki açık rıza, GDPR kapsamında sınır ötesi veri aktarımına ilişkin son çarelerden biri olarak düşünülmüş ve “istisnalar” başlığı altında düzenlenmiştir. GDPR’ın sınır ötesi veri aktarımlarında aradığı ilk unsur ise bir yeterlilik kararının varlığıdır. Avrupa Komisyonu vermiş olduğu yeterlilik kararları ile bir “beyaz liste” oluşturmuş ve bu beyaz listede AB ile denk bir koruma sağladığı belirlenmiş olan ülkelere yer vermiştir. Her ne kadar GDPR’ın yeterlilik kararı düzenlemesine benzer bir hüküm KVKK’da da yer almaktaysa da yeterli korumanın bulunduğu ülkelerin listesi henüz Kişisel Verileri Koruma Kurulu tarafından yayınlanmadığından ve dolayısıyla “hiçbir ülke güvenli koruma teşkil etmediği” için bu hükmün uygulaması bulunmamaktadır.

KVKK kapsamında yurt dışına veri aktarılmasına ilişkin mevcut olan son imkân ise Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul’un söz konusu aktarıma ilişkin izninin bulunması halidir. Yukarıda “Güvenlik Tedbirlerinin Varlığı” başlığı altında açıklandığı üzere GDPR’da da benzer iki imkânın düzenlendiği söylenebilecektir. Bu imkanlardan ilki “standart sözleşme maddeleri” olarak bilinmektedir. Bu yöntem, Komisyon tarafından önceden kabul edilmiş standart sözleşme maddelerinin bütünüyle ve değişiklik yapılmadan kullanılması halinde sınır ötesi veri aktarımının mümkün olduğu bir veri aktarım yöntemidir. Bir veri koruma otoritesinin izninin alınmasına gerek olmaması bu yöntemi KVKK’da düzenlenen ilgili yöntemden ayırmaktadır. GDPR kapsamında sözü edilen ikinci imkân ise veri aktaran ile veri aktarılan arasındaki sözleşmeye koyulacak hükümlerle uygun güvenlik tedbirlerinin sağlandığı yöntemdir. Söz konusu sözleşme hükümlerinin aktarımın yapılacağı AEA ülkesinin düzenleyici otoritesinin onayını içermesi gerekmektedir. Ancak tekrar eklemek gerekir ki Avrupa Veri Koruma Kurulu tarafından

onayın hangi şartlar altında verileceğine dair bir rehber henüz yayınlanmadığından hiçbir yerel veri koruma otoritesi bu kapsamda bir onay vermemiştir. Bu GDPR düzenlemesi ile KVKK'daki ilgili düzenleme arasındaki en önemli fark ise söz konusu imkanların rolü açısındandır. KVKK kapsamında sınır ötesi veri aktarımına ilişkin karşılıklı taahhüt ve Kurul'un onayının alınması (uygulamadaki şartlar nedeniyle[187]) esas yöntem iken, GDPR kapsamında diğer birçok alternatif veri sorumluları ve veri işleyenler için uygulanabilir enstrümanlardır.

GDPR'da sayılan bu imkanlar dışında altı farklı "uygun güvence" enstrümanı bulunmaktadır. Görülmektedir ki birbirinden oldukça farklı alanları kapsayan bu imkanlar sayesinde GDPR, sınır ötesi veri aktarımını için alternatif yollar belirlemiş, her bir seçenek için kişisel verilerin aktarıldığı yerde korunmasını temin etmiştir. Söz konusu imkanlar yukarıda "Güvenlik Tedbirlerinin Varlığı" başlığı altında detaylıca açıklandığından burada ayrıca incelenmeyecektir.

GDPR kapsamında sınır ötesi veri aktarılmasına ilişkin son basamakta ise "istisnalar" yer almaktadır. Yukarıda da belirtildiği üzere açık rıza, Avrupa Birliği hukukunda veri aktarımları için istisnalar kapsamında düzenlenmektedir ve bu çerçevede alınacak açık rıza için oldukça katı gereklilikler öngörülmüş, aksi takdirde aktarım için hukuki dayanak teşkil edemeyeceği düzenlenmiştir. KVKK ile karşılaştırıldığında, KVKK'nın 9. maddesi kapsamında aktarıma temel edecek bir açık rıza kabul edilebilirken aynı rıza GDPR'ın uluslararası aktarımlar için geçerli dayanak olarak değerlendireceği rıza kriterlerini sağlamayabilecektir. Dolayısıyla açık rıza uyarınca aktarımlarda -bu anlamda- daha katı bir tutum sergilendiği söylenebilecektir.

İstisnalar özelinde vurgulanması gereken bir nokta da bazı istisnaların KVKK 5. maddenin ikinci fıkrasında düzenlenen veri işleme şartlarıyla olan benzerliğidir. Buradaki temel farklılık; GDPR'da düzenlenen istisnaların sınır ötesi veri aktarılmasına tek başına dayanak olabilmesidir. KVKK 5 inci maddenin ikinci fıkrasında düzenlenen veri işleme şartlarının ise böyle bir aktarıma tek başına dayanak teşkil edemeyeceği, aktarımın ayrıca yeterli korumanın bulunduğu ülkelere yapılması veya karşılıklı taahhüt ve Kurul'un onayının alınması gerektiği düzenlenmektedir.

[187] Burada kastedilen, devamlı bir şekilde yurt dışına kişisel veri aktarımı gerçekleştirmenin ticari işin gereği olan hallerde her daim açık rıza ile hareket edilmesinin sürdürülebilir olmaması ve KVKK'dan düzenlenmiş olmakla beraber mevcut bir güvenli ülke listesinin yayınlanmamış olmasıdır.

5. Güncel Gelişmeler

4.1. 108 Sayılı Konvansiyon'un Modernizasyon Süreci

2013 ile 2016 yılları arasında 108 Sayılı Konvansiyon Komitesi tarafından 108 Sayılı Konvansiyon'un modernize edilmesine ilişkin sunulan teklifler, devletlerarası bir komite tarafından incelenmiştir ve bu çalışmalar sonucunda Avrupa Konseyi Bakanlar Komitesi'ne tadil protokolü taslağı sunulmuştur[188]. Taslak ile 108 Sayılı Konvansiyon ilkesel seviyede korunmakla beraber detaylandırılmış ve özellikle AB yasal düzenlemelerine uyumluluk hedeflenmiştir. Avrupa Konseyi Bakanlar Komitesi'nin 128 inci toplantısında alınan kararla 18 Mayıs 2018'de Konvansiyon 108+ yayınlanmıştır. 10 Ekim 2018'de imzaya açılan Konvansiyon 108+; (bu çalışmanın hazırlandığı tarih itibariyle) 38 ülke tarafından imzalanmış olup bu ülkelerden üç tanesi tarafından onaylanmıştır[189].

Ülkeler[190]	108 Sayılı Konvansiyon [191]	Konvansiyon 108+
Avrupa Konseyi Üye Devletleri		
Almanya	19/06/1985	
Andora	06/05/2008	
Arnavutluk	14/02/2005	X
Avusturya	30/03/1988	
Azerbaycan	03/05/2010	X
Belçika	28/05/1993	
Birleşik Krallık	26/08/1987	
Bosna Hersek	31/03/2006	X
Bulgaristan	18/09/2002	10/12/2019
Çekya	09/07/2001	
Danimarka	23/10/1989	X
Ermenistan	09/05/2012	
Estonya	14/11/2001	
Finlandiya	02/12/1991	
Fransa	24/03/1983	

[188] Taraf ülkeler listesi: "Modernisation of the Data Protection "Convention 108," Council of Europe, erişim 12 Kasım, 2019, https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.
[189] Council of Europe- "Chart of signatures and ratifications of Treaty 223-Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data."
[190] **Koyu** olarak yazılmış olanlar Avrupa Birliği üye devletleridir.
[191] Taraf ülkeler listesi: "Chart of signatures and ratifications of Treaty 108-Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," Council of Europe, erişim 18 Şubat, 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

Güney Kıbrıs Rum Yönetimi	21/02/2002	
Gürcistan	14/12/2005	X
Hırvatistan	21/06/2005	18/12/2019
Hollanda	24/08/1993	
İrlanda	25/04/1990	
İzlanda	25/03/1991	
İspanya	31/01/1984	
İsveç	29/09/1982	
İsviçre	02/10/1997	
İtalya	29/03/1997	
Karadağ	06/09/2005	X
Kuzey Makedonya	24/03/2006	
Letonya	30/05/2001	
Lihtenştayn	11/05/2004	X
Litvanya	01/06/2001	23/01/2020
Lüksemburg	10/02/1988	
Macaristan	08/10/1997	
Malta	28/02/2003	X
Moldova Cumhuriyeti	28/02/2008	X
Monaco	24/12/2008	
Norveç	20/02/1984	
Polonya	23/05/2002	
Portekiz	02/09/1993	
Romanya	27/02/2002	X
Rusya Federasyonu	15/05/2013	
San Marino	28/05/2015	
Sırbistan	06/09/2005	
Slovakya	13/09/2000	
Slovenya	27/05/1994	
Türkiye	02/05/2016	X
Ukrayna	30/09/2010	X
Yunanistan	11/08/1995	
Avrupa Konseyi Üyesi Olmayan Devletler		
Arjantin	25/02/2019	
Burkina Faso	X	X

Fas	28/05/2019	X
Meksika	28/06/2018	X
Morityus	17/06/2016	X
Senegal	25/08/2016	X
Tunus	18/07/2017	
Uruguay	10/04/2013	
Yeşil Burun Adaları	19/06/2018	X
Toplam:	**55 Taraf Devlet**	**38 İmzacı**

Avrupa Birliği'nin de Konvansiyon 108+'a taraf olabileceği 26. maddede belirtilmiştir. Yukarıda da belirtildiği üzere, uluslararası kuruluşların da artık Konvansiyon 108+'a katılması mümkündür. Konvansiyon 108+'a herhangi bir ülkenin katılımı mümkündür ve bu şekilde tek bir küresel standardın getirilmiş olacağı söylenebilecektir[192].

Konvansiyon 108+ ile esnek ve çok taraflı bir yasal düzenleme getirilmiş, bu şekilde bir yandan kişisel verilerin korunmasına ilişkin gerekli güvenlik tedbirleri getirerek diğer yandan kişisel verilerin sınır ötesi aktarılmaları kolaylaştırılmıştır. Bunlara ek olarak kişisel verilerin işlenmesine ilişkin olarak bireylerin korunması ile, başta gizlilik hakkı olmak üzere, insan haklarına ve özgürlüklerine katkıda bulunulacağı belirtilmiştir[193]. Aşağıda yer verilen ilkeler ve düzenlemeler kişisel verilerin hem otomatik hem otomatik olmayan yollarla işlendiği hallere uygulanacaktır ve 108 Sayılı Konvansiyon'da kullanılan terimler de daha kapsayıcı şekilde revize edilmiştir. Örneğin Konvansiyon 108+ kapsamına genetik ve biyometrik veriler ile etnik kökene ve sendika üyeliğine ilişkin kişisel veriler de -özel veri kategorileri olarak- eklenmiştir. Dolayısıyla Konvansiyon 108+ hem özel sektör hem kamu sektöründe gerçekleştirilen (otomatik yollarla olsun veya olmasın) veri işleme faaliyetlerinin tümüne[194] uygulanır hale gelmiştir.

İçerik olarak değerlendirildiğinde 108 Sayılı Konvansiyon, modernize edilerek GDPR ile benzer/paralel bir düzeye getirilmiştir. Konvansiyon 108+'de yer alan tanımlar, ilkeler, gizliliğe ilişkin konseptler ve ilgili kişi hakları gibi düzenlemeler GDPR'a benzerlik göstermektedir. Bununla beraber 108 Sayılı Konvansiyon'un kapsamının (hem veri işleme türü hem işlenen veri türleri açısından)

[192] "Enhancing data protection globally: Council of Europe updates its landmark convention," Council of Europe, erişim 12 Kasım, 2019, https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976.

[193] Amaç maddesinin (bkz. Konvansiyon 108+ madde 1) lafzının değiştirilmesi ile sayılan haklara vurgu yapılmasının amaçlandığı Avrupa Konseyi tarafından açıkça belirtilmektedir; "The modernised Convention 108: novelties in a nutshell," Council of Europe, erişim 12 Kasım, 2019, https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

[194] Ancak belirtmek gerekir ki 108+ Konvansiyon, tamamen kişisel veya ev halkına ilişkin faaliyetler kapsamında bireyler tarafından gerçekleştirilen kişisel veri işlemelerine uygulanmamaktadır.

genişletilmesi de GDPR ile Konvansiyon 108+'in beraber uygulama bulacağı alanları artırmıştır. Dolayısıyla internet ve iletişim teknolojilerinden kaynaklanan veri koruma ve gizlilik problemlerinin önüne geçmeye çalışan bu iki metin birbirleri ile uyumlu hale getirilmiştir. Aşağıdaki tabloda yurt dışına veri aktarımına ilişkin GDPR ile Konvansiyon 108+ arasındaki paralellik takip edilebilecektir.

Avrupa Birliği	Ele Alınan Konular	Avrupa Konseyi
Kişisel veri aktarımları		
GDPR, Madde 44	Konsept	Konvansiyon 108+, Madde 14 (1) ve (2)
Kişisel verilerin serbest dolaşım		
GDPR, Madde 1 (3) ve Giriş Hükmü 170	AB Üye Devletleri Arasında	
	108 Sayılı Konvansiyon'a taraf olan taraflar arasında	Konvansiyon 108+, Madde 14 (1)
Üçüncü ülkelere ya da uluslararası organizasyonlara kişisel veri aktarımları		
GDPR, Madde 45 C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 2015	Uygunluk kararı/yeterli düzeyde korumaya sahip üçüncü ülkeler ve uluslararası organizasyonlar	Konvansiyon 108+, Madde 14 (2)
GDPR, Madde 46 (1) ve 46 (2)	Standart sözleşme hükümleri, bağlayıcı şirket kuralları, davranış kuralları ve sertifikasyon mekanizmaları yoluyla sağlanan, ilgili kişiler için uygulanabilen haklar ve hukuki çareler dahil olmak üzere uygun korumalar	Konvansiyon 108+, Madde 14 (2), (3), (5) ve (6)
GDPR, Madde 46 (3)	Yetkin denetleyici otorite tarafından yetkilendirmeye tabi olan: kamu otoriteleri	

	arasındaki idari düzenlemelerin içerdiği sözleşmesel şartlar ve hükümler	
GDPR, Madde 46 (5)	Direktif 95/46 temelinde mevcut olan yetkilendirmeler	
GDPR, Madde 47	Bağlayıcı şirket kuralları	
GDPR, Madde 49	Özel durumlar için istisnalar	Konvansiyon 108+, Madde 14 (4)
Örnekler: AB–ABD PNR Anlaşması AB–ABD SWIFT Anlaşması	Uluslararası anlaşmalar	Konvansiyon 108+, Madde 14 (3) (a)

Bibliyografya

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

2. Kişisel Verileri Koruma Kurumu. "Açık Rızanın Hizmet Şartına Bağlanması." Erişim 15 Şubat, 2020. https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi.

3. Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi." Erişim 15 Şubat, 2020. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf.

4. ICO. "International Transfers- Exception 1. Has the individual given his or her explicit consent to the restricted transfer?." Erişim 3 Şubat 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

5. European Data Protection Board – EDPB. "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679." Son güncelleme 25 Mayıs,2018. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

6. Kişisel Verileri Koruma Kurumu. "Yurtdışına Aktarım." Erişim 12 Ocak, 2020. https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim.

7. Article 29 Working Party. "Working document on Adequacy Referential, WP 254 Rev.01." Son güncelleme 2 Şubat, 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

8. Kişisel Verileri Koruma Kurumu. "Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler." Erişim 12 Ocak, 2020. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/60d987a1-ba9d-4285-a8ce-c3f41ff4e47f.pdf.

9. European Commission. Communication from the Commission to the European Parliament and the Council-Exchanging and Protecting Personal Data in a Globalised World. Brussels. 2017.

10. European Data Protection Supervisor. "International Transfers." Erişim 14 Ocak, 2020. https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en.

11. Theodorakis, Nikolaos I.."Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US." *Stanford-Vienna TTLF Working Papers*, no. 39. https://www-cdn.law.stanford.edu/wp-content/uploads/2018/09/theodorakis_wp39.pdf.

12. ICO. "How do we apply legitimate interests in practice?" Erişim 15 Şubat, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/.

13. European Commission. "Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers." Son güncelleme 10 Ocak, 2017. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15.

14. European Commission. "List of companies for which the EU BCR cooperation procedure is closed." Erişim 15 Şubat, 2020. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841.

15. European Data Protection Board. "Article 29 Working Party." Erişim 17 Şubat, 2020. https://edpb.europa.eu/our-work-tools/article-29-working-party_en.

16. Article 29 Working Party. "Guidelines on Consent under Regulation 2016/679, WP 259 Rev.01." Son güncelleme 7 Haziran, 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

17. Kişisel Verileri Koruma Kurumu. "Açık Rıza." Erişim 17 Şubat, 2020. https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf.

18. Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC. 2001. *Official Journal of the European Communities* L 181/19. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en.

Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries. 2004. *Official Journal of the European Union* L 385/74. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN.

19. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. 2010. Official Journal of the European Union L 39/5. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en.

20. Kişisel Verileri Koruma Kurumu. "Taahhütnameler." Son güncelleme 16 Mayıs, 2018. https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler.

21. European Commission. "Types of EU law." Erişim 17 Şubat, 2020. https://ec.europa.eu/info/law/law-making-process/types-eu-law_en.

22. European Commission. "GDPR Implementation- Updated State of play in the Member States (11/04/2019)." Erişim 17 Şubat, 2020. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306.

23. European Union. "Precedence of European law." Erişim 18 Şubat, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14548.

24. The International Trade Administration (ITA)- U.S. Department of Commerce. "Welcome to the Privacy Shield." Erişim 18 Şubat, 2020. https://www.privacyshield.gov/welcome.

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

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

27. Article 29 Working Party. "Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors, WP 263 Rev.01." Son güncelleme 16 Nisan, 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

28. Blair, Tess, Vincent M. Catanzaro ve Sarah E.Moran. "Appropriate Safeguards in the GDPR- the Edata Guide to GDPR." Son güncelleme 14 Şubat, 2019. https://www.morganlewis.com/pubs/appropriate-safeguards-in-the-gdpr.

29. Article 29 Working Party. "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)." Son güncelleme 22 Kasım, 2006. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.

30. Kişisel Verileri Koruma Kurumu. "6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi kapsamında, yurtdışına veri aktarımında veri

sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlar." Son güncelleme 16 Mayıs, 2018. https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler.

31. Kişisel Verileri Koruma Kurumu. "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü." Erişim 18 Şubat, 2020. https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu.

32. Gelir İdaresi Başkanlığı. "FATCA Anlaşmasıyla İlgili Sıkça Sorulan Sorular." Erişim 12 Kasım, 2019. https://www.gib.gov.tr/uluslararasi_mevzuat/fatca-sorular.

33. Şanlı, Cemal, Emre Esen, ve İnci Ataman-Figanmeşe. *Milletlerarası Özel Hukuk*. İstanbul: Vedat Kitapçılık Basım Yayım Dağıtım Ltd. Şti., 2018.

34. Council of Europe. "Enhancing data protection globally: Council of Europe updates its landmark convention." Erişim 12 Kasım, 2019. https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976.

35. Council of Europe. "The modernised Convention 108: novelties in a nutshell." Erişim 12 Kasım, 2019. https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

36. International Court of Justice. "Legal Consequences for States of the Continued Presence of South Africa in Namibia (South-West Africa) notwithstanding Security Council Resolution 276 (1970) Advisory Opinion of 21 June 1971." Erişim 12 Kasım, 2019, https://www.icj-cij.org/files/case-related/53/053-19710621-ADV-01-00-EN.pdf.

37. Göçer, Mahmut. "Uluslararası İnsan Hakları Andlaşmalarının Bağdaşmazlığı Sorunu ve Uluslararası Hukuk." *Ankara Üniversitesi SBF Dergisi* Cilt/Sayı 56-3. 47-70.

38. Tanaka, Yoshifumi. "Protection of Community Interests in International Law: The Case of the Law of the Sea." *Max Planck Yearbook of United Nations Law* Vol.15. 2011. 329-375.

39. Council of Europe. "Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data."Son güncelleme 28 Ocak, 1981. https://rm.coe.int/16800ca434.

40. Hague Conference on Private International Law. Status Table 14: Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters. Son güncelleme 22.11.2019. https://www.hcch.net/en/instruments/conventions/status-table/?cid=17.

41. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. 2016. *Official Journal of the European Union* L 207/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

42. Council of Europe. Reservations and Declarations for Treaty No.108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Erişim 18 Şubat, 2020. https://www.coe.int/en/web/conventions/full-list/-

/conventions/treaty/108/declarations?p_auth=YP6ZdjNO&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=TUR&_coeconventions_WAR_coeconventionsportlet_codeNature=3.

43. Council of Europe."Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows." Son güncelleme 8 Kasım, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce56.

44. The Office of the High Commissioner for Human Rights. "Right to privacy-Note by the Secretary-General." Erişim 18 Şubat, 2020. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_73_45712.docx.

45. Kuner, Christopher. "Extraterritoriality and regulation of international data transfers in EU data protection law." *International Data Privacy Law* Volume 5, Issue 4 (2015 November), 235-245. Erişim 15 Şubat, 2020. https://doi.org/10.1093/idpl/ipv019.

46. Kierkegaard, Sylvia, Nigel Waters, Graham Greenleaf, Lee A. Bygrave, Ian Lloyd, Steve Saxby. "30 years on – The review of the Council of Europe Data Protection Convention 108." *Computer Law & Security Review* Volume 27, Issue 3, (2011 June), 223-231. Erişim 18 Şubat, 2020.

47. Greenleaf, Graham. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108." *International Data Privacy Law* Volume 2, Issue 2, (2012). Erişim 15 Şubat, 2020.

48. Greenleaf, Graham. "'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?" *Computer Law& Security Review* Volume 29, Issue 4, (2013 August), 430-436. https://doi.org/10.1016/j.clsr.2013.05.015.

49. Greenleaf, Graham. "Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives." Privacy Laws& Business International Report 142, (2016 August), 14-17.

50. De Hert, Paul, Vagelis Papakonstantinou. "The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition." *Computer Law& Security Review* Volume 30, Issue 6, (2014 December), 633-642. Erişim 21 Şubat, 2020. https://doi.org/10.1016/j.clsr.2014.09.002.

51. Irion, Kristina. "EU Law on Cross-Border Flows of Personal Data in a Global Perspective." (2018).

52. Cory, Nigel. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Son güncelleme 1 Mayıs, 2017. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

53. Bu-Pasha, Shakila. "Cross-border issues under EU data protection law with regards to personal data protection." Information & Communications Technology Law Volume 26, Issue 3, (2017), 213-228. Erişim 18 Şubat, 2020. https://doi.org/10.1080/13600834.2017.1330740.

54. European Commission. “Communication on Building a European Data Economy.” Son güncelleme 10 Ocak, 2017. https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy.

55. IDC. “The Digitization of the World: From Edge to Core.” Son güncelleme Kasım, 2018. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

56. European Commission. “European Data Strategy.” Son güncelleme 19 Şubat, 2020. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

57. UNCTAD. “Data protection regulations and international data flows: Implications for trade and development.” Son güncelleme 19 Nisan, 2016. https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

58. Ferracane, Martina F., *Restrictions on Cross-Border data flows: a taxonomy*. ECIPE, 2017. https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf.

59. World Economic Forum. “Exploring International Data Flow Governance Platform for Shaping the Future of Trade and Global Economic Interdependence.” Son güncelleme 17 Aralık, 2019. http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.

60. Digital Competition Expert Panel. “Unlocking digital competition: Report of the Digital Competition Expert Panel.” Son güncelleme 13 Mart, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.