İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
HUKUK YÜKSEK LİSANS PROGRAMI

KİŞİSEL VERİLERİN KORUNMASINDA HESAP VEREBİLİRLİK ARAÇLARI: DAVRANIŞ KURALLARI VE SERTİFİKASYON

İlayda ÇELİK
118613032

Doç. Dr. Mehmet Bedii KAYA

İSTANBUL
2023

Kişisel Verilerin Korunmasında Hesap Verebilirlik Araçları:
Davranış Kuralları ve Sertifikasyon
Data Protection Accountability Tools: Codes of Conduct and Certification

İlayda ÇELİK
118613032

Tez Danışmanı : **Doç. Dr. Mehmet Bedii KAYA**
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Prof. Dr. Leyla KESER BERBER**
İstanbul Bilgi Üniversitesi

Doç. Dr. Mesut Serdar ÇEKİN
Türk-Alman Üniversitesi

Tezin Onaylandığı Tarih : 19.06.2023
Toplam Sayfa Sayısı : 161

Anahtar Kelimeler (Türkçe)
1) AB Genel Veri Koruma Tüzüğü
2) Kişisel Verilerin Korunması
3) Hesap Verebilirlik
4) Davranış Kuralları
5) Sertifikasyon

Anahtar Kelimeler (İngilizce)
1) General Data Protection Regulation
2) Protection of Personal Data
3) Accountability
4) Codes of Conduct
5) Certification

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASINDA TEMEL HESAP VEREBİLİRLİK ARAÇLARI

DÖRDÜNCÜ BÖLÜM
HESAP VEREBİLİRLİK ARACI OLARAK DAVRANIŞ KURALLARI

BEŞİNCİ BÖLÜM
HESAP VEREBİLİRLİK ARACI OLARAK SERTİFİKASYON

ALTINCI BÖLÜM
TÜRK HUKUKUNDA HESAP VEREBİLİRLİK

KISALTMALAR

AB	**:**	Avrupa Birliği
ABAD	**:**	Court of Justice of the European Union (Avrupa Birliği Adalet Divanı)
AEA	**:**	Avrupa Ekonomik Alanı
A.g.e.	**:**	Adı Geçen Eser
AİHM	**:**	Avrupa İnsan Hakları Mahkemesi
AİHS	**:**	İnsan Hakları Ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme
APEC	**:**	Asya-Pasifik Ekonomik İşbirliği
bkz.		Bakınız
dn.	**:**	Dipnot
EDPB	**:**	European Data Protection Board (Avrupa Veri Koruma Kurulu)
GVK Tüzüğü	**:**	General Data Protection Regulation (2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü)
IEC	**:**	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
ISO	**:**	International Organization for Standardisation (Uluslararası Standardizasyon Kurumu)
Komisyon	**:**	European Commission (Avrupa Komisyonu)
KVK Kurulu	**:**	Kişisel Verileri Koruma Kurulu
KVK Kurumu	**:**	Kişisel Verileri Koruma Kurumu
m.	**:**	Madde
OECD	**:**	Organisation for Economic Co-operation and Development (İktisadi İşbirliği ve Kalkınma Teşkilatı)
p.	**:**	Paragraf

OECD Rehber İlkeleri	**:**	OECD'nin Özel Yaşamın Gizliliğinin ve Sınır Aşan Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeleri
s.	**:**	Sayfa
TBMM	**:**	Türkiye Büyük Millet Meclisi
vd.	**:**	Ve devamı, Ve diğerleri
WP 29	**:**	Working Party 29 (Madde 29 Çalışma Grubu)
108 Sayılı Sözleşme	**:**	108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
108+ Sayılı Sözleşme	**:**	Convention 108+ (Modernize Edilmiş 108 Sayılı Sözleşme)
KVK Kanunu	**:**	6698 sayılı Kişisel Verilerin Korunması Kanunu
95/46 sayılı Direktif	**:**	Data Protection Directive 95/46/EC (95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi)

ÖZET

Bilgi ve iletişim teknolojilerinde özellikle son çeyrek yüzyılda yaşanan gelişmeler, önceki dönemlere kıyasla daha yüksek hacimli kişisel verilerin işlenmesi, işlenen kişisel verilerin çeşitliliği artması ve sınır ötesi aktarımlar dâhil olmak üzere kişisel verilerin dolaşımının yoğunlaşması ve hızlanmasına vesile olmuştur. Dijitalleşmedeki artış ile kişilerin bilgiye erişimi imkânı ve ilgili kişilerin kişisel verilerinin güvenliği konusundaki hassasiyeti artmış, kişisel verilerin takibi ve kontrolü güçleşmiştir. Kişisel verilerin bu kadar büyük ölçekte ve hızda işlenmesi, beraberinde veri işleme faaliyetlerinin hukuka uygunluğunun denetlenmesi bakımından güçlükler ortaya çıkarmaktadır. Bilhassa kişisel verilerin hukuka uygun olarak işlenip işlenmediğinin gözetiminden sorumlu veri koruma otoritelerinin zaman ve maliyet anlamında daha yönetilebilir ve belirli bir standarda dayalı çözümlere ihtiyaç duyması kaçınılmazdır.

Kişisel veri işleme süreçlerinin kompleks hale gelmesi yürürlükteki kişisel verilerin korunması mevzuatına uyumun ötesine geçilerek bu uyumluluğun yetkili kuruluşlar nezdinde ispat edilebilir hale gelmesini gerektirmektedir. Avrupa Birliği'nin veri koruma alanındaki öncü düzenlemesi olan 95/46 sayılı Direktif'in yeni tehditler karşısında kişisel verilerin etkin şekilde korunması ihtiyacını karşılayamaması üzerine, 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ("GVK Tüzüğü") yürürlüğe konulmuştur. GVK Tüzüğü, kişisel veri koruma hukukuna kazandırdığı hesap verebilirlik ilkesiyle kişisel verilerin korunmasında temel bir paradigma değişikliğine gitmiştir.

Bu çalışma ile "hesap verebilirlik ilkesi ışığında veri koruma mevzuatına uyumluluk nasıl ispat edilebilir ve ispat için hangi araçlar kullanılabilir?" sorularına cevap aranmaktadır. Çalışmada GVK Tüzüğü'ndeki hesap verebilirlik ilkesinin kapsamı, bu ilkeyi uygulamak için getirilen temel araçların niteliği, bilhassa da davranış kuralları ve sertifikasyon araçlarının temel çerçevesi ele alınacaktır.

Anahtar Kelimeler: AB Genel Veri Koruma Tüzüğü, kişisel verilerin korunması, hesap verebilirlik, davranış kuralları, sertifikasyon

ABSTRACT

Developments in information and communication technologies -especially in the last quarter century- have led to the processing of higher volumes of personal data, increasing the diversity of data processed, and intensification and acceleration of data circulation including the cross-border transfers. With the increase in digitalization, the individuals' ability to access information and sensitivity to their security of personal data have increased, and it has become difficult to monitor and control personal data. Processing personal data on such a large scale and speed creates difficulties in controlling the processing in accordance with the law. In particular, it is inevitable that data protection authorities responsible for overseeing whether personal data are processed in accordance with the law, need solutions that are more manageable in terms of time and cost, and with a certain standard.

Due to the complexity of data processing processes, it is necessary to go beyond compliance with the applicable personal data protection legislation and to make this compliance provable before the authorized institutions. Upon the failure of the Data Protection Directive 95/46/EC, the pioneering personal data regulation of the European Union, to meet the need for effective protection against new threats, the General Data Protection Regulation ("GDPR") entered into force. The GDPR has gone through a fundamental paradigm shift in the protection of personal data with the principle of accountability it brought to the personal data protection law.

This study seeks to answer the questions of *"How to demonstrate compliance with EU data protection legislation in light of the principle of accountability and what tools can be used to prove compliance?"*. In the study, the scope of the accountability principle in the GDPR, the nature of the basic tools brought to implement this principle, and especially the basic framework of the codes of conduct and certification tools will be discussed.

Keywords: General Data Protection Regulation, protection of personal data, accountability, codes of conduct, certification

GİRİŞ

Kişisel verilerin korunması uzun yıllardır, özellikle de Avrupa Birliği ("AB") hukukunda, önemli bir yer teşkil etmekte ve gerçek kişilerin temel hak ve özgürlüklerinin korunması ile doğrudan ilişkili bu tarz düzenlemeler gün geçtikçe daha da önem kazanmaktadır. 95/46 sayılı Direktif'in yürürlükte olduğu dönemde, kişisel verilerin korunması ihtiyaçtan ziyade külfet olarak görülmüş, mahremiyetin sağlanması bakımından veri sorumlusuna ait olması gereken sorumluluk kişisel verilerin sahibi olan ilgili kişilerin üstünde kalmıştır[1].

Bilgi ve iletişim teknolojilerindeki yeniliklerin giderek fazlalaşması (bulut bilişim ve e-ticaret araçlarının[2], çevrimiçi hizmetlerin kullanımının artması vb.), kişisel verilerin serbest akışının hızlanması ve yoğunlaşması ve ilgili kişilerin verileri üzerinde bireysel kontrollerinin azalması gibi sebeplerden ötürü, kişisel verilerin korunması ile ilgili yürürlükteki düzenlemeler yetersiz kalmıştır. Bu yetersizlik, mahremiyetin korunmasına hizmet eden hesap verebilirlik ve şeffaflık gibi önemli kavramlara duyulan ihtiyacı da kapsamaktaydı[3]. Zira hesap verebilirlik ilkesinin AB veri koruma mevzuatına normatif anlamda kazandırılmasının, mevzuata uyumluluk için etkili politika ve mekanizmalar oluşturması konusunda veri sorumlularını destekleyeceği düşünülmeye başlanmıştı[4]. Bu bağlamda 95/46 sayılı Direktif'in yetersiz hale gelmesiyle, veri sorumluları ve ilgili mevzuatta düzenlenen hallerde veri işleyenler ile ilgili daha kapsamlı yükümlülükler getiren GVK Tüzüğü kabul edilerek yürürlüğe girmiştir.

---

[1] Strauß, S. (2020). Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment (1st ed.). *How to regain control? - Assessing privacy by design and privacy impact assessment.* Routledge. s.206.
[2] Alhadeff, J., van Alsenoy, B., & Dumortier, J. (Eylül 2011). *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions.* In D. Guagnin, L. Hempel, C. Ilten, et al. (Eds.), Managing Privacy through Accountability, s. 49.
[3] Strauß (2020), s.11.
[4] Alhadeff et al. (2011), s. 49.

Farklı disiplinlerde karşılığı olan hesap verebilirlik kavramı genel itibariyle, bir tarafın sorumluluk alanı içindeki davranış ve işlemleri ile ilgili yetkili taraflara açıklama yapabilir/cevap verebilir durumda olması anlamına gelir. GVK Tüzüğü'nde öngörülen hesap verebilirlik ilkesi ise, veri sorumlularının ilgili mevzuattan doğan yükümlülüklerinin dış dünyadan kendilerine yönelen yeni bir kontrol mekanizması ile denetlenmesine imkân sağlamıştır. AB veri koruma hukukuna kazandırılan hesap verebilirlik ilkesi ve çeşitli hesap verebilirlik araçları sayesinde kişisel veri işleme faaliyetlerinin veri koruma mevzuatına uygun olarak yürütüldüğü yönünde bir karine ortaya konulması da mümkün hale gelmiştir.

Çalışma, toplamda altı ana bölümden oluşmaktadır. Çalışmanın ilk bölümünde, hesap verebilirlik ilkesine genel bir bakış yapılarak hesap verebilirlik kavramının anlamı ve hesap verebilirlik ilkesinin AB veri koruma hukuku dışındaki muhtelif disiplin ve düzlemlerdeki karşılıkları incelenecektir.

Çalışmanın ikinci bölümde, ilk olarak hesap verebilirlik ilkesinin AB bilişim ve teknoloji hukukundaki yeri incelenecek, daha sonra bu ilkenin AB kişisel veri mevzuatındaki karşılığı ile temel özelliklerinden bahsedilecektir.

Çalışmanın üçüncü bölümü, temel hesap verebilirlik araçlarından olan ve GVK Tüzüğü'nün 40. ve 41. maddelerinde düzenlenen davranış kuralları ile 42. ve 43. maddelerinde düzenlenen sertifikasyon mekanizmalarını genel hatlarıyla inceleyecek ve bunlar arasındaki ilişkiyi anlamaya çalışılacaktır. Bu bağlamda, davranış kuralları ile sertifikasyon gerek kavramsal gerek fonksiyonel özellikleri bakımından değerlendirilecektir.

Çalışmanın dördüncü bölümü, GVK Tüzüğü m.40-41'de düzenlenen davranış kurallarına odaklanacaktır. Önceki bölümde davranış kuralları için genel bir çerçevesi çizilmesi dolayısıyla bu bölümde ilk olarak davranış kurallarının kapsamı ve davranış kuralları ile ilgili aktörler detaylandırılacaktır. Ardından, hesap verebilirlik araçlarından davranış kurallarının onaylı hale gelerek geçerli olabilmesi

için izlenmesi gereken adımların neler olduğu açıklanacak ve son olarak üçüncü ülkelere veri aktarımı gerçekleştirilmesi için bu kurallardan nasıl yararlanılabileceği somutlaştırılmaya çalışılacaktır.

Çalışmanın beşinci bölümü, GVK Tüzüğü, m.41-42'de düzenlenen hesap verebilirlik araçlarından sertifikasyona odaklanacaktır. Bu bölümde ilk olarak sertifikasyonun temel bileşenleri ve kapsamı, akreditasyon kavramı ile ilişkisi incelenecek, daha sonra sertifikasyon ve akreditasyon aktörleri ile bunların görev ve yetkileri, sertifikasyon kriterleri ve prosedürü ele alınacaktır. Bölümün sonunda sertifikasyonun üçüncü ülkelere transfer aracı olarak kullanılmasına dair açıklamalar yapılacaktır.

Çalışmanın altıncı ve son bölümünde ise hesap verebilirlik ilkesi, hâlihazırda yürürlükte olan Türk hukuku düzenlemeleri, bilakis Türk veri koruma perspektifinde ele alınacaktır. Bu bağlamda, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVK Kanunu") çerçevesinde yürütülen kişisel veri işleme faaliyetlerinin ilgili mevzuata uyumluluğunu göstermeye yarayan araçlar olup olmadığı ve Kişisel Verileri Koruma Kurumu'nun ("KVK Kurumu") hesap verebilirlik kavramına yaklaşımı değerlendirilecektir.

Çalışmanın merkezinde GVK Tüzüğü'ndeki anlam ve kapsamıyla hesap verebilirlik ilkesi bulunmaktadır. Bu bağlamda hesap verebilirlik araçlarından davranış kuralları ve sertifikasyon AB hukuku tahtında ele alınacak olup hesap verebilirlik ilkesinin muhtelif disiplinlerdeki görünümlerine yalnızca gerekli yerlerde ve önemli olduğu ölçüde değinilecektir. Çalışmanın hazırlığında doktrinsel inceleme metotlarına başvurulacaktır. Ayrıca çalışmanın son bölümünde, hesap verebilirlik ilkesi ve araçlarının Türk veri koruma hukukundaki yeri inceleneceğinden, metodolojik olarak mukayeseli hukuk yöntemleri kullanılacaktır. Esas alınan konu itibariyle çalışma kapsamında ampirik (nicel) veya karma yöntemlere başvurulmamış ve nitel araştırma yöntemlerinden yararlanılmıştır.

Çalışma ile ulaşılmak istenen nihai amaç; hesap verebilirlik ilkesinin tarihsel gelişimi ile AB veri koruma hukukundaki yerinin incelenmesi, GVK Tüzüğü'nde düzenlenen hesap verebilirlik araçlarından davranış kuralları ve sertifikasyonun avantaj/dezavantajlarının ele alınması ve mevzuata uyumun ispatı bakımından yeterliliğinin değerlendirilmesi, hesap verebilirlik ilkesinin Türk hukukundaki yerinin incelenmesi, AB hukuku ile kıyaslanması ve Türk hukukundaki eksiklik ve iyileştirme alanlarının tespit edilmesi, bu konularda gelecekte yapılacak çalışmalar için Türkçe kaynak oluşturularak hukuk literatürüne katkı sağlanmasıdır.

BİRİNCİ BÖLÜM

HESAP VEREBİLİRLİK İLKESİNE GENEL BAKIŞ

1.1. HESAP VEREBİLİRLİK KAVRAMI

Hesap verebilirlik, birden fazla disiplini ilgilendiren ve tek bir tanımı olmayan bir kavramdır. Genel bir tanımlama yapmak gerekirse hesap verebilirlik; *"kişilerin eylemleri dolayısıyla yetkili otoriteler nezdinde hukuksal, yönetsel, idari ve politik anlamda sorumlu tutulabilmesi*[5] *ve gerçekleştirilen eylemlerin hesap sorma yetkisini haiz ilgili otorite nezdinde savunulması*[6]*"* anlamına gelmektedir. Bu bağlamda, kişilerin eylemlerini uygun araçlarla açıklayabilmesi, her türlü eylem ve kararının sonuçları olduğunu bilmesi ve bu sonuçları kabul etmesi hesap verebilirlik kavramının temelini oluşturmaktadır. Teknik olarak hesap verebilirlik, yalnızca hesap veren tarafların sahip olduğu sorumluluklarla ilgilenmez, bu sorumluluklara uyumun ilgili taraflarca nasıl belgelendiğine de bakar[7]. Bu bağlamda, etkili bir hesap verebilirlikten bahsedilebilmesi için 'sorumluluk' ve 'belgeleme' olmak üzere iki temel unsurun varlığı aranacak ve iki unsur birbirinden ayrı düşünülemeyecektir.

Esasında farklı disiplinlerde kendine yer bulan hesap verebilirlik çatı bir kavram olup bu kavram, türüne göre; **(i)** yönetsel hesap verebilirlik, **(ii)** siyasi hesap verebilirlik, **(iii)** profesyonel hesap verebilirlik, **(iv)** kamusal hesap verebilirlik ve **(iv)** hukuki hesap verebilirlik olarak kategorize etmek mümkündür. Bu sınıflandırma, okuyucu nezdinde hesap verebilirlik kavramı ile ilgili genel ve

[5] Aktan, C. C., Dileyici, D., & Vural, İ. Y. (2006). *Kamu Maliyesinde Çağdaş Yaklaşımlar* (1. Baskı), s.228; Burke, C. S., Sims, D. E., Lazzara, E. H., & Salas, E. (2007). Trust in leadership: A multi-level review and integration. *The Leadership Quarterly*, 18(6), s.619.

[6] Aktan et al. (2006), s.228; Buckley, M. R., Beu, D. S., Frink, D. D., Howard, J. L., Berkson, H., Mobbs, T. A., & Ferris, G. R. (2001). Ethical issues in human resources systems. *Human Resource Management Review, 11*,, s.18.

[7] Madde 29 Çalışma Grubu (13 Temmuz 2010). *Opinion 3/2010 on the principle of accountability*, s.7. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (Erişim Tarihi: 29.05.2023)

anlaşılır bir çerçeve çizilebilmesi için yapılmış olup bu sınıflandırmanın farklı şekillerde yapılması mümkündür. Keza bu kavramın, hesap verebilirlik kavramının ele alındığı farklı akademik disiplinlerde nispeten farklı şekilde ve/veya detayda kategorize edildiği haller vardır[8].

1.1.1. Hesap Verebilirlik Türleri

Yönetsel hesap verebilirlik, idarenin kendi bünyesindeki yapılar tarafından denetlenmesi ve idare tarafından kendi içinde yer alan kişi, kurum ya da organlara hesap verilmesi[9] anlamına gelmektedir. Yönetsel hesap verebilirlik bazı kaynaklarda bürokratik hesap verebilirlik veya hiyerarşik hesap verebilirlik olarak da adlandırılabilmektedir. Esasında hiyerarşik hesap verebilirlik, yönetsel hesap verebilirliğin bir parçası olup bu kavram ilgili kuruluş içerisindeki hiyerarşide üst kademeye hesap verilmesi anlamına gelir. Yönetsel hesap verebilir sayesinde idare bünyesinde kamu gücü kullanan taraflarca yürütülen idari eylem ve işlemler kontrole tabi tutulur ve bahsi geçen eylem ve işlemlerin hukuka uygunluğu denetlenir.

Geleneksel anlamda **siyasi hesap verebilirlik**, devlet otoritesinin işletmekle görevli hükümet ile hükümet bünyesindeki siyasi aktörlerin parlamentoya hesap vermesi olarak karşımıza çıkmaktadır[10]. Günümüz anlayışına göre siyasi veya politik hesap verebilirlik ise politikacıların, demokratik sistemlerde siyasal iktidarın meşruiyetini sağlamaya yarayan seçimler aracılığıyla kendisine siyasi güç sağlanmasına ilişkin karar veren halk tarafından denetlemesi anlamına

[8] Farklı sınıflandırmalar için bkz. Romzek, B. S. (2000). Dynamics of Public Sector Accountability in an Era of Reform. *International Review of Administrative Sciences*, 66, s.23; Jabbra, J. G., & Dwivedi, O. P. (Eds.). (1989). Public service accountability: A comparative perspective (s. 273). Connecticut, Kumarian Press; Cendón, A.B. (1999*). Accountability and Public Administration: Concepts, Dimensions, Developments*.

[9] Eryılmaz, B., & Biricikoğlu, H. (2011). Kamu yönetiminde hesap verebilirlik ve etik. *İş Ahlakı Dergisi*, 4, s.26.

[10] Balcı, A., Nohutçu, A., Öztürk, N. K., & Coşkun, B. (2013). *Kamu Yönetiminde Çağdaş Yaklaşımlar: Sorunlar, Tartışmalar, Çözüm Önerileri, Modeller, Dünya ve Türkiye Yansımaları* (3. Baskı), s. 119.

gelmektedir[11]. İlaveten, siyasi hesap verebilirliğin siyasilerin yanı sıra bu kişiler tarafından atanan yöneticileri de içeren bir kavram olduğu söylenebilecektir[12]. Literatürde bu kavramın, politik hesap verebilirlik olarak adlandırıldığı da görülür.

Profesyonel hesap verebilirlik ile kast edilen, belirli alanlarda uzmanlaşmış profesyonellerin sahip oldukları yetkinlikleri bakımından, ilgili uzmanlık alanlarında teknik bilgi sahibi organlara karşı hesap verebilmesidir.

Kamusal hesap verebilirlik, kamu örgütündeki çalışanların kendilerine verilen yetkileri gereği gibi kullanıp kullanmadığı ile söz konusu yetkileri kullanılması sonucu arzu edilen sonuçlara adil ve etkin bir şekilde ulaşılıp ulaşılmadığının kontrolünü amaçlar[13]. Bu kontrolün kamu idarelerine yetki veren halk tarafından kamuoyunun gücünü kullanmak suretiyle gerçekleştirilmesi esastır. Bovens'a göre[14], kontrole tabi çalışanlar çoğunlukla kendilerini performansları bakımından kamuoyuna hesap verme yükümlülüğü altında hisseder.

Nihayet, **hukuki veya yasal hesap verebilirlik**, hukuk devleti ve hukukun üstünlüğü ilkelerinin gereği olarak, her türlü eylem, işlem ve tasarruflar bakımından gerektiğinde yetkili otoriteler nezdinde hesap verilmesini ifade etmektedir. Bu ilkenin varlığı, idare tarafından gerçekleştirilen eylem, işlem ve tasarrufların adilliği, rasyonelliği ve hukuka uygunluğunu temin eder. Kamusal faaliyetlerin yürütülmesinde yetkili tarafların söz konusu faaliyetleri ile ilgili olarak mahkemeler nezdinde hesap vermesi hukuki hesap verebilirlik olarak

[11] Aktan et al. (2006), s.171.
[12] Mulgan, R. (2003). *Holding Power to Account: Accountability in Modern Democracies.* London, England: Springer.
[13] Gül, S. K. (2008). Kamu yönetiminde ve güvenlik hizmetlerinde hesap verebilirlik. *Polis Bilimleri Dergisi*, 10, s.79.
[14] Bovens, M. (2007). Analyzing and Assessing Accountability: *A Conceptual Framework. European Law Journal,* 13, s. 457.

karşımıza çıkmaktadır[15]. Bununla birlikte hukuki hesap verebilirlik kavramı, kuruluşların tabi oldukları yasal düzenlemelere uygun davranılması bakımından yetkili otoriteler karşısında hesap verebilir olması[16] anlamına da gelir. Çalışmanın temelinde AB kişisel verilerin korunması mevzuatına uyum olduğundan, çalışma kapsamında hukuki hesap verebilirlik ele alınacaktır.

1.2. ULUSLARARASI DÜZENLEMELERDE HESAP VEREBİLİRLİK

Hesap verebilirlik ilkesinin muhtelif disiplinlerde karşılık bulması dolayısıyla gerek bağlayıcı gerekse açıklayıcı veya yol gösterici olan birçok kaynakta hesap verebilirlik ile ilgili düzenlemelere yer verildiği görülmektedir. Bu düzenlemelerden bazıları lafzi olarak hesap verebilirlik ilkesine referans içerirken bazıları ise doğrudan bir referansta bulunmasa bile ruhu itibariyle hesap verebilirlik ilkesi ile ilişki içerisindedir.

Çalışmanın bu kısmında, hukuk disiplinde kendine yer bulan ve sıklıkla mahremiyet kavramı ile ilişkilendirilen hesap verebilirlik ilkesinin, AB hukukunun ötesine geçen farklı düzlemlerdeki en temel yansımaları ile sınırlı bir inceleme yapılacak[17] olup AB hukukundaki düzenlemeler çalışmanın ikinci bölümünde ele alınacaktır. Küresel çerçevede bir değerlendirme yapıldığında, hesap verebilirlik ilkesinin hem uluslararası anlaşmalar, standartlar ve sair düzenlemelerde kendine yer bulduğu hem Avrupa kıtasında yer almayan birçok ülkenin hukuk sistemine konu olduğu görülür.

---

[15] Tutar, H., & Altınöz, M. (2017). Hesap verebilirlik bağlamında iç denetim ve sorun alanları: Eleştirel bir analiz. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 8, s.232; Gül, 2008, s.78.

[16] Quelle, C. (2017). The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too. In R. Leenes, R. van Brakel, S. Gutwirth, & P. De Hert (Eds.), *Data Protection and Privacy: The Age of Intelligent Machines (Forthcoming).* Tilburg Law School Research Paper No. 17. Tilburg University - Tilburg Institute for Law, Technology, and Society (TILT). https://ssrn.com/abstract=3000382 (Erişim Tarihi: 29.05.2023)

[17] Bu başlık altında konuyla ilgili en temel kaynaklardan olmaması dolayısıyla ayrıca kendine yer bulamamış olan, ancak hesap verebilirlik ilkesi ile ilgili sair düzenlemeler için bkz. Kaya (2020), s.1887.

1.2.1. İktisadi İşbirliği ve Kalkınma Teşkilatı

23 Eylül 1980 tarihinde İktisadi İşbirliği ve Kalkınma Teşkilatı ("OECD") tarafından kabul edilen Özel Yaşamın Gizliliğinin ve Sınır Aşan Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler ("OECD Rehber İlkeleri") hukuken bağlayıcı olmamakla birlikte, hesap verebilirlik ilkesini ilk olarak ayrı bir veri koruma ilkesi olarak tanıtması[18] bakımından oldukça önemli bir kaynaktır.

OECD Rehber İlkeleri'nin 14. maddesinde "*veri sorumlusunun belirtilen ilkelere uyulması için öngörülen önlemlere uymaması halinde sorumluluk taşıyacağı*" denilmek suretiyle hesap verebilirlik ilkesine yer verilmiş olup ilgili maddede anılan ilkeler, aynı rehberin 7 ila 13 maddeleri arasında sayılmaktadır[19]. OECD Rehber İlkeleri ile hesap verebilirlik ilkesine yer verilmesi iki amaca hizmet eder. Bunlardan ilki, veri sorumlusunun ilgili veri koruma düzenlemelerine uyum bakımından sorumlu kişi olarak adreslenmesi iken; ikincisi ise uyumun sağlanması sorumluluğunu yerine getirmeyen veri sorumlusunun hesap vermesi için üye devletlerin gerekli mekanizmalar kurgulamasını teşvik eder[20].

1980 yılında kabul edilen OECD Rehber İlkeleri'nde 2013 yılında yapılan değişiklikler ile, veri sorumluları için öngörülen sorumluluklara ilave olarak hesap verebilirlik ilkesinin uygulamasına ilişkin birtakım düzenlemeler getirmiştir. OECD Rehber İlkeleri'nin önceki versiyonunda bulunmayıp güncellenmiş versiyonun "üçüncü bölüm" başlığı ve 15. maddesine yapılan eklemeler, veri sorumlusundan uygulamaya koyması beklenen 'mahremiyet uyum programı' kavramını ve bu kavramın kapsamını düzenlemektedir. Bu bağlamda veri sorumlusu, ilgili 15. maddenin (a) bendinde belirtilen kapsama uygun olan düzenlenen bir mahremiyet uyum programı hazır bulundurmakla ve yetkili mahremiyet otoritesinin kendisinden bu yönde bir talebi olması halinde bu

[18] Alhadeff et al. (2011), s. 55.
[19] Bahsi geçen ilkeler sırasıyla; veri toplamanın sınırlanması, veri kalitesi, işleme amacının belirli olması, kullanımın sınırlanması, veri güvenliği, açıklık ve kişisel katılımdır.
[20] A.g.e., s. 55.

programı ilgili otoriteye sunmakla yükümlüdür. Ayrıca, aynı maddenin (b) bendi ile veri sorumlusu, işlediği kişisel verileri etkileyen esaslı bir güvenlik ihlali olması durumunda yetkili mahremiyet otoritesini bilgilendirmekle sorumlu tutulmuştur.

2013 yılında yapılan güncellemelere rağmen OECD Rehber İlkeleri, veri sorumlusunun sorumluluk rejimi kapsamında yaptırım düzenlemeleri getirmemesi ve dolayısıyla 'sorumluluk olmaksızın hesap verebilirlik' yaratması sebebiyle eleştirilmiştir[21]. Yine de, OECD Rehber İlkeleri hesap verebilirlik ilkesine hakkında farkındalık ve tanınırlık kazanılmasına öncülük etmiş, aynı zamanda bu ilkenin ulusal ve uluslararası nitelikte olan çeşitli veri koruma düzenlemelerinde kendisine yer bulmasına zemin hazırlamıştır[22].

1.2.2. ISO/IEC 29100, ISO/IEC 27701 ve ISO/DIS 31700 Standartları

Uluslararası Standardizasyon Kurumu ("ISO") ile Uluslararası Elektroteknik Komisyonu ("IEC") işbirliği ile hazırlanan "Bilgi Teknolojileri - Güvenlik Teknikleri - Gizlilik Çerçevesi" ISO/IEC 29100 Standardı[23] ("ISO/IEC 29100"), bilgi ve iletişim teknolojilerinde kişisel verilerin korunması ile ilgili düzenlemeler içermektedir. ISO/IEC 29100 ile hedeflenen kişisel verilerin işlenmesinde dikkate alınacak mevcut güvenlik standartlarının iyileştirilmesi ile sınırlı olmadığı gibi, aynı zamanda bu standart sayesinde kişisel verilerin korunması bakımından hukuk dünyası ile bilgi ve iletişim teknolojileri dünyası arasında ortak bir anlayış yaratılmak istenmiştir. Ortak bir anlayış ortaya koyma çabası ise, hukuk dünyası

[21] Greenleaf, G. (2019, Mayıs). Accountability Without Liability: 'To Whom'and 'With What Consequences'? (Questions for the 2019 OECD Privacy Guidelines Review). *UNSW Law Research Paper No. 19-67.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427 (Erişim Tarihi: 29.05.2023); Tene, O. (2013). Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. Ohio State Law Journal, 74(6), s.1222. https://core.ac.uk/download/pdf/159560945.pdf (Erişim Tarihi: 29.05.2023)

[22] Tene (2013), s.1221.

[23] ISO/IEC. (2011). ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework. https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en (Erişim Tarihi: 29.05.2023)

ve teknik dünyaya ait kurallar arasındaki *"çapraz etkileşim"*in bir gereğidir[24]. ISO/IEC 29100 standardında, bilgi ve iletişim teknolojileri sistemlerinde kişisel verilerin korunmasına yönelik somut ve pratik tedbirler alınmasını gerektiği vurgulanmış ve bu kapsamda veri koruma ilkelerine uyumluluğun ortaya konulabilmesi adına birtakım teknik ve idari tedbirler öngörülmüştür. Başka bir deyişle, hesap verebilirlik ilkesinin gerekliliklerinin yerine getirilmesi için kuruluşlar tarafından atılması gereken adımlar[25] bir standart haline getirilmiştir.

Kişisel verilerin işlenmesi bakımından kuruluşlara güvenlik standartları getirilmesi amacıyla ISO ve IEC tarafından hazırlanan ve 2019 yılından yayımlanan bir diğer standart ise, "Güvenlik teknikleri - Gizlilik bilgi yönetimi için ISO/IEC 27001 ve ISO/IEC 27002'ye ek - Gereklilikler ve rehber"[26] ("ISO/IEC 27701") standardıdır. ISO/IEC 29100'de olduğu gibi, ISO/IEC 27701 içerisinde de hesap verebilirlik ilkesine yer verilmiş olmakla birlikte, kullanılabilecek hesap verebilirlik araçları için ISO/IEC 29100'e atıf yapılmakla yetinilmiştir.

En son 31 Ocak 2023 tarihinde ISO tarafından ISO 31700-1 ve ISO/TR 31700-2 standartları[27] yayımlanmıştır. Bu standartlar, tüketim malları ve hizmetleri için tasarım yoluyla gizlilik suretiyle tüketicinin gizlilik ihtiyaçlarının karşılanması ve dolayısıyla güveninin artmasına hizmet etmek üzere oluşturulmuştur. ISO 31700-1 standardı ile "personally identifiable information (PII)" kavramı tanımlanmış olup tüketicilere ait kişisel verilerin, *kişisel olarak tanımlanabilir bilgiler* – yani

[24] Berber, L. K. & Bilgili, A. C. (2020, Ocak). Çapraz Etkileşim: Mahremiyete İlişkin Mevzuat ve Mahremiyet Standartları Arasındaki İlişki. *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku. Marmara Hukuk Bilimsel Toplantılar Serisi – 1*, s. 2. On İki Levha Yayıncılık.
[25] Kaya (2020), s. 1876-1877.
[26] ISO/IEC. (2019). *ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en (Erişim Tarihi: 29.05.2023)
[27] ISO. (2017). ISO 31700-1, *Consumer protection - Privacy by design for consumer goods and services - Part 1: High-level requirements.* https://www.iso.org/obp/ui/#iso:std:iso:tr:31700:-2:ed-1:v1:en (Erişim Tarihi: 29.05.2023); ISO. (2019). ISO 31700-1, *Consumer protection - Privacy by design for consumer goods and services - Part 2: Use cases.* https://www.iso.org/obp/ui/#iso:std:iso:tr:31700:-2:ed-1:v1:en (Erişim Tarihi: 29.05.2023)

PII- olarak adlandırıldığı görülmektedir. Ayrıca bu standarda göre, "tasarım yoluyla gizlilik" üç yol gösterici ilke ile açıklanabilecektir. Bu ilkelerden biri olan "Güçlendirme ve şeffaflık" başlığı altında, dijitalleşmenin bir sonucu olarak PII işleyen tüketici ürünlerinin tasarımı ve işletilmesi söz konusu olduğunda şeffaf ve hesap verebilir olma ihtiyacının arttığı belirtilerek hesap verebilirlik ilkesinden bahsedilmektedir. Ayrıca ilgili standardın kavramlar ve anlamlarını düzenleyen başlığı altındaki 3.17. numaralı "bilgi güvenliği (information security)" tanımda da hesap verebilirlik ilkesinden bahsedildiği görülmektedir.

1.2.3. Avrupa Konseyi'nin 108 ve 108+ Sayılı Sözleşmeleri

Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ("108 Sayılı Sözleşmesi"), kişisel verilerin korunması alanında bağlayıcı nitelikte bir uluslararası belge olup bu sözleşmede hesap verebilirlik ilkesinden açıkça bahsedilmemektedir. Buna karşın, 108 Sayılı Sözleşme ile getirilen bazı şartların doğrudan değilse bile dolaylı olarak hesap verebilirliğe hizmet ettiği söylenebilecektir[28].

Bilgi ve iletişim teknolojileri alanındaki hızlı gelişmeler karşısında yeterli görülmeyen 108 Sayılı Sözleşme'de reforma gidilmiş ve 108+ Sayılı Sözleşme kabul edilmiştir. Esasen reform sonrası kabul edilen bu yeni sözleşme "223 numaralı Sözleşme" olmakla birlikte, içerik olarak 108 Sayılı Sözleşme'de ele alınan konulardan sapmayıp bunlarla ilgili daha kapsayıcı düzenlemelere yer verdiğinden 108+ Sayılı Sözleşme olarak adlandırıldığı görülmektedir. Hesap verebilirlik ilkesi, 108 Sayılı Sözleşme'de olduğu gibi 108+ Sayılı Sözleşme'nin lafzında da yer almamaktadır. Buna karşın, 108+ Sayılı Sözleşme ile getirilen yenilikler sayesinde, hesap verebilirlik ilkesinin lafzi olarak değilse bile sözleşmenin ruhunda bulunduğu söylenebilecektir[29]. Hesap verebilirlik ilkesi ile

[28] Detaylar için bkz. Kaya (2020), s.1878.
[29] A.g.e., s.1893.

ilişkilendirilebilecek yenilikler, 108+ Sayılı Sözleşme'nin, kişisel verilerin ilgili kişilerin bilgilendirilmesi suretiyle adil ve şeffaf bir şekilde işlenmesini konu alan 8. maddesi ile *"uyumluluğun sağlanması amacıyla gerekli tedbirlerin alınması ile uyumluluğun ortaya konmasını"* konu alan 10. maddesidir. Nitekim 108+ Sayılı Sözleşme'nin 10. maddesinde bahsedilen uyumluluğun ortaya konması konsepti hesap verebilirlik için aranan 'uyum sorumluluğu ile sorumluluğun belgelendirilmesi' konseptiyle benzeşmektedir.

1.2.4. Avrupa İnsan Hakları Sözleşmesi ve AİHM

Avrupa Konseyi tarafından hazırlanan ve 3 Eylül 1953 tarihinde yürürlüğe giren insan haklarının korunmasına yönelik Avrupa İnsan Hakları Sözleşmesi ("AİHS") içerisinde ne hesap verebilirlik ilkesi ne de kişisel verilerin korunması ile ilgili düzenlemeler açıkça yer alır. Öte yandan, veri koruma hukuku temelinde kişisel veri işleme faaliyetlerinin yürütülmesi esnasında dikkate alınması gereken temel hak haklardan *"Özel hayata ve aile hayatına saygı hakkı"* AİHS'in 8. maddesinde düzenlenmiştir. AİHS ve ek protokolleri ile güvence altına alınan hakların ihlali durumunda Avrupa İnsan Hakları Mahkemesi'ne ("AİHM") başvuru yapılması mümkün olup AİHM tarafından AİHS'nin 8. maddesi temelinde verilen bir kararda[30] hesap verebilirlik ilkesi bağlamında önemli bir vurgu yapılmıştır[31].

Anılan karara göre AİHM, risk temelli bir değerlendirme yaparak kişisel verilerin korunması anlamında bir ihlalden bahsedebilmek için somut bir ihlal olması gerekmediğini ve veri ihlali riskinin varlığının ihlalden bahsedilebilmek için yeterli olduğuna değinmiştir. Başka bir ifadeyle, AİHM'e göre, olası bir ihlalin ortadan kaldırılması için yeterli ve gerekli önemlerin alınmamış olması dahi mevzuat uyum gerekliliklerinin yerine getirilmediği anlamına gelecektir. O halde

[30] Kaya (2020), s.1874; European Court of Human Rights. (17 Temmuz 2008). *Case of I v. Finland* (Application no. 20511/03) https://hudoc.echr.coe.int/eng?i=001-87510.(Erişim Tarihi: 29.05.2023)
[31] Kaya (2020), s.1874.

AİHM'in ilgili mevzuatta yer alan düzenlemelere uyumun sağlanması dışında uyumun ortaya konmasını da beklediği söylenebilecektir. Bu karar ile AİHM tarafından ilk kez hesap verebilirlik ilkesi ile ilişkilendirilebilir değerlendirilmeler yapılmıştır.

1.2.5. Asya-Pasifik Ekonomik İşbirliği

Asya-Pasifik Ekonomik İşbirliği ("APEC"), Büyük Okyanus kıyısındaki toplulukların bağlarının güçlendirilmesi ve Asya-Pasifik bölgesinde sürdürülebilir ekonomik büyüme ile refah düzeyinin artırılması amacıyla 1989 yılında 21 ülkenin katılımıyla kurulmuş olan uluslararası bir örgüttür. OECD Rehber İlkeleri'nden ilhamla oluşturulan ve 2005 yılında APEC tarafından yayımlanan APEC Mahremiyet Çerçevesi içerisinde veri sorumluları tarafından uyulması gereken dokuz temel prensibe yer verilmiştir. Bu prensiplerden biri de hesap verebilirliktir.

APEC Mahremiyet Çerçevesi'nin yürürlüğe girmesi üzerine APEC tarafından "Pathfinder" olarak adlandırılan projelere başlanarak hesap verebilirlik çerçevesinde verilerin sınır ötesi aktarımına odaklanılmıştır[32]. Pathfinder projeleri bir bakıma, kişisel verilerin APEC yetki alanındaki bölgeler arasındaki aktarımı bakımından veri ihracatçısının söz konusu aktarımları yasal düzenlemelere uygun şekilde gerçekleştirdiği yönündeki iddiasını destekleyen mekanizmalar geliştirmeyi amaçlamıştır[33]. Bu doğrultuda, APEC Sınır Ötesi Mahremiyet Kuralları Sistemi oluşturulmuş ve bu kurallar kapsamında sınır ötesi veri aktarımı gerçekleştirilmek isteyen veri sorumlusu tarafından hesap verebilirlik temsilcisi *(accountability agent)* atanması zorunlu tutulmuştur. Hesap verebilirlik ilkesinin odağı "sorumluluğun yerine getirilmesi" iken, APEC'in, Pathfinder projelerinde benimsediği yaklaşım neticesinde bu odak "sorumluluğu yerine getirme

[32] Alhadeff et al. (2011), s. 57.
[33] Greenleaf, G. (2019, Haziran). Five Years of the Apec Privacy Framework: Failure or Promise? *Computer Law & Security Report*, 25, s.32. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2022907 (Erişim Tarihi: 29.05.2023)

kapasitesinin gösterilmesi" tarafına kaymıştır[34]. APEC Mahremiyet Çerçevesi OECD Rehber İlkeleri'nden ilhamla hazırlanmış olmasına rağmen birçok yönüyle daha zayıf görülmüş[35] olsa da, uyumluluğun sağlanması için öngörüldüğü mekanizmaların esnek olması bakımından ise takdir görmüştür.

Çalışmanın bu bölümde hesap verebilirlik ilkesinin yalnızca AB hukukuna ait bir ilke olmadığına, bilakis AB hukukunun ötesinde bir yeri olduğuna değinilmiştir. Hükümetler arası örgütler veya uluslararası sivil toplum kuruluşlarınca[36] hazırlanan düzenlemelerde doğrudan zikredilsin veya zikredilmesin, hesap verebilirlik ilkesine karşılık gelen veya bu ilkeyi anımsatan tüm düzenlemeler, hesap verebilirliğin küresel boyuttaki önemini ortaya koyar. Bu bağlamda OECD, öngördüğü mahremiyet uyum programı ile hesap verebilirliği soyut bir kavram olmaktan çıkarırken, ISO tarafından hazırlanan standartlar ile hesap verebilirlik kavramı tanımlanmış ve hesap verebilirliğin sağlanması için izlenmesi gereken adımlar düzenlenerek yine bu ilke somutlaştırılmıştır. APEC OECD Rehber İlkeleri'nden alınan ilhamla hazırlanmasına rağmen bu ilkelerin üzerine birçok konuda çıkamamış, buna rağmen APEC'in dünya ekonomisinin yaklaşık %60'ını temsil eden 21 ülke tarafından kabul edilmesi dahi başlı başına hesap verebilirlik ilkesinin tanınırlığını artırmıştır. Hesap verebilirlik uluslararası etkiye sahip 108+ sayılı Sözleşme'nin lafzında olmasa bile ruhunda ele alınmış, ayrıca AİHM'in AİHS m.8 tahtında yaptığı bir değerlendirmede sonucu bu ilkeyi anımsatan bir karar verdiği görülmüştür.

[34] Alhadeff et al. (2011), s. 58.
[35] Greenleaf (2019, Haziran), s.33.
[36] Uluslararası kuruluş tanımı için bkz. Vikipedi, Özgür Ansiklopedi. Erişim için: https://tr.wikipedia.org/wiki/Uluslararas%C4%B1_kurulu%C5%9F (Erişim Tarihi: 29.05.2023). Bu kısımda anılan hükümetler arası örgütler veya uluslararası sivil toplum kuruluşlarına örnek olarak; dünya halkının ekonomik ve sosyal refahını iyileştirmeye yönelik çalışmalar yürüten OECD, insan haklarının uluslararası alanda korunması için faaliyet gösteren Avrupa Konseyi veya dünya çapında uygulanabilir standartların geliştiricisi ISO gösterilebilecektir.

1.2.6. Enron Skandalı ve Sarbanes-Oxley Yasası

Enron skandalı, enerji sektöründe faaliyet gösteren Enron isimli bir şirketin 2001 yılında Amerika Birleşik Devletleri'nde karıştığı yolsuzluk olayları neticesinde iflası ile sonuçlanan büyük bir kurumsal skandaldır. Bu skandalın bir diğer sonucuysa dünyanın en büyük beş bağımsız denetim firmalarından biri olup o dönemde Enron'a hizmet veren Arthur Andersen isimli firmanın dağılmasıdır. Enron skandalı, şirketin üst düzey yöneticileri tarafından finansal tabloların manipüle edilerek ve karlılık görüntüsü yaratılarak şirketin gerçek zarar ve borçlarının gerçeği yansıtmayan raporlar dâhil çeşitli yöntemlerle saklanması nedeniyle ortaya çıkmıştır. Şirketin üst düzey yöneticileri ile çalışanlarının faaliyetlerini şeffaf bir şekilde raporlamadığı ve yapılan raporlamaları doğrulamak için hesap verme sorumluluğunu üstlenmediklerini göstermiş olup bu skandal dolayısıyla kurumsal yönetim ilkelerine ve özellikle hesap verebilirlik ilkesine olan ihtiyaç doğmuştur.

Enron skandalı ve benzer muhasebe ve denetim skandalların ardından Amerika Birleşik Devletleri hükümeti ve düzenleyici kurumlar tarafından benzer usulsüzlüklerin yaşanmasını önlemek amacıyla alınan düzenleyici önemler çerçevesinde, Sarbanes-Oxley Act olarak da bilinen Sarbanes-Oxley Yasası kabul edilerek 2002 yılında yürürlüğe girmiştir. Bu yasa, şirketlerin finansal raporlama ve hesap verebilirlik süreçlerini düzenleyerek finansal sorumluluklarını artırmayı, şeffaflığı sağlamayı ve yatırımcıların güvenini yeniden tesis etmeyi amaçlamaktadır. Ayrıca Sarbanes-Oxley Yasası ile şirketlerin iç kontrol sistemlerinin güçlendirilmesi, bağımsız denetimlere tabi olması, eksik veya yanlış finansal beyan veya raporlamaların önüne geçilmesi amacıyla üst düzey yöneticilerin sorumluluğunun artırılması hedeflenmiştir. Bu yasanın 11 ana başlığından birinin "Kurumsal Yolsuzluk ve Hesap Verebilirlik" olması da hesap verebilirlik ilkesine atfedilen önemi ortaya koymaktadır.

Sarbanes-Oxley Yasası'nın yürürlüğe girdiği dönemde yürürlükte olan 95/46 sayılı Direktif'te hesap verebilirlik ilkesi bulunmasa da Amerika Birleşik Devletleri'nde büyük yankı uyandıran bu yasanın, hesap verebilirlik ilkesinin AB düzenlemelerinde kendisine yer bulmasına ön ayak olduğu söylenebilecektir.

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİ HUKUKUNDA HESAP VEREBİLİRLİK

AB hukukunun yazılı kaynakları; **(i)** birincil hukuk kaynakları **(ii)** AB üyesi olmayan ülkelerle veya uluslararası kuruluşlarla yapılan uluslararası anlaşmalar ve **(iii)** ikincil hukuk kaynaklarından oluşur. Yazılı olmayan kaynaklar ise uluslararası teamül hukuku ve AB hukukunun genel ilkeleri olarak özetlenebilir, ancak bunlar çalışmanın konusunu oluşturmadığından incelenmeyecektir. Buna karşılık, yazılı kaynakların incelenmesi, çalışmanın temelini oluşturan davranış kuralları ve sertifikasyon mekanizmalarının kolay anlaşılması bakımından faydalı olacaktır. Bu doğrultuda gerçekleştirilecek incelemenin konusunu AB hukukundaki tüm yazılı kaynakları yerine bilişim ve teknoloji hukukunu[37] ilgilendiren kaynaklar oluşturacaktır.

Yazılı kaynakların hiyerarşi piramidindeki yerleri yukarıdan aşağıya doğru "birincil hukuk kaynakları" – "uluslararası anlaşmalar" – "ikincil hukuk kaynakları" şeklindedir. Bu piramidin ortasında yer alan uluslararası anlaşmalar, birincil ve ikincil hukuk kaynaklarından niteliği itibariyle farklı olup başlı başına bir kategori oluşturmaktadır.

Piramidin en üstünde yer alan birincil hukuk kaynakları AB'nin kurucu anlaşmaları ile protokolleri iken, ikincil hukuk kaynakları ise AB'nin yasama yetkileri veya yasama dışı yetkilerinin kullanılması sonucu kabul edilen düzenlemelerdir. Direktif, tüzük veya kararlar, yasama usulü ile kabul edilen hukuki tasarruflardandır. Bunların dışında, AB hukukunun ikincil kaynakları arasında *"yetki devrine dayanan tasarruf (delegated acts)"* ve *"uygulama tasarrufu (implementing acts)"* olarak adlandırılan yasama dışı tasarruflar[38]

[37] Bilişim ve teknoloji hukukunun kapsam ve metodolojisi ile ilgili bilgi için bkz. https://mbkaya.com/bilisim-ve-teknoloji-hukuku/. (Erişim Tarihi: 29.05.2023)

[38] "Yetki devrine dayanan tasarruflar" ile "uygulama tasarrufları" ayrı kavramlar olup farklı amaçlara hizmet ederler. Yetki devrine dayanan tasarruf, AB tarafından Avrupa Komisyonu'na

bulunmaktadır. Piramidin son basamağını oluşturan ikincil kaynakların da kendi arasında bir hiyerarşisi olup yasama tasarrufları diğer iki tür tasarrufun üstündedir.

2.1. AB BİLİŞİM VE TEKNOLOJİ HUKUKUNDA HESAP VEREBİLİRLİK

Bilişim ve teknoloji hukukunun siber güvenlikten bilişim suçlarına, elektronik ticaret hukukundan veri analitiğine ve bunun gibi daha nice alana uzanan oldukça kapsayıcı bir hukuktur. Kişisel verilerin korunması hukuku da bilişim ve teknoloji hukukunun ilgilendiği alanlardan biridir.

Bu çalışma kişisel veri koruma hukuku temelinde yapılacağından, AB veri koruma mevzuatında yer alan hesap verebilirlik ilkesi ile ilgili düzenlemeler incelenmeden evvel AB'nin bilişim ve teknoloji alanındaki diğer ilgili düzenlemelerine kısaca değinmekte fayda vardır. Bu doğrultuda, hesap verebilirlik ilkesinin muhtelif AB düzenlemelerindeki yeri aşağıda kısaca ve bu bölüm ile sınırlı olmak kaydıyla açıklanacaktır.

2.1.1. Avrupa Birliği Yapay Zekâ Stratejisi ve Taslak Yapay Zekâ Yasası

Bilişim ve teknoloji hukuku kapsamında ilk olarak, yapay zekâyı temel alan AB düzenlemelerinden AB Yapay Zekâ Stratejisi kapsamında hesap verebilirlik ilkesine değinildiği görülür. Ardından 21 Nisan 2021 tarihinde Komisyon tarafından yayımlanan ve AB sınırları içinde yapay zekâ odaklı ürün, hizmet ve sistemler ile ilgili olan Yapay Zekâ Yasası *(European Union Draft Artificial Intelligence Act)* hakkındaki yasama teklifi[39] kapsamında bu ilkenin zikredildiği

devredilen yetkiye dayanılarak yasama tasarruflarının asli olmayan kısımlarının tamamlanması veya değiştirilmesi iken; uygulama tasarrufu ise Birlik tasarruflarının AB genelinde yeknesak uygulanması için Komisyon veya çok sınırlı hallerde Avrupa Konseyi tarafından kurallar getirilmesini ifade eder. Detaylı bilgi için: Council of the European Union. (n.d.). Implementing and delegated acts. https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_en (Erişim Tarihi: 29.05.2023)

[39] Bu çalışmanın hazırlandığı esnada bu teklif AB Konseyi tarafından onaylanmamış olup onaylanması halinde Yapay Zekâ Yasası tüm üye ülkelerde yürürlüğe girecektir.

görülür. Teklife konu edilen Yapay Zekâ Yasası ile hesap verebilirlik kavramı da ele alınmıştır. Yüksek riskli yapay zekâ sistemlerinin sağlayıcıları özelinde getirilen birtakım ek yükümlülükler ile anılan sağlayıcılara mevzuata uyumun dışında, bunların değerlendirmesi için bir kalite yönetim sistemini uygulamaya koymaları gerekmektedir. Sistematik şekilde belgelendirilmesi gereken bu kalite yönetim sisteminin asgari olarak içermesi gereken hususları düzenleyen 17. maddenin ilgili m bendinde ise: *"Bu maddede belirtilen tüm unsurlarla ilgili olarak yönetimin ve diğer davranışların sorumluluklarını yerine getirmek için bir hesap verebilirlik çerçevesi."* denilmektedir.

2.1.2. Dijital Hizmetler Yasası

AB dijital kurallarının bir parçası olan ve çevrimiçi platformlar bakımından düzenlemeler getiren Dijital Hizmetler Yasası *(Digital Services Act)* 27 Ekim 2022 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayınlanmıştır. Bu yasanın beslendiği ilkeye göre, çevrimdışında yasa dışı olan çevrimiçi ortamda da yasa dışı sayılmalıdır[40].

Dijital Hizmetler Yasası ile ulaşılmak istenen temel amaç; çevrimiçi platformlar aracılığıyla elde edilen veya kullanılan verilerin güvenliğinin sağlanarak tüketicilerin temel haklarının korunmasıdır. Bu bağlamda Dijital Hizmetler Yasası çevrimiçi hizmet sağlayıcılar için şeffaflık ve hesap verebilirlik çerçevesi çizmektedir.

Dijital Hizmetler Yasası ile bu konularda getirilen düzenlemeler, çevrimiçi hizmet sağlayıcıların dijital alandaki içerik denetleme uygulamalarından sorumlu tutulmalarını gerekli kılar. Bu kapsamda çevrimiçi hizmet sağlayıcıların içerik

[40] Council of the European Union. (25 Kasım 2021). "What is illegal offline should be illegal online": Council agrees on position on the Digital Services Act. https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/ (Erişim Tarihi: 29.05.2023)

denetimi, veri paylaşımı ve yayından kaldırma süreçleriyle ilgili kurallar, reklamcılık uygulamaları ile içerik sıralama/önerisini etkileyen algoritmalar hakkındaki bilgileri tüketiciler ile paylaşma gibi sorumlulukları vardır.

2.1.3. Dijital Operasyonel Dayanıklılık Yasası

Aralık 2022'de Avrupa Birliği Resmi Gazetesi'nde yayımlanarak AB siber güvenlik mevzuatının bir parçası haline gelen Dijital Operasyonel Dayanıklılık Yasası *(Digital Operational Resilience Act – DORA)*, finansal hizmetler sektörü için birtakım düzenlemeler getirir. Bu yasa ile amaçlanan, finansal kuruluşların dijital operasyonel dayanıklılık ve siber güvenliğin sağlanması, yani firmaların siber saldırılara karşı direnmesine yardımcı olunmasıdır. Dijital dayanıklılığın tüm seviyelerinde sağlaması için getirilen bu yasa kapsamında; bilgi ve iletişim teknolojileri ("BİT") risk yönetimi, BİT ile ilgili olay raporlama, dijital operasyonel dayanıklılık testi ve BİT üçüncü taraf risk yönetimi konularında kurallar öngörülmüştür.

BİT üçüncü taraf risk yönetimi kapsamında, finansal kuruluşların BİT üçüncü taraf hizmet sağlayıcıları ile akdedeceği sözleşmeler bakımından bazı gereklilikler ile kritik BİT üçüncü taraf hizmet sağlayıcıları gözetimine ilişkin kurallar öngörülmekte, ayrıca finansal kuruluşların şeffaf bir BİT üçüncü taraf risk yönetimi strateji yürütmeleri beklenmektedir. Bu yönüyle Dijital Operasyonel Dayanıklılık Yasası kapsamında hesap verebilirlik ilkesine yer verildiği söylenebilecektir.

2.1.4. Avrupa Birliği Adalet Divanı Kararları

GVK Tüzüğü'nün Avrupa Birliği Adalet Divanı ("ABAD") önünde zaman zaman ihtilaflara konu olduğu, hatta GVK Tüzüğü ile getirilen hesap verebilirlik ilkesinin de ABAD tarafından yapılan değerlendirmeler kapsamında tartışıldığı

görülmektedir[41]. Bu doğrultuda, C-61/19 referanslı davada ABAD Hukuk Sözcüsü Szupunar tarafından sunulan görüş kapsamında; ilgili kişinin açık rızaya dayalı olarak kişisel veri işlendiği hallerde ilgili kişilerin kişisel verilerinin işlenmesine rıza gösterdiğinin ispatı bakımından veri sorumlusunun yükümlü olduğu belirtilerek hesap verebilirlik ilkesine atıfta bulunulduğu görülür[42].

Yine C-129/21 referanslı dava hesap verebilirlik ilkesinden bahsedilmektedir. C-129/21 referanslı dava, bir telekomünikasyon operatörü tarafından abonelerinin kişisel verilerinin ilgili dizin sağlayıcıya iletilmesi için rızasının alınması sonucu aktarılması ve ilgili dizin sağlayıcı tarafından kendisine aktarılan bu verilerin aynı rıza temelinde diğer dizin sağlayıcılara iletilmesiyle ilgilidir. Yapılan değerlendirmeler neticesinde ABAD'ın, ABAD Hukuk Sözcüsü Collins tarafından ilgili dava kapsamında sunulan görüşe[43] paralel karar verdiği görülmektedir.

ABAD tarafından verilen karar kapsamında; (mevcut davada olduğu gibi) birden fazla veri sorumlusunun kişisel verilerin aynı amaçla işlenmesi için ilgili kişinden alınan tek bir rızaya dayandığı durumlarda, bu rızaya dayanarak veri işleyen tüm veri sorumlularına -imkânsız olmadığı veya orantısız bir çaba gerektirmediği sürece- rızanın geri çekildiğine ilişkin bildirimde bulunulması gerektiği, bu bildirim yükümlülüğünün GVK Tüzüğü m.24 kapsamındaki uygun güvenlik tedbirlerinden sayılacağı değerlendirilmiştir. Bu sebeple ABAD'ın verdiği karara göre; GVK Tüzüğü'nün 5(2) ve 24. maddeleri, ilgili veri koruma

[41] Kaya (2020), s. 1883.
[42] Court of Justice of the European Union (4 Mart 2020). Case C-61/19. Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal. Opinion of Advocate General Szpunar. https://curia.europa.eu/juris/document/document.jsf?text=accountability&docid=224083&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=10154021#ctx1 (Erişim Tarihi: 29.05.2023)
[43] Court of Justice of the European Union (28 Nisan 2022). Case C-129/21. Proximus NV (Public electronic directories) v Gegevensbeschermingsautoriteit. Opinion of Advocate General Collins. https://curia.europa.eu/juris/document/document.jsf?text=accountability&docid=258506&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=10154021#ctx1 (Erişim Tarihi: 29.05.2023)

otoritesi tarafından rızanın geri çekilmesi hakkında diğer dizin sağlayıcıların bilgilendirmesi ile ilgili olarak ilgili dizin sağlayıcıdan uygun teknik ve idari tedbirleri almasını talep edilebileceği şeklinde yorumlanmalıdır.

Schrems II olarak adlandırılan ve veri koruma alanında büyük bir yankı uyandıran dava[44] ise, İrlanda Yüksek Mahkemesi tarafından ABAD'dan AB dışında veri aktarımına imkân veren standart sözleşme maddelerinin *(standart contractual clauses – SCC)* geçerliliği konusunda görüş talep edilmesi[45] üzerine görülmeye başlanmıştır. Yapılan değerlendirmeler neticesinde ABAD 16 Temmuz 2020 tarihinde kararını yayımlamış olup verilen karara göre, AB'de yerleşik veri aktaran ile üçüncü ülkede yerleşik veri alıcısı arasındaki transferler bakımından standart sözleşme maddeleri dikkate alınacaktır. Ayrıca, Schrems II kararı akabinde, standart sözleşme maddelerine dayalı gerçekleştirilecek aktarımlarda "transfer etki analizi" yükümlülüğü getirilmiştir. Yapılacak etki analizi verileri aktaran tarafa, aktarımın gerçekleştirileceği ülkedeki hukuki ve fiili durumu araştırma sorumluluğu yükler. Bu uygulama ilgili risklerin tespiti ve tespit edilen riskler bağlamında gerekli önemlerin alınmasını sağladığından, hesap verebilirlik açısından önemlidir[46].

4 Mayıs 2023 tarihinde ABAD'ın yayımladığı kişisel verilerin korunması ile ilgili bir diğer kararında, GVK Tüzüğü düzenlenmelerinin yorumlanması bakımından oldukça önemli değerlendirmeler yapılmıştır. Öyle ki, bunlardan bir tanesi özellikle hesap verebilirlik ilkesine odaklanmaktadır. Almanya Federal Cumhuriyeti ile UZ arasındaki esas dava bakımından yetkili Alman İdari Mahkemesi tarafından ABAD'a yapılan ön karar talepli başvuru üzerine, C-60/22

[44] Court of Justice of the European Union (16 Temmuz 2020). Case C-311/18 Facebook Ireland Ltd v Maximillian Schrems. Judgment of The Court (Grand Chamber. https://curia.europa.eu/juris/document/document.jsf;jsessionid=920F8236EAD65FFA7730C23834493B78?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2052319 (Erişim Tarihi: 29.05.2023)

[45] Dülger, M. V., & Gümüş, G. (17 Haziran 2021). *Scherms II Kararı ve Sonuçları (Scherms II Decision and Results)*, s.42. https://ssrn.com/abstract=3869038 (Erişim Tarihi: 29.05.2023)

[46] Çekin, M. S., Berktaş, A. E., & Akıncı, M. F. (2023). *Veri Hukuku,* s.226. On İki Levha Yayıncılık.

referanslı dava[47] ABAD'ın 5. Dairesi tarafından görülmeye başlanmıştır. Bu dava kapsamında Alman İdari Mahkemesi tarafından ABAD'a üç ayrı soru yöneltilmiştir. Hukuk Sözcüsü tarafından herhangi bir görüş verilmeyen ve ABAD tarafından ilgili soruların yanıtlanmasıyla hükme bağlanan dava kapsamında yanıt aranan sorulardan biri; "*veri sorumlusu tarafından GVK Tüzüğü'nün 26. ve 30 maddelerinin ihlal edilmiş olmasının, GVK Tüzüğü'nün 17(1)(d) maddesi ile 18(1)(b) maddesindeki anlamıyla 'hukuka aykırı veri işleme' kabul edilip edilmeyeceği"*dir. ABAD bu konuyu iki ayrı senaryo üzerinden kurgulayarak değerlendirmiş ve senaryolarında GVK Tüzüğü'nün 26 ve 30. maddelerinin ihlalini ele almıştır.

ABAD'a göre, hesap verebilirlik gerekliliklerinden olan ve GVK Tüzüğü'nün 26. ve 30 maddelerinde düzenlenen 'ortak veri sorumlusu ile sözleşme imzalanması' veya 'veri işleme faaliyetlerinin kayıtlarının tutulması" gerekliliklerinin veri sorumlusu tarafından ihlal edilmiş olması, söz konusu işleme faaliyetlerinin hukuka aykırı olduğunu söylemek için tek başına yeterli değildir. Bu bağlamda ABAD, veri sorumlusu tarafından 26 ve 30. maddelerinde öngörülen gerekliliklerin yerine getirilmemesi dolayısıyla veri işleme faaliyetlerinin hukuka aykırılığından bahsedebilmek için GVK Tüzüğü'nün genel ilkelerden 'yasallık, adillik ve şeffaflık' ile ilgili 5(1)(a) ve hukuka uygun veri işleme şartlarını düzenleyen 6(1) maddeleriyle birlikte değerlendirme yapılması gerekir. Başka bir deyişle, GVK Tüzüğü'nün hesap verebilirlik ilkesini düzenleyen 5(2) maddesi ile 5(1)(a) ve 6(1) maddeleri birlikte değerlendirildiğinde hesap verebilirlik ilkesinin ihlalin anlamına geliyor ise hukuka aykırı bir veri işlemeden bahsedilebilecektir.

[47] Court of Justice of the European Union (4 Mayıs 2023). Case C-60/22. UZ v Bundesrepublik Deutschland. Judgment of The Court (Fifth Chamber). https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3395552 (Erişim Tarihi: 29.05.2023)

2.1.5. Şebeke ve Bilgi Güvenliği Direktifi

Temmuz 2016'da, AB siber güvenlik mevzuatının ilk parçası olan Şebeke ve Bilgi Güvenliği Direktifi ("NIS 1") kabul edilmiştir. Daha sonra bu direktifin kapsamı genişletilmiş ve 14 Aralık 2022 tarihinde "NIS 2" olarak anılan düzenlemeler yürürlüğe girmiştir. NIS 1 veya NIS 2'ye bakıldığında, yukarıda yer verilen AB yasal düzlemindeki diğer düzenlemelerden farklı olarak hesap verebilirlik kavramının doğrudan zikredilmediği görülür. Buna karşın, NIS Direktifi, tıpkı GVK Tüzüğü gibi veri sorumluları ve veri işleyenlere teknik ve organizasyonel önlemler alma bakımından sorumluluk yüklemektedir.

2.2. AB VERİ KORUMA HUKUKUNDA HESAP VEREBİLİRLİK

2.2.1. Madde 29 Çalışma Grubu Hesap Verebilirlik Raporu

GVK Tüzüğü'nün 68. maddesi çerçevesinde günümüzde Avrupa Veri Koruma Kurulu ("EDPB") olarak adlandırılan organ kurulmadan ve GVK Tüzüğü yürürlüğe girmeden önce yürürlükte olan 95/46 sayılı Direktif'in 29. maddesi ile bir çalışma grubu kurulmuştu. Madde 29 Çalışma Grubu ("WP 29") olarak anılan bu çalışma grubu, EDPB 25 May 2018 tarihi itibariyle resmen WP 29'un yerine geçmeden önce, 95/46 sayılı Direktif'in 29. maddesi ile direktifin nasıl uygulanacağına ilişkin yol gösterici raporlar yayımlamaktan sorumluydu.

13 Temmuz 2010 tarihinde WP 29 tarafından hesap verebilirlik ilkesi üzerine bir görüş[48] yayımlanmış olup hesap verebilirlik ilkesi bakımından atılan bu adım, o dönemde yürürlükte olan 95/46 sayılı Direktif'te yer almayan bu ilkenin GVK Tüzüğü'nde düzenlenmesine öncülük etmiştir.

[48] Madde 29 Çalışma Grubu (2010).

WP 29 tarafından yayımlanan ilgili görüşte, hâlihazırda yürürlükte olan veri koruma düzenlemelerinin efektif bir biçimde uygulanması bakımından eksiklikler olduğu değerlendirilmiştir. Ayrıca WP 29'a göre bu eksikliklerin sebebi yürürlükteki veri koruma düzenlemelerinin bilgi teknolojilerindeki hızlı gelişmelere ayak uyduramaması ve kişisel veri işleme faaliyetlerin gün geçtikçe fazlalaşmasıyla birlikte veri işleme faaliyetlerinin güvenli şekilde sürdürülebilmesi bakımından mevcut yasal düzenlemelerin yeterli teminatı sağlamamasıydı. Bu sebeplerle WP 29, Avrupa Komisyonu'na ("Komisyon") hesap verebilirlik odaklı bir mekanizma kurgulanmasını önermiştir[49]. Bu öneri çerçevesinde, kişisel verileri koruma mevzuatına uyum sağlanması yükümlülüğüne ilave olarak, uyum sağlandığının ispat edilebilmesi için veri sorumluları tarafından birtakım mekanizmalar kurgulanması gündeme gelmiştir[50].

WP 29 tarafından hesap verebilirlik kavramı bakımından detaylı bir tanım yapılmasa da genel hatlarıyla "*sorumluluğun ne şekilde yerine getirildiğin gösterilmesi ve bu durumun ispatlanması*"[51] şeklinde bir tanımlamaya gidildiği görülmektedir. Yani WP 29'a göre, sorumluluk ve hesap verebilirlik kavramları birbirinden ayrı düşünülemeyecek ve birbirini tamamlayacaktır. Başka bir ifadeyle, WP 29'a göre hesap verebilirlik ilkesi, veri koruma mevzuatında yer alan prensiplere bir ilave niteliğinde olmayıp söz konusu ilkelerin uygulayıcısı, bir nevi bütünleyicisi, niteliğindedir[52]. O halde hesap verebilirlik kavramının özünü oluşturan iki elementten biri veri sorumlularının yasal yükümlülükleri iken, diğeri ise bu yükümlülüklerin yerine getirildiğinin ilgili taraflara veya makamlara ispatını sağlayan mekanizmalardır.

[49] Madde 29 Çalışma Grubu (2010), s.3-5.
[50] Hal böyle olunca, 95/46 sayılı Direktif'te reform yapılması ihtiyacı doğmuştur.
[51] A.g.e., s.7.
[52] A.g.e., s.10.

Hesap verebilirlik ilkesine yasal düzenlemelerde yer verilmesi ile hedeflenenin; *kişisel verilerin korunması bakımından mevcut olan temel prensipler bakımından bir değişiklik yaratılmasından ziyade, yürürlükte olan düzenlemelerin daha efektif bir şekilde uygulanması*[53] olduğu belirtilmiştir[54].

Hesap verebilirlik ilkesinin tamamlayıcı doğasından hareketle, hesap verebilirlik mekanizmalarının kurgulanması ile birlikte kişisel veri işleme faaliyeti yürüten tarafların sorumluluğunun sona ermediği, ancak bu mekanizmaların varlığının *"yetkili veri koruma otoriteleri*[55] *tarafından olası bir uyum değerlendirmesine dikkate alınacak bir ölçüt olduğu"*[56] söylenmektedir. Daha önemlisi, hesap verebilirliğin, yetkili veri koruma otoritelerinin mevcut yetkilerine zeval getirmeksizin, söz konusu otoriteler tarafından yürürlükte olan genel veri koruma prensiplerinin uygulanması konusunda daha etkin denetim süreçleri yürütülmesine sebep olacağı değerlendirilmektedir[57]. Ayrıca WP 29'a göre, hesap verebilirlik mekanizmaları hem kamu hem de özel sektörler açısından önemlidir

[53] WP29 tarafından bir önceki yıl yayımlanan çalışma raporunun aksine açıklamalar içerdiği görülmektedir. Bkz. Madde 29 Çalışma Grubu. (1 Aralık 2009). *The Future of Privacy*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf (Erişim Tarihi: 29.05.2023)

[54] Madde 29 Çalışma Grubu (2010), s.5.

[55] GVK Tüzüğü m.4'te yer alan tanıma göre "supervisory authority"; AB üyesi devletlerden biri tarafından GVK Tüzüğü'nün 51. maddesi uyarınca kurulan ve bağımsız niteliği haiz kamu kuruluşuna karşılık gelmektedir. GVK Tüzüğü'nün resmi Türkçe çevirisi yayımlanmamış olmakla birlikte, açık internet kaynakları incelendiğinde Avrupa Birliği Başkanlığı tarafından iletildiği belirtilen gayri resmi bir Türkçe tercüme dokümanına rastlanmaktadır. (İlgili açık internet kaynakları için bkz. Kişisel Verilerin Korunması. (n.d.). Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Türkçe Çeviri. https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri/; Legal Bülten. (2021, Ocak). GDPR Türkçe Çeviri - Tercüme. https://legalbulten.com/2021/01/gdpr-turkce-ceviri-tercume/) Her ne kadar bu gayri resmî tercüme dokümanı içerisinde "supervisory authority" ifadesi "denetim makamı" olarak çevrilmişse de, Türk hukukundaki kavramları da göz önünde bulundurarak "supervisory authority" olarak tanımlanan kuruluş -aksi gerekli görülmediği takdirde- çalışmanın devamında "yetkili veri koruma otoritesi" olarak anılacaktır. Bu kavramların örtüştüğü yönündeki doktrin görüşü için: Leenes, R. (2020). Article 42 certification. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation: A Commentary* (s. 732-743). Oxford, UK: Oxford University Press, s.735. Ayrıca, veri koruma otoritesinin sahip olduğu süpervize yetkisi dolayısıyla "supervisory authority" olarak anıldığına dair Avrupa Komisyonu tarafından yapılan açıklamaya erişim için: https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (Erişim Tarihi: 29.05.2023).

[56] Madde 29 Çalışma Grubu (2010), s.11.

[57] Ag.e., s.16.

zira bahsi geçen teknolojik gelişmeler sonucu ortaya çıkması muhtemel veri ihlallerinin çok daha ciddi sonuçları ve sektör fark etmeksizin bu ihlallerin ekonomik yansımaları olabilir[58].

WP 29'un yayımladığı hesap verebilirlik araçlarına ilişkin listede[59] hesap verebilirlik araçları sınırlı sayıda (tahdidi) olmayacak şekilde örneklenmiş, devam eden bölümlerde ise veri sorumluları tarafından işlenen kişisel verilerin niteliği ve veri işleme şartlarına göre doğabilecek risklerin farklılaşabilecek olması gerekçesiyle, hesap verebilirlikten bahsedebilmek için ilgili mevzuata uyumluluğun ispatının "özel yapım *(custom built)*" olması gerektiği vurgulanmıştır. Bu sayede, birbirinden farklı sektörlerde faaliyet gösteren ve veri işleme süreçleri nitel ve nicel anlamlarda farklılaşan tüm veri sorumluları bakımından tek bir çerçeve çizilmeyecek ve dolayısıyla nihayetinde başarısızlıkla sonuçlanması muhtemel yükümlülükler öngörülmemiş olacaktır[60].

WP 29'a göre hesap verebilirlik ilkesi, ilgili mevzuat gereği tabi olunan yasal yükümlülüklerin ispatı ile sınırlı olmayabilir. Başka bir deyişle, veri sorumlularının tamamı bakımından geçerli olan hukuki yükümlülükler (prosedürlerin uygulanması ve delil muhafazası gibi[61]) bakımından hesap verebilir olma ilk kademe iken, "minimum yasal gereklilikleri aşmak suretiyle gönüllük esasına göre uygulanan ilave güvenceler (sertifikasyon gibi[62])" ikinci kademe olarak düşünülebilecektir. Bu husus, hesap verebilirlik ile gönüllülük esasına arasındaki ilişkinin inceleneceği bölümde detaylıca ele alınacaktır.

[58] Madde 29 Çalışma Grubu (2010), s.5.
[59] Madde 29 Çalışma Grubu'nun hazırlamış olduğu tahdidi olmayan, dolayısıyla hesap verebilirlik araçlarına ilişkin örnekleri içeren listeyi incelemek için bkz. Ag.e., s.11-12, p.41.
[60] A.g.e., s.13.
[61] Kaya (2020), s.1879.
[62] Madde 29 Çalışma Grubu gönüllü hesap verebilirlik aracı olan sertifikasyon uygulamalarına önem atfederek, bu uygulamalara ilişkin özel yasal düzenlemeler getirilmesi gereğinden bahsetmiştir. Detaylı bilgi için bkz. Madde 29 Çalışma Grubu (2010), s.17 vd.

Özetle; WP 29 görüşü kapsamında hesap verebilirlik ilkesi, başta terminolojik, içeriksel ve fonksiyonel olmak üzere birçok farklı anlamda incelenmiş olup bu sayede hesap verebilirlik kavramının GVK Tüzüğü içerisinde açıkça zikredilmesine öncülük edilmiştir.

2.2.2. Avrupa Birliği Genel Veri Koruma Tüzüğü

Bilgi ve iletişim teknolojilerinde yaşanan gelişme ve değişimler sebebiyle veri sorumluları tarafından işlenen kişisel verilerin hacmi ve çeşitliliği arttığı gibi, verilerin dolaşımı da giderek artmaktadır. Dijitalleşmenin artmasıyla birlikte 95/46 sayılı Direktif'teki düzenlemelerin dönemin ihtiyaçları karşılamadığı, veri koruma mevzuatına uyumun ortaya konabilmesi adına ilave mekanizmalara ihtiyaç duyulduğu anlaşılmıştır. Bunun sonucunda ortaya çıkan "hesap verebilirlik" kavramı, paydaşların daha hızlı ve etkin şekilde denetlenmesinin sağlanması için ortaya konulan yeni bir yaklaşımın ürünüdür[63].

Hesap verebilirlik, AB'nin 95/46 sayılı Direktif'inde yer almayan ve WP 29'un öneri üzerine ilk kez GVK Tüzüğü'nde yer verilerek veri koruma hukukuna normatif anlamda kazandırılan bir ilkedir. Bu ilke, kişisel verilerin korunması mevzuatına uyumun sağlanması ve böylece ilgili yasal düzenlemelere aykırılığın giderilmesi adına veri sorumluları ve/veya veri işleyenlere daha önceden sahip olmadıkları bir sorumluluk yüklemektedir. Böylece veri sorumlusu ve/veya veri işleyenlerin yetkili veri koruma otoriteleri nezdinde hesap verebilir hale gelmiş ve doğrudan devlet yoluyla yapılan bir denetleme olmaksızın işletilebilir bir mekanizma kurgulanmıştır[64].

Hesap verebilir durumda olma, kişisel veri işleme faaliyetlerinin ilgili mevzuatına uygun olarak yürütüldüğü yönünde bir karine teşkil etmesi açısından da önemli bir rol oynamaktadır. Bu ilke sayesinde GVK Tüzüğü'ne uyum

[63] Alhadeff et al. (2011), s.65; Kaya (2020), s.1893.
[64] Kaya (2020), s.1881.

sağlanması ve mevzuata uyumun belgelenebilir hale gelmesi temin edilmiş olup uyumun varlığı bakımından ispat yükü veri sorumlusu üzerindedir[65]. Ayrıca bu yeni ilkeyle, reaktif bir yaklaşımdan proaktif bir yaklaşıma geçilmiştir[66].

Normatif anlamda ilk kez GVK Tüzüğü'nde düzenlenen "hesap verebilirlik" ilkesi, kişisel verilerin korunması hukuku ilkelerinden biridir. GVK Tüzüğü'nün 5. maddesinin ilk fıkrasında, kişisel verilerin işlenmesine ilişkin ilkeler sırasıyla, *'hukukilik, dürüstlük ve şeffaflık ilkesi', 'amaçla sınırlılık ilkesi', 'veri minimizasyonu ilkesi', 'doğruluk ilkesi', 'saklama süresinin sınırlandırılması ilkesi'* ve *'bütünlük ve gizlilik ilkesi'* olarak sayılırken, aynı maddenin 2. fıkrasında *"Veri sorumlusu, 1. fıkraya uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir."* denilerek hesap verebilirlik ilkesi ile 1. fıkrada sayılan ilkeler arasında bir bağlantı kurulmuştur. GVK Tüzüğü'nün 5(2) maddesinde hareketle hesap verebilirlik ilkesinin iki kriterden oluştuğu söylenebilir. Bunlardan ilki; "veri sorumlusu sıfatıyla hareket eden tarafın sorumlu olması" iken, bir diğer ise "veri sorumlusu tarafından ilgili mevzuatta kaynaklanan yükümlülüklerinin yeri getirildiğinin ortaya konması" olarak karşımıza çıkmaktadır.

2.2.2.1. Hesap Verebilirlik İlkesini Somutlaştıran GVK Tüzüğü Düzenlemeleri

Hesap verebilirlik ilkesinin açıkça zikredildiği maddeler GVK Tüzüğü'nün 5. maddesi ve Resital 85 ile sınırlı olmakla birlikte, bu ilkenin, GVK Tüzüğü'nün veri sorumlularının yükümlülüklerini düzenleyen 24. maddesi ile somut bir uygulama alanı kazandığı görülmektedir.

Madde 24(1) uyarınca, veri sorumlusu tarafından işleme faaliyetlerinin GVK Tüzüğü'ne uygun bir şekilde gerçekleştirilmesi ve bu şekilde gerçekleştirildiğinin

[65] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide (1st ed.). Cham: Springer International Publishing. s,31.
[66] Alhadeff et al. (2011),

gösterilebilmesi için uygun teknik ve idari tedbirlerin alınması, bu tedbirlerin gözden geçirilmesi ve gerektiğinde güncellenmesi gerekmektedir.

GVK Tüzüğü'nün hesap verebilirlik ilkesini düzenleyen 5. maddesi ile bu kavramı genel bir çerçeve çizerek somutlaştıran 24 maddesi dışında, bu ilkeye hizmet eden başkaca düzenlemeler de vardır. Bu bağlamda GVK Tüzüğü'nün 24 (1) maddesinde anılan teknik ve idari tedbirlere, GVK Tüzüğü'nün aşağıdaki sayılan maddeleri (tahdidi olmamak kaydıyla) örnek gösterilebilecektir:

a) Veri koruma politikalarının benimsenmesi ve uygulanması (GVK Tüzüğü, m. 24(2) ve Resital 78)

b) "Data protection by design and by default *(tasarımla ve varsayılan ayarlarla veri koruma)*[67]" yaklaşımının benimsenmesi (GVK Tüzüğü, m. 25 ve Resital 78)

c) Alt veri işleyenler dâhil olmak üzere veri işleyen kuruluşlar ile veri sorumlusu arasında yazılı sözleşmeler imzalanması (GVK Tüzüğü, m. 28 ve Resital 81)

d) Veri işleme faaliyetlerinin kayıt altına alınması (GVK Tüzüğü, m.7(1), 30, 33(5) ve Resital 42, 82)

e) Verilerin korunması bakımından uygun güvenlik önlemlerinin alınması (GVK Tüzüğü, m. 24(1), 32 ve Resital 39, 83)

f) Verilerin üçüncü ülkelere aktarılması bakımından uygun güvenlik önlemlerinin alınması (GVK Tüzüğü, m. 46(2) ve Resital 108, 109)

g) Veri ihlallerinin kayıt altına alınması ve yetkili makama bildirilmesi (GVK Tüzüğü, m. 33, 34 ve Resital 85-88)

h) Gerekli hallerde veri koruma etki değerlendirmesi (DPIA) yapılması (GVK Tüzüğü, m.35, 36 ve Resital 84, 89-95)

[67] Anılan kavram ile ilgili detaylı bilgi için: Noain-Sánchez, A. (2016). 2016. "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. *Journal of Information, Communication and Ethics in Society,* 14**,** s.124-138; Cavoukian, A. (2010). Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D. *Identity in the Information Society*, 3, s.247-251.

i) Gerekli hallerde veri koruma görevlisi atanması (GVK Tüzüğü, m. 37-39 ve Resital 97)

GVK Tüzüğü'nün atıfta bulunulan ilgili maddeleri ışığında, hesap verebilirliğin sağlanması için veri sorumluları tarafında kişisel verilerin ne amaçla elde edildiği, kişisel verilerden hangilerinin, ne şekilde ve hangi amaçlarla işlendiği, işlenen bu verilerin ne kadar süreyle işlenmeye devam edildiği, kişisel verilerin güvenliğinin sağlanması için teknik ve idari olarak ne tarz önlemler alındığı ve alınan önemlerin yeterli olup olmadığının kontrolünü sağlayan ne tarz mekanizmalar kurgulandığı, olası bir veri ihlali durumunda ilgili veri sorumlusu bünyesinde alınacak aksiyonlara ilişkin ne tarz süreçler ve politikalar kurgulandığı, söz konusu kişisel verilerin kimlere, hangi amaçlarla ve hangi kapsamda aktarıldığı gibi konulara ilişkin tevsik edici belgelerin bulunması önemlidir[68]. Zira, kişisel veri işleme faaliyetlerinin veri koruma ilkelerine uygun olarak yürütüldüğünün ortaya konulması "hesap verebilirlik" ile ilgilidir.

Veri sorumluları tarafından hesap verebilirlik ilkesine uygun davranıldığının söylenebilmesi için; işlenen kişisel verilerin güvenliği için gerekli her türlü teknik ve idari tedbirin alınmış olması, kişisel veri işleme süreçlerine ilişkin düzenli olarak kontrol ve değerlendirmeler yapılması ve ilgili mevzuata uygunluğun sağlanmasına ilişkin kayıtların eksiksiz olarak tutulması[69] gerekmektedir.

Kişisel verilerin korunması için gerekli önlemlerin alınması hesap verebilirlik ilkesinin bir gereği olup bu ilke sayesinde veri sorumlusunun hem veri koruma konusundaki anlayışı hem de pratikteki bağlılığı güçlenir[70].

[68] Çekin, M. S. (2018). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s.138, p.282. On İki Levha Yayıncılık.
[69] Voigt and Von dem Bussche, 2017, s.31.
[70] A.g.e, s.31.; Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role* (1st ed.), s.23 & s.168.

Hesap verebilir durumda olma, veri sorumluların yürürlükte olan kişisel verilerin korunması düzenlemelerine uygunluk sağlamalarının temin edilmesinin yanı sıra kişisel verileri işlenen ilgili kişiler nezdinde güven yaratılması bakımından da önem arz etmektedir.

2.2.3. Gönüllülük Esasına Dayanması Bakımından Hesap Verebilirlik

95/46 sayılı Direktif'in 29. maddesi ile kurulan ve WP 29 olarak adlandırılan çalışma grubunun danışma komitesi görevini üstlendiği dönemde vermiş olduğu görüşte, hesap verebilirlik mekanizmalarının "iki kademeli" olarak değerlendirilmesi gerekmektedir. Bu kademelerden ilki, kişisel veri işleme faaliyetleri bakımından veri sorumlusu olarak hareket eden tarafların yasal yükümlülüklerini oluşturur. İkinci kademe ise, bir taraftan "birinci kademe" hesap verebilirliğin uygulanmasına yardımcı olur iken, diğer taraftan yürürlükte olan asgari düzeydeki veri koruma kuralların ötesine geçerek[71] birtakım ilave güvenceler sağlaması ile ilgilidir.

WP 29'un bahsettiği ikinci kademe mekanizmalar[72], davranış kuralları ve sertifikasyon gibi GVK Tüzüğü kapsamında uygulanması zorunlu olmayan, ancak ilgili kuruluşlar tarafından kabul edildiği hallerde bağlayıcı olup uygun davranılması gerekecek olan mekanizmalardır. Dolayısıyla "gönüllü hesap verebilirlik" bir anlamda, mevzuattan kaynaklanan sorumlulukların yerine getirilmesi zorunluluğuna ilave olarak, kişisel veri işleme faaliyeti yürütülen tarafın bu sorumluluğu kabul etmeye istekli olması olarak nitelendirilebilir[73].

---

[71] Centre for Information Policy Leadership. (2018). *The case for accountability: How it enables effective data protection and trust in the digital society.* The central role of organisational accountability in data protection. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf (Erişim Tarihi: 29.05.2023)

[72] Madde 29 Çalışma Grubu (2010), s.6.

[73] Sümer, B. (2019). *The certification mechanism under the EU General Data Protection Regulation* (Yüksek Lisans Tezi). Marmara Üniversitesi, s.25.

2.2.4. Hesap Verebilirliğin Müstakil Bir İlke Olup Olmadığı Tartışması

Hesap verebilirlik ilkesinin müstakil bir ilke olup olmadığı -özellikle AB içerisinde- süregelen tartışmalara konu olmaktadır. Bir görüşe[74] göre, hesap verebilirlik başlı başına uyulması gereken bir ilke olmayıp ihlali halinde hukuken doğrudan bir sonuç doğurmayan ve yalnızca ilgili olduğu muhtelif ülkelerin uygulanmasını sağlamak amacıyla var olan bir ilkedir. Buna karşın, diğer görüş[75], hesap verebilirliğin başlı başına uyulması gereken bir ilke olduğunu savunur. Veri koruma hukuku bağlamındaki anlamıyla hesap verebilirlik, kişisel veri işleme faaliyetlerinin ilgili yasal düzenlemelere uyumluluğu konusunda yetkili makam ve otoritelere hesap verilmesini sağlamaktadır. Bu yönüyle, hesap verebilirliğin müstakil bir ilke olarak kabul edilmesi gerekir ki GVK Tüzüğü ile veri koruma hukukuna kazandırılan bu ilkenin maddi sonuçları[76] ve dolayısıyla caydırıcı bir etkisi olsun[77]. İkinci görüşün, risk temelli yaklaşımın bir sonucu olarak ortaya çıktığı söylenebilecektir.

Öte yandan, ABAD tarafından Mayıs 2023'ye yayımlanan C-60/22 referanslı dava78 kapsamında yapılan değerlendirmeye göre, hesap verebilirlik gerekliliklerinin ihlali, tek başına veri işleme faaliyetlerini hukuka aykırı hale getirmeyecektir. ABAD'ın bu yorumundan hareketle, hesap verebilirlik ilkesinin müstakil bir ilke olarak görülmediği söylenebilecektir. O halde ABAD'a göre hesap verebilirlik, asli uyum yükümlülüğü olmayıp yan uyum yükümlülüğü vasfını haizdir. Yine de, ABAD tarafından yapılan değerlendirmenin merkezinde hesap verebilirlik ilkesi olduğundan hareketle, kişisel veri koruma mevzuatı ve etkili bir veri koruma programı bakımından bu ilkenin önemi yadsınamayacaktır.

---

[74] Gunasekara, G. (2013). Paddling in unison or just paddling? International trends in reforming information privacy law. *International Journal of Law and Information Technology*, 21(2), s.163.
[75] Kuner, C., Bygrave, L. A., & Docksey, C. (2021). *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. Oxford, UK: Oxford University Press*, s.566-567.
[76] Bu ilkeye aykırı davranılmasının bağımsız olarak ayrı bir dava sebebi olması buna bir örnek olabilir. (Alhadeff et al. (2011), s.66)
[77] Kaya (2020), s.1884.
[78] Detaylı bilgi için bkz. çalışmanın "2.1.4. Avrupa Birliği Adalet Divanı Kararları" başlığı.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINDA TEMEL HESAP VEREBİLİRLİK ARAÇLARI

3.1. GVK TÜZÜĞÜ'NDEKİ TEMEL HESAP VEREBİLİRLİK ARAÇLARI

Hesap verebilirlik araçları, veri işleme süreçlerinin belli standartlara bağlanması ve bu sayede veri işleme faaliyeti yürüten taraflar ile yetkili veri koruma otoriteleri arasındaki bilgi asimetrisinin azalması[79] bakımından oldukça yararlıdır. Önceki bölümde değinildiği üzere, hesap verebilirlik araçlarından bazıları GVK Tüzüğü ile veri işleme faaliyeti yürüten taraflara getirilen yükümlülüklere uyumun ortaya konması için başvurulması gereken zorunlu yöntemler iken, bazıları ise veri sorumluları veya veri işleyenlerin gönüllü olarak başvurmaları için dizayn edilmiştir.

Bazı hesap verebilirlik araçları vardır ki, yürütülen veri işleme faaliyetleri bakımından bunlara uygun davranılması ilgili mevzuata uyum açısından zorunludur. Bunlar; işlenen kişisel verilerin korunmasını teminen gerekli ve uygun teknik ve idari tedbirlerin alınması, veri koruma politikalarının benimsenmesi, veri işleme faaliyetlerinin kayıt altında tutulması, veri sorumluları tarafından kendi adına veri işleyen taraflar ile sözleşmeler imzalanması, veri ihlallerinin kayıt altına alınması ve ihlallerin yetkili otoritelere bildirilmesi, veri işleme faaliyetlerde *"data protection by design and by default (tasarımla ve varsayılan ayarlarla veri koruma)"* yaklaşımın benimsenmesi olarak sayılabilir. Bahse konu araçlara başvurulmaksızın veri işleme faaliyetleri yürütülmesi GVK Tüzüğü'nün ihlali sonucu doğuracağından, bunlara zorunlu hesap verebilirlik araçları demek yanlış olmayacaktır.

[79] Strauß (2020), s.208.

Zorunlu hesap verebilirlik araçlarının da kendi içinde ayrıştığı noktalar vardır. Buna göre, zorunlu hesap verebilirlik araçlarından bazıları, veri sorumlusuna veri işleme faaliyetinin niteliği, hacmi, işleyen tarafın sıfatından bağımsız olarak her hâlükârda sorumluluk yüklemekle birlikte, bazıları ise yalnızca belli şartların sağlanması halinde uyulması gereken kurallar getirmektedir. Belli şartların sağlanması halinde zorunlu olacak hesap verebilirlik araçlarına örnek olarak, veri koruma sorumlusu ("DPO") atanması ve veri koruma etki değerlendirmesi ("DPIA")[80] yapılması verilebilecektir[81].

Zorunlu araçlarının aksine, gönüllü hesap verebilirlik araçları yalnızca ilgili kuruluşlar tarafından uygulanması tercih edilen hallerde bağlayıcıdır. Çalışmanın

[80] EDPB. (4 Haziran 2019). *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (Version 2.0)*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf (Erişim Tarihi: 29.05.2023)

[81] Veri koruma görevlisi atanması ile DPIA, 95/46 sayılı Direktif'in yürürlükte olduğu dönemlerde bulunmayan ve GVK Tüzüğü ile yasal düzenleme haline getirilen konseptlerdir. Buna karşın, veri koruma görevlisi atanması ilk kez GVK Tüzüğü ile birlikte ortaya çıkmamıştır. Zira GVK Tüzüğü'nün yürürlük tarihinden önce de AB üye devletleri tarafından veri koruma görevlisi (DPO) atama uygulamasına yer yer başvurulmuştur. GVK Tüzüğü'nün 37 ila 39 maddelerinde düzenlenen "veri koruma görevlisi (DPO)", veri işleme faaliyeti yürüten tarafın veri sorumlusu veya veri işleyen olduğuna bakılmaksızın, GVK Tüzüğü'nün 37. maddesinin 1. fıkrasında sayılan hallerde atanır. Ancak bir atama ile yetkilendirme söz konusu olması, veri koruma görevlisinin veri sorumlusu veya veri işleyenin talimatlarına bağlı olarak hareket edeceği anlamına gelmez. Veri koruma görevlisi, GVK Tüzüğü, m.38(3) uyarınca bağımsız bir fonksiyonda olup varlık amacı veri koruma hukukunun paydaşları arasında aracı gibi hareket etmektir. Veri sorumlusu veya veri işleyenden bağımsız bir aktör olan veri koruma görevlisinin, ilgili veri koruma mevzuatına uyumun sağlanması bakımından bir sorumluluğu bulunmamaktadır. Başka bir deyişle, mevzuata uyum yükümlülüğü, veri koruma görevlisi atanan hallerde dahi veri sorumlusu veya veri işleyene ait olmaya devam etmektedir. GVK Tüzüğü'nün 37. maddesinin 1. fıkrasında sayılan hallerde haricinde veri koruma görevlisi atanması veri işleme faaliyeti yürüten tarafların inisiyatifine kaldığından, bu konseptin belli şartların varlığı halinde zorunlu hale gelen hesap verebilirlik araçlarından olduğu açıktır. Veri koruma görevlisi atanmasında olduğu gibi, DPIA yapılması da yalnızca GVK Tüzüğü'nde açıkça belirtilen hallerde zorunludur. DPIA, veri işleme faaliyetleri açısından olası riskleri tespit ve analiz edilmesi, analizlerin değerlendirilmesi ve ortadan kaldırılması için gerekli aksiyonların alınması açısından önemli bir fonksiyona sahiptir. Öte yandan, DPIA'in her durumda zorunlu olmaması ve risk yönetimi kapsamında yalnızca belli hallerde zorunlu tutulması, GVK Tüzüğü'nde anılan *risk temelli yaklaşım* ile örtüşmektedir. GVK Tüzüğü'nün 24(1) maddesine göre DPIA yapılması gerekip gerekmediğinin tespitinde, "*gerçek kişilerin hak ve özgürlüklerine yönelik değişen olasılık ve şiddetteki riskler"* dikkate alınır ve ilgili kişilere yönelik yürütülen veri işleme faaliyetlerinin bu kişilerin temel hak ve özgürlüklerinin korunması bakımından yüksek risk oluşturabileceği öngörülen süreçlerde DPIA zorunlu bir araçtır. Bu sayede, yüksek riskle sonuçlanması olası süreçler, veri işleme faaliyeti başlamadan evvel analiz edilerek düzeltici aksiyonlar alınabilmektedir. Bu yönüyle adete bir simülasyon niteliğini haiz olan DPIA, ilgili mevzuata uyumun sağlandığının ve takip edildiğinin ortaya konulmasına imkan veren en temel hesap verebilirlik araçlarındandır.

konusu oluşturan davranış kuralları ve sertifikasyon mekanizmalarının her ikisi de gönüllü hesap verebilirlik araçlarından olup ilerleyen bölümlerde detaylı bir şekilde ele alınacaktır. Ancak gönüllü hesap verebilirlik araçlarının davranış kuralları ve sertifikasyon ile sınırlı olmadığını bilmek gerekir[82].

GVK Tüzüğü'nde öngörülen hesap verebilirlik araçları sayesinde, veri sorumlusunun mevzuata uyum sağlama ve uyumluluğunu *ex ante* bir şekilde ortaya koyabilme[83] imkânı olacaktır. Diğer taraftan, veri sorumlularının GVK Tüzüğü'nün 24. maddesinde öngörülen yükümlülüklerini yerine getirirken, veri işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçları ile kişisel verisi işlenen gerçek kişilerin hak ve özgürlükleri bakımından çeşitli senaryo ve risk seviyelerini dikkate almaları, veri koruma hukukundaki risk temelli bir yaklaşımın *(risk-based approach)*[84] varlığına işaret etmektedir. Tek başına bu yaklaşım dahi, hesap verebilirlik ilkesinin başlı başına uyulması gereken bir ilke olarak kabul edilmesi gerekliliği şeklinde yorumlanabilecektir[85].

Risk temelli yaklaşıma göre, veri işleme faaliyetlerinin mahiyetine ve risk seviyelerine bağlı olarak veri sorumlularının mevzuata uyum için yerine getirmesi gereken yükümlülüklerinin kapsamı değişkenlik gösterebilecektir. Hal böyle iken, veri sorumlularının yükümlülüklerinin risk temelli yaklaşım sayesinde "ölçeklenebilir" hale geldiğini söylemek yanlış olmayacaktır[86].

---

[82] Örnek vermek gerekirse; GVK Tüzüğü'nün 47. maddesinde düzenlenen Binding Corporate Rules (Bağlayıcı Şirket Kuralları-"BCR") da zorunlu olmayan uyum ispat araçları arasındadır. Özel sektörü tarafından hazırlanmakla birlikte, geçerli hale gelebilmesi için kamu ve özel sektörün ortak çalışması gerektirmesi bakımından benzerlik gösteren bu iki hesap verebilirlik aracı, kurallara uygun davranacak taraflar bakımından farklılaşmaktadır. Bu doğrultuda, bağlayıcı şirket kuralları, grup şirketleri bakımından öngörülmüş olup ilgili grup bakımından düzenleme getirirken, davranış kurallarının belirli bir sektör düzeyinde düzenleme getirmektedir (Koščík & Myška (2018), s.144 - 145).

[83] Kuner et al. (2021), s. 242.

[84] Anılan kavram ile ilgili detaylı bilgi için bkz. Quelle, C. (2018). Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation,* 9(3), s. 502-526.

[85] Kaya (2020), s.1884.

[86] Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review,* 35, Article 105342, s.7.

Hesap verebilirlik kavramını somutlaştıran 24. maddenin 1. fıkrasında bu ilke ışığında veri sorumluları tarafından alınması gereken aksiyonlar düzenlenirken, aynı maddenin 3. fıkrasında bu çalışmanın temelini oluşturan davranış kuralları ve sertifikasyon mekanizması hakkında da düzenleme yapılmıştır. Bu düzenlemeye göre; *40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı sertifikasyon mekanizmalarına uygun hareket edilmesi veri sorumlusunun yükümlülüklerine uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.".* O halde davranış kuralları ve sertifikasyon, mevzuata uyumun belgelenmesi bakımından elverişli hesap verebilirlik araçlarındandır[87].

3.2. HESAP VEREBİLİRLİK BAKIMINDAN DAVRANIŞ KURALLARI VE SERTİFİKASYON

Davranış kuralları ve sertifikasyon mekanizmaları, veri sorumlusu ve veri işleyenlerin üçüncü kişilere karşı hesap verebilir durumda olmasına hizmet eder. Onaylı davranış kurallarının veya sertifikasyonun varlığı tek başına ilgili mevzuata uyumluluğu kanıtlamasa da uyumluluk iddiasının ispatı açısından önemli birer göstergedir[88].

3.2.1. Regülasyon Yapma Yöntemi Bakımından Davranış Kuralları ve Sertifikasyon

Bu enstrümanlar geleneksel devlet düzenlemelerinden farklı olarak içeriğin ilgili paydaşlar tarafından düzenlendiği alternatif bir regülasyon yönetimi olan öz-düzenleme[89] şeklinde karşımıza çıkmaktadır. Hirsch, regülasyon yapma yöntemlerini "devlet eliyle düzenleme *(direct government regulation)*", "beraber

[87] Çekin (2018), s.233.
[88] Curtis, P., & Prazeres, N. (2021). *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4.bask*ı), s.305. IT Governance Publishing.
[89] Genel itibariyle "öz-düzenleme", gönüllü olarak üyelerinin davranışlarını, eylemlerini ve standartlarını düzenleyen veya yönlendiren kurallar ya da davranış kuralları geliştiren bir grup ekonomik aktörü (belirli bir sektörde faaliyet gösteren veya profesyonel bir grupta yer alan firmalar gibi) içermektedir. Bkz. Hepburn, G. (2009). *OECD Report: Alternatives to Traditional Regulation.*

düzenleme *(co-regulation)*" ve "öz-düzenleme *(self-regulation)*" olarak üç ayrı kategoriye ayırır[90]. Devlet eliyle düzenleme yönteminde kurallar yalnızca kamu tarafından belirlenirken, beraber düzenleme yönteminde ise devlet ve özel sektör birlikte hareket ederek kuralları hazırlanması ve uygulanması bakımından sorumluluğu paylaşır[91].

Yani öz-düzenleme ve devlet eliyle düzenleme iki uç kutupta iken; "beraber düzenleme" bunların ortasında bir yerdedir. İki karşıt kutba ait bu yöntemlerin avantajları olduğu gibi dezavantajları da mevcuttur. Bu sebeple "beraber düzenleme" yönteminde, diğer yöntemlerin yalnızca yönleri bir araya getirilmek istenmiş ve özel teşebbüs kuralların hazırlayıcısı, devlet ise denetleyicisi olarak konumlandırılmıştır[92]. Devlet ve özel teşebbüslerin birlikte çalıştığı bu yöntemden bahsedilirken co-regulation yerine *regulated self-regulation, enforced self-regulation, enforced voluntary regulation, audited self-regulation* kavramları kullanılabilmektedir[93].

WP 29 tarafından yapılan öz-düzenleme tanıma göre: *"Aynı meslek veya sektörden çok sayıda veri sorumlusu için geçerli olan ve içeriği önceden ilgili sektör veya meslek mensupları tarafından belirlenen veri koruma kuralları dizisi"*[94] anlamına gelmektedir. Diğer bir ifadeyle öz-düzenleme; belirli bir sektör veya meslek mensuplarının oluşturduğu bir organ tarafından, gönüllü olarak ve kamu müdahalesi olmaksızın hazırlanan kurallardır. Devlet bu tür düzenlemelerin denetleyen pozisyonunda dahi değildir[95]. Bu yaklaşıma göre hazırlanan kuralların

[90] Hirsch, D. D. (2013). In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct. *Ohio State Law Journal*, 74, s. 1527-1556, s. 1039.
[91] Kamara, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology*, 8(1), s.12.
[92] Çekin (2018), s.232.
[93] A.g.e., 232.
[94] Madde 29 Çalışma Grubu. (1998). Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp7_en.pdf (Erişim Tarihi: 29.05.2023)
[95] Çekin (2018), s.232.

daha sonra herhangi bir kamu otoritesinin onayına sunulması söz konusu değildir. Kamu dâhiliyetinin olmaması dolayısıyla öz-düzenlemede kontrol süreçleri çok daha hızlı bir şekilde işler, zira bürokratik süreçler bu yaklaşımda ekarte edilmiş durumdadır.

Devlet müdahalesi içermeyen tek regülasyon yapma yöntemi öz-düzenleme olduğundan, bazı hallerde teknoloji alanında yaşanan değişikliklerinin hızını bu şekilde yakalamak mümkün olabilmektedir[96]. Hal böyle iken, teknolojinin gelişimiyle hızla değişen ve gelişen dinamik sektörlerin gereklerine uyum sağlanabilmesi açısından bu yaklaşım, diğer regülasyon yapma yöntemlerine nazaran daha esnek ve aynı zamanda daha düşük maliyetli bir çözüm sunmaktadır.

Gerek öz-düzenleme yönteminin esnek bir yapıya sahip olması, gerek de ilgili sektör veya meslek mensuplarınca düzenlenen kuralları içermesi sebebiyle, sektör-spesifik düzenlemeler getirilmesi kaçınılmaz olup bu sayede sektör özelinde iyi uygulamalar ortaya konulması mümkündür. Bu yönüyle öz-düzenleme, veri koruma hukukundaki "tasarım yoluyla gizlilik *(privacy by design)*" yaklaşımıyla benzeşir. Düşük maliyetli, hızlı, esnek ve sektöre özel düzenlemelerin oluşturulmasına imkân vermesi açısından öz-düzenlemenin büyük avantajları bulunmakla birlikte, Hirsch'e göre öz-düzenleme; gerek pratik gerek teorik bazı yönleriyle eleştirilmeye mahkûmdur ve hatta bu yaklaşımın bazı özellikleri avantajdan ziyade dezavantaj yaratmaktadır. İlgili sektör veya meslek mensuplarınca düzenlenen kuralların, yürürlükte olan ve kamu idaresini içeren yasal düzenlemelere uygun olup olmadığı konusunda herhangi bir teminat bulunmaması Hirsh'in öz-düzenleme yönetimini en çok eleştirdiği noktalarından biridir. Ayrıca, çok sayıda sınır ötesi veri transferinin söz konusu olduğu hallerde farklı ülkelerin ulusal mevzuatına sağlanması gerekeceğinden, öz-düzenlemenin düşük maliyetli olma özelliğini yitirmesi işten bile değildir[97]. Buna karşın, özellikle sınır ötesi veri aktarımlarının söz konusu olduğu haller ile teknoloji

[96]Çekin (2018), s.231.
[97] Hirsch (2013), s.1042-1043.

çağında hızla değişmeyi gerektiren sektörlerin varlığı gözetildiğinde, tamamen devlet düzenlemesine dayanan bir sistem de yeterli olmayacaktır[98].

Regülasyon yapma yöntemlerinden öz-düzenleme yönteminin doğal bir sonucu öz denetim olduğundan, her iki enstrümanın da başta risk analizi ve uyum süreci olmak üzere birçok anlamda ilgili veri sorumlusu veya veri işleyene öz denetim imkânı tanıdığı söylenebilecektir[99]. Kişisel verilerin korunması bakımından gerekliliklerin her bir sektör bakımından gün geçtikçe farklılaştığı bir dünyada, öz-düzenleme yöntemiyle ve ilgili paydaşların somut çıkarları gözetilerek hazırlanan davranış kuralları ve sertifikasyonlar, verilerin korunması bakımından paydaşlarına esnek ve isabetli çözümler sunmaktadır. Regülasyon yöntemlerinden öz-düzenleme yönteminden faydalanılmakla birlikte, davranış kuralları ve sertifikasyon bakımından ilgili otoriteler ile işbirliği içerisinde hareket edilir[100].

Davranış kuralları ve sertifikasyon, hazırlık aşamasında devlet müdahalesi barındırmaması sebebiyle öz-düzenleme yöntemleri arasında kabul edilir. Buna karşın, AB hukukuna son dönemlerde kazandırılan düzenlemelerde öz-düzenleme yönteminin yetersiz kaldığına değinildiği görülür[101]. Her ne kadar AB'nin öz-düzenleme yönteminden tamamen uzaklaştığı söylenemeyecekse bile, son dönemlerde yasal olarak bağlayıcı düzenlemelerin dahi oldukça kazuistik olması

[98] Hirsch (2013), s.1045.
[99] Çekin (2018), s.232-233.
[100] A.g.e., s.231.
[101] AB'nin 14 Eylül 2022 tarihli ve kısaca "Dijital Pazarlar Yasası (Digital Markets Act)" olarak adlandırılan yeni direktifi henüz yürürlüğe girmeden önce bu direktifle ilgili bir öneri (proposal) sunulmuştu. Bu taslak versiyonda yer alan "enstrüman tercihi *(choice of instrument)*" başlığı altında direktifin hazırlanmasında faydalanılan regülasyon yapma yöntemine değinilmiştir. Bu bağlamda, problemlerin çözümü için yasal olarak bağlayıcı olan ve AB genelinde aynı şekilde uygulama alanı bulan düzenlemelerin önemi vurgulanmıştır. Yürürlüğe giren Dijital Pazarlar Yasası'na erişim için: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925; Dijital Pazarlar Yasası'nın yürürlüğünden önce öneri olarak sunulan versiyona erişim için: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en (Erişim Tarihi: 29.05.2023). Benzer şekilde, 27 Ekim 2022 tarihli ve kısaca "Dijital Hizmetler Yasası (Digital Services Act)" olarak adlandırılan yeni direktifinin yürürlüğü öncesi sunulan öneride de benzer bir vurgu yapıldığı ve öz-düzenlemenin yetersiz kaldığı durumlara değinildiği görülmektedir. Bkz. Dijital Hizmetler Yasası, s.7. Dijital Pazarlar Yasası'na erişim için: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN (Erişim Tarihi: 29.05.2023).

AB hukukunda yeni bir paradigmanın habercisi olabilir. Yani AB regülasyon dünyasında norm temelli yaklaşıma kıyasla, ilke temelli yaklaşıma daha tercih edilir hale gelmeye başladığı söylenebilir[102].

3.2.2. Genel Hatlarıyla Davranış Kuralları

3.2.2.1. Kavramsal Olarak Davranış Kuralları

GVK Tüzüğü'nün 40. ve 41. maddelerinde detaylı olarak düzenlenen ve kendisine yer yer sair maddelerde[103] atıflarda bulunulan davranış kuralları, aslında ilk olarak 95/46 sayılı Direktif'in 27. maddesinde ele anılan bir kavramdır. Ancak GVK Tüzüğü'nün yürürlüğe girmesiyle birlikte, bu kavrama çok daha ayrıntılı (davranış kurallarının oluşturulma ve kabul usulü gibi detayları içeren) bir şekilde yer verilmiştir[104]. GVK Tüzüğü, m.40(1)'e göre; *"Üye devletler, yetkili veri koruma otoriteleri, Kurul ve Komisyon, çeşitli işleme sektörlerinin spesifik özellikleri ve mikro, küçük ve orta büyüklükteki işletmelerin spesifik ihtiyaçlarını dikkate alarak, bu Tüzük'ün düzgün bir şekilde uygulanmasına katkıda bulunması amaçlanan davranış kurallarının hazırlanmasını teşvik eder."*.

[102] Kaya, M. B. (2022). *Avrupa Birliği P2B Tüzüğü: Aracı Hizmet Sağlayıcılar ve Arama Motorları İçin Adil ve Şeffaf Platform Kuralları,* s.107-108. On İki Levha Yayıncılık.
[103] Bkz. GVK Tüzüğü, m.40-41; GVK Tüzüğü, Resital 98-99.
[104] 95/46 sayılı Direktif'te düzenlenen davranış kurallarının, GVK Tüzüğü'nde daha detaylı ve geniş kapsamlı olarak düzenlenmesi ve bu yolla tekrar teşvik edilmesinin sebebinin hukuk güvenliği kavramı ile ilgili olduğu söylenebilecektir. Kişisel veri koruma mevzuatına uyumun sağlanması bakımından veri sorumlularına yüklenen sorumlulukların, küçük ölçekli ve az kaynağa sahip şirketler tarafından bile üstlenilmesi gerekmektedir. Ancak ilgili mevzuata uyum için gerekli maliyet ve eforun veri sorumlularının tamamı tarafından eksiksiz sağlanması mümkün olmayabileceğinden, uygulamada risk temelli yaklaşımın benimsenerek bazı risk kabulleri ile ilerlendiği olabilmektedir. Nitekim veri sorumlusu olarak hareket eden bir şirketin ölçeği gibi başkaca faktörler de risk temelli yaklaşımı gerekli kılabilir. Siber güvenlik alanına benzer olarak, doğası gereği kişisel verilerin korunması ile ilgili konularda da her zaman sıfır riskten bahsetmek mümkün olmayacaktır. Bu gibi durumlarda hukuk güvenliği daha da önem kazanır. Zira hukuk güvenliği sayesinde, beyaz veya siyah olarak nitelendirilemeyip gri alanda kalan konularda belirli, öngörülebilir ve güvenilirliğe duyulan ihtiyaç artar. GVK Tüzüğü'nde öngörülen davranış kuralları ve sertifikasyonun bu ihtiyacın karşılanmasına ve dolayısıyla hukuk güvenliğinin sağlanması hizmet eden araçlardan olduğu yorumu yapılabilecektir.

GVK Tüzüğü'nde davranış kurallarının tanımı yapılmamış, ancak 40(2) maddesinde davranış kurallarının kimler tarafından hangi hususlar dikkate alınarak hazırlanabileceği ve bu kuralların hazırlanmasının hangi makamlarca teşvik edilmesi gerektiğine ilişkin genel bir çerçeve çizilmiştir. Bununla birlikte, hem 95/46 sayılı Direktif'te hem de GVK Tüzüğü'nde, davranış kurallarının hazırlanmasında farklı ölçekteki işletmelerin[105] spesifik ihtiyaçlarının dikkate alınması gerektiği vurgulanmıştır. Genel bir tanım yapılacak olursa, davranış kuralları; *"belirli sektörlerin ihtiyaçları dikkate alınarak tasarlanan, bir işletmenin veri işleme süreçlerinin birçoğunu adresleyerek bu işleme süreçlerinin hukuka uygun olarak yürütülmesini amaçlayan kurallar bütünü"*nü ifade eder[106].

GVK Tüzüğü ile GVK Tüzüğü'nün davranış kurallarını düzenleyen maddelerinin uygulanması bakımından yol göstermek adına EDPB tarafından yayımlanan ana rehbere[107] göre, davranış kurallarının hazırlanması ve bu sayede GVK Tüzüğü'nde yer alan düzenlemelerin etkin bir şekilde uygulanması açısından, AB üye devletleri, yetkili veri koruma otoritesi, EDPB ve Kurul'un veri sorumlularını teşvik etme yükümlülüğü vardır. Bu yükümlülük, GVK Tüzüğü'nün 40. maddesinin 1. fıkrasıyla getirilmiş olup aynı maddenin devam eden 2. fıkrasında davranış kurallarını hazırlama, değiştirme ve kapsamını genişletme hakkı ve yetkisi, birlikler ile veri sorumlusu veya veri işleyenleri temsil eden diğer organlara (örneğin: ticaret birlikleri, sektörel örgütler, akademik örgütler ve çıkar grupları[108]) tanınmıştır.

Birlikler veya diğer organlar tarafından hazırlanan davranış kurallarına katılmak suretiyle bunları kabul eden tarafların kimler olabileceği ise 95/46 sayılı

[105] 20 Mayıs 2003 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayımlanan Komisyon tavsiyesindeki mikro, küçük ve orta ölçekli işletmelerin tanımı için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361&from=EN (Erişim Tarihi: 29.05.2023)
[106] Çekin (2018), s.233.
[107] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*.
[108] A.g.e., s.11.

Direktif ile GVK Tüzüğü'nde farklılık göstermiştir. 95/46 sayılı Direktif'in davranış kuralları ile ilgili maddeleri yalnızca 95/46 sayılı Direktif'e tabi olan taraflar bakımından geçerli iken; GVK Tüzüğü ile onaylı davranış kurallarına katılabilecekler arasına GVK Tüzüğü'ne tabi olmayan[109] tarafların da eklendiği görülmektedir. GVK Tüzüğü'nün 40(3) maddesine göre, GVK Tüzüğü'ne tabi olan veri sorumluları ve veri işleyenin yanı sıra, GVK Tüzüğü'ne tabi olmayan veri sorumluları ve veri işleyenler de belli şartların sağlanması kaydıyla davranış kurallarına katılabilirler. GVK Tüzüğü'nün 46(2) maddesinin (e) bendine yapılan atıf yapılmak suretiyle bu şartlara işaret edilmiştir.

Madde 46 (2)(e)'ye göre AEA dışında kalan üçüncü ülkelerdeki veri sorumluları veya veri işleyenler, onaylı davranış kurallarının, ilgili kişilerin hakları da dâhil olmak üzere uygun güvenceleri uygulamaya yönelik bağlayıcı ve uygulanabilir taahhütler ile birlikte sağlanması kaydıyla, GVK Tüzüğü'nün 40. ve 41. maddelerine konu davranış kurallarına katılabilecektir. Bu bağlayıcı taahhütler, sözleşme veya sair bağlayıcı belgeler vasıtasıyla sağlanabilir. GVK Tüzüğü'ne tabi olmayan veri sorumluları ve işleyenlere GVK Tüzüğü ile sağlanan bu imkân, davranış kuralları konsepti bakımından oldukça yeni ve önemlidir.

[109]GVK Tüzüğü'nün kapsamını, yani uygulama alanlarını, düzenleyen iki ayrı madde bulunmaktadır. Bunlardan ilki maddi kapsama ilişkin 2. maddesi iken, diğer ise bölgesel kapsama ilişkin 3. maddesidir. GVK Tüzüğü'nün 2. maddesinin 1. fıkrası uyarınca, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine GVK Tüzüğü uygulanacaktır. Aynı maddede 2. fıkrasında ise GVK Tüzüğü'nün uygulama alanı bulacağı haller yerine uygulama alanı bulmayacağı haller sayılarak maddi kapsamın sınırlarının çizildiği görülür. Bu fıkraya göre GVK Tüzüğü; (i) AB hukukunun kapsamı dışında kalan bir faaliyetler sırasında, (ii) AB'ye üye devletlerin AB Anlaşması'nın V. Başlığı'nın 2. Bölümü kapsamına giren faaliyetleri gerçekleştirmesi halinde, (iii) bir gerçek kişi tarafından yürütülen salt kişisel veya ailevi faaliyetler sırasında, (iv) yetkili makamlar tarafından kamu güvenliğine yönelik tehditlerin önlenmesi ve bunların önlenmesi de dâhil olmak üzere cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması ya da cezaların uygulanması amacıyla işlenmesi hallerinde uygulama alanı bulmaz. GVK Tüzüğü'nün bölgesel kapsamı düzenleyen 3. maddesine göre GVK Tüzüğü; (i) veri işlemenin AB dâhilinde gerçekleşip gerçekleşmediğine bakılmaksızın, kişisel verilerin bir veri sorumlusunun veya veri işleyenin AB dahilindeki işletmesinin faaliyetleri çerçevesinde işlenmesi halinde; (ii) AB dahilinde bulunan ilgili kişilerin kişisel verilerinin AB dahilinde işletmesi bulunmayan veri sorumlusu veya veri işleyen tarafından işlenmesi halinde, işleme faaliyetlerinin ücret karşılığında gerçekleşip gerçekleşmediğine bakılmaksızın ilgili kişilere mal veya hizmet sunulmasına veya (iii) AB dahilindeki ilgili kişilerin davranışlarının izlenmesine ilişkin olması halinde uygulama alanı bulacaktır.

Davranış kurallarının, kişisel verilerin GVK Tüzüğü düzenlemelerine uygun olarak yurt dışına aktarılması bakımından sahip olduğu fonksiyon, çalışmanın 4.5. başlığı altında ayrıca ele alınacaktır.

3.2.2.2. İşlevi Bakımından Davranış Kuralları

GVK Tüzüğü'nün 40 ve 41. maddelerinde düzenlenen davranış kuralları; çeşitli işleme sektörleri ile mikro, küçük ve orta büyüklükteki işletmelerin spesifik ihtiyaçlarını dikkate alınarak hazırlanır ve bu kuralları benimseyen ilgili paydaşların veri işleme faaliyetlerini hukuka uygun olarak yürütmesi için uyması gereken yükümlülüklerini içerir. Davranış kurallarının belirli bir sektör açısından standart yaratması ve bu standartların yürüttükleri veri işleme faaliyetleri bakımından birbirine benzerlik gösteren kuruluşlar tarafından oluşturulması, hem bu kuralların kabul edilmesini kolaylaştıracak, hem de bu kurallara uyumun sağlanması bakımından ilgili veri sorumluları ve veri işleyenler tarafından azami çaba gösterildiği şeklinde yorumlanabilecektir[110]. Keza davranış kuralları, bu kuralları hazırlayan birlikler veya diğer organlara üye olan tarafların GVK Tüzüğü'ne uyuma ilişkin taahhütlerini içermekle birlikte, aynı zamanda söz konusu taahhütlerin yerine getirilmesi bakımından ilgili paydaşların sarf ettiği eforu da ortaya koyar[111]. Davranış kurallarının, uygulayıcısı olan paydaşın ilgili mevzuata uyum konusundaki hassasiyetini gösterir. Bu sayede, kişisel verisi işlenen ilgili kişilerin güveni kazanılır.

Davranış kurallarının ilgili sektöre özel dizayn edilmesi sebebiyle *"*tasarım yoluyla gizlilik*"* yaklaşımıyla da örtüştüğü görülür. Bu kurallar aynı zamanda, GVK Tüzüğü'ne tabi olan AB üye devletlerinde yürürlükte olan yerel düzenlemelerdeki farklılıkları minimize ederek ortak bir uygulama zemini

[110] Hirsch (2013), s.1051.

[111] Çekin'e göre davranış kuralları; veri sorumlusu ve veri işleyenlerin yükümlülükleri, veri güvenliğinin sağlanması ve veri koruma etki analizinin yapılmasına yönelik yükümlülükler, üçüncü ülkelere hukuka uygun veri aktarımı gibi birçok konuda GVK Tüzüğü'nde yapılan düzenlemeler bakımından olumlu etki sağlar. (Çekin (2018), s.236, p.521)

oluşturulması açısından önem arz etmektedir. Ayrıca davranış kuralları, sektör ihtiyaçlarına aşina paydaşlar tarafından tasarlanması sebebiyle uygun maliyetli *(cost effective)* bir yöntem olarak kabul edilebilecektir. Daha da önemlisi bu kurallar, GVK Tüzüğü ile getirilen soyut veri koruma gereksinimlerinin yerine getirilmesi bakımından somut bir çözüm sunar[112].

Diğer taraftan GVK Tüzüğü'nün 40 ve 41. maddelerinde düzenlenen davranış kuralları ile bir işletme/kuruluş içerisinde geliştirilen iş ve/veya davranış kurallarını birbirine karıştırmamak gerekir. Bir işletme/kuruluş içinde oluşturulan ve zaman zaman farklı şekillerde adlandırılan bu tarz kurallar, esas olarak ilgili işletmenin/kuruluşun vizyonu, misyonu, değerleri ve hedefleri gibi üçüncü kişiler nezdinde oluşturmak istediği imajına ve hedeflerine ilişkin düzenlemeler içerir. Bunlar, ilgili kuruluş açısından üçüncü kişilere açıklanan ve dolayısıyla bir nevi 'taahhüt' olarak değerlendirilebilecek hususları içerse dahi, GVK Tüzüğü kapsamındaki davranış kurallarından hem bağlayıcılık hem de nitelik ve kapsam anlamında farklıdır.

3.2.3. Genel Hatlarıyla Sertifikasyon

3.2.3.1. Kavramsal Olarak Sertifikasyon

Kökeni itibariyle sertifikasyon, oldukça eski zamanlardan beri var olan ve iddia edilen bir durumun gerçekliğini doğrulamak için kullanılan bir prosedürdür[113]. Öyle ki, sertifikasyonun, bağlam ve etki alanı bakımından AB hukukunda çeşitli konularda düzenlenen bir enstrüman olduğu görülmektedir. Başka bir ifadeyle, sertifikasyon kavramı, yalnızca kişisel veri koruma hukuku ile ilgili bir kavram değildir. Daha geniş bir perspektifte sertifikasyon, *bir ürünün, bir hizmetin veya üretim veya hizmetin sağlanması ile ilgili bir sürecin ilgili mevzuat ve standartlara*

[112] Voigt & Von dem Bussche (2017), s.73
[113] Lachaud, E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review*, 34(2), s. 247.

uygunluğunu doğrulamak[114] adına üretici veya hizmet sağlayıcılar tarafından kullanılan bir araç olarak nitelendirilebilir[115]. Çalışmada, GVK Tüzüğü'nde düzenlenen sertifikasyon kavramı ele alınacak olup bu kavram, zaman zaman ve gerekli olduğu ölçüde bilgi güvenliği ve farklı disiplinlerdeki anlam ve kapsamlarıyla incelenebilecektir.

GVK Tüzüğü'nün 42. ve 43 maddelerinde sertifikasyon mekanizmasıyla ilgili düzenlemeler getirilmekle birlikte, sertifikasyon kavramına dair bir tanıma yer verilmediği görülür. GVK Tüzüğü'nde herhangi bir tanımlama yapılmaması, sertifikasyonun ne anlama geldiği ile ilgili farklı yaklaşım ve görüşler ortaya çıkarmıştır. Bir grup yazara göre sertifikasyon; *"harici ve akredite bir denetçi tarafından gerçekleştirilen ve yetkili otoriteler tarafından öngörülen gereklilikler temelinde değerlendirilen gönüllü bir uygunluk değerlendirme süreci"* olarak tanımlanabilecektir[116]. Diğer taraftan ISO, sertifikasyonu bir uygunluk değerlendirme sürecinden öte bir 'uygunluk tasdiki' olarak görmektedir. ISO tarafından yapılan tanımlamaya göre[117] sertifikasyon; *"ürünler, süreçler, sistemler veya kişiler hakkında üçüncü taraflarca gerçekleştirilen tasdik"* anlamına gelir. Dolayısıyla, ISO'nun tanımı doğrultusunda sertifikasyon kavramı, uygunluk değerlendirilmesi yapılmasının yanı sıra, mevzuata uyumun devamlılığını da kapsar. Ayrıca, gerçekleştirilen uygunluk değerlendirmesinin olumlu sonuçlanması şartına bağlı olarak sertifikasyon düzenlenebildiğinden hareketle, ISO tarafından yapılan tanımın daha kapsayıcı ve yerinde olduğu söylenebilir.

[114] Papakonstantinou, V. (2018). Introduction: Privacy and Data Protection Seals. In *Privacy and Data Protection Seals*, s.3.
[115] A.g.e., s.4.
[116] Lachaud, E. (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. *Computer Law & Security Review*, 32(6), s.2.
[117] ISO/IEC. (2019). *ISO/IEC 17000:2020 Conformity assessment — Vocabulary and general principles* (Eski hali: ISO/IEC 17000:2004 - Conformity assessment) https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en (Erişim Tarihi: 29.05.2023)

GVK Tüzüğü'nün 42. ve 43 maddelerinde düzenlenen sertifikasyon mekanizması bakımından yol gösterici olması adına EDPB tarafından yayımlanan rehberden[118], EDPB'nin de ISO'nun sertifikasyon ile ilgili tanımlamasını esas aldığı anlaşılmaktadır. EDPB'nin yaklaşımına göre sertifikasyon; *"GVK Tüzüğü'ndeki gerekliliklerine uyumunun ortaya konması adına gönüllük esasına dayalı bir ispat aracı olup mikro, küçük ve orta ölçekli işletmelerin spesifik ihtiyaçlarının dikkate alınması suretiyle oluşturulan, üye devletler, yetkili veri koruma otoriteleri, EDPB ve Komisyon tarafından özellikle AB düzeyinde oluşturulması teşvik edilen ve veri sorumluları veya veri işleyenler tarafından yürütülen işleme faaliyetlerinin üçüncü taraflarca tasdiki sonucunu doğuran veri koruma belgelendirme mekanizmaları (sertifika), veri koruma mühürleri ve işaretlerinin tümü"* anlamına gelir[119].

Yukarıda açıklandığı üzere, 'sertifikasyon' genel bir ifade olup veri koruma belgelendirme mekanizmaları (sertifika), veri koruma mühürleri ve işaretlerinin tümünü içermektedir. GVK Tüzüğü'nde ne çatı sertifikasyon kavramıyla ne de bu çatı kavramın altındaki belge (sertifika), mühür ve işaretler ile ilgili herhangi bir tanımlama yapılmaktadır[120]. GVK Tüzüğü'nde açık bir şekilde düzenlemeyen bu husus, EDPB'nin sertifikasyon ile ilgili açıklama getiren bir rehberinde ele alınmış ve bu sayede belge (sertifika), mühür ve işaretin ne anlama geldiğine açıklanmıştır.

---

[118] EDPB. (4 Haziran 2019). *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation (Version 3.0).* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf (Erişim Tarihi: 29.05.2023)

[119] A.g.e., s.8; EDPB tarafından öngörülen sertifikasyon tanımı kapsayıcı olmakla birlikte, önerilen tanımın GVK Tüzüğü'nde tanımlanan sertifikasyon konsepti ile tam anlamıyla örtüşmediği sebep gösterilerek Lachaud tarafından eleştirilmiştir. Zira Lachaud, GVK Tüzüğü'ndeki sertifikasyon düzenlemelerinin EDPB tarafından öngörülen sertifikasyon tanımdan daha detaylı olduğunu söyler. (Lachaud, E. (2020). What GDPR tells about certification. Computer Law & Security Review, 38, s.12.).

[120] Kamara, I. & De Hert, P. (2018). Data protection certification in the EU: Possibilities, Actors And Building Blocks In a Reformed Landscape. *Privacy and Data Protection Seals*, s.30.

EDPB'ye göre belge (sertifika) bir *"uygunluk beyanı"* iken, mühür veya işaret ise *"sertifikanın varlığına ek olarak, bağımsız üçüncü bir tarafça yürütülen sertifikasyon sürecinin başarı bir şekilde tamamlandığı ve ilgili mevzuata uyumluluğu gösteren bir logo veya sembol"* şeklinde tanımlanabilir[121].

GVK Tüzüğü, m.42(1)'e göre, sertifikasyon mekanizması ile veri koruma mührü ve işaretlerinin kurgulanma amacı, veri sorumlusu veya veri işleyenler tarafından yürütülen kişisel veri işleme operasyonlarının GVK Tüzüğü'ne uygunluğunun sağlanmasıdır. Aynı maddenin bir sonraki fıkrası ise, bu mekanizmalara AEA içerisindeki veri sorumlusu veya veri işleyenlerin yanı sıra, belirli koşulları sağlamak kaydıyla üçüncü ülkelerdeki veri sorumluları ve veri işleyenlerin de uyumluluğunu ortaya koymak adına başvurabileceğinden bahsedilmiştir. Bu düzenlemelerden hareketle, yalnızca GVK Tüzüğü, m.4(7) ve m4(8) doğrultusunda veri sorumlusu veya veri işleyenlerin[122] hesap verebilirlik araçlarından sertifikasyona başvurabileceği söylenebilir. Kişisel verilerin GVK Tüzüğü çerçevesinde üçüncü ülkelere aktarılmasında hesap verebilirlik araçlarından sertifikasyonun önemi, çalışmanın 5.6. başlığı altında detaylandırılacaktır.

3.2.3.2. İşlevi Bakımından Sertifikasyon

Sertifikasyonun varlığı, GVK Tüzüğü madde 42(4)'de açıkça belirtildiği üzere, düzenlenen sertifikasyon, sahibi veri sorumlusu veya veri işleyenin ilgili mevzuata uyum yükümlülüklerini ortadan kaldırmadığı gibi, bu yükümlüleri azaltmaz da. Aslen GVK Tüzüğü'nde öngörülen sertifikasyon mekanizması, sertifikasyonun

[121] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.* s.8.
[122] Bu hususta EDPB tarafından verilen bir örnekte, sertifikasyonun yalnızca veri sorumluları ve veri işleyenleri için öngörüldüğünü, veri koruma görevlilerinin ise sertifikasyondan faydalanamadığı belirtilmiştir. Bkz. A.g.e. s.16.

kapsamında kalan konularda[123] ilgili veri sorumlusu veya veri işleyen tarafından GVK Tüzüğü'ne uyum konusunda gerekli teknik ve idari tedbirlerin alındığı ve tatmin edici bir şekilde uygulandığını ortaya koyan ve gönüllü olarak başvurulabilen bir uyum ispat aracıdır[124]. Buna karşılık, sertifikasyonun gönüllülük esasına dayalı olarak başvurulan bir yöntem olması, bu mekanizmanın ilgili mevzuatta öngörülen şekilde kurgulandığı takdirde bağlayıcılık anlamında yetersiz bir etkiye sahip olduğu anlamına gelmeyecektir.

Sertifikasyon düzenlenebilmesi için gerçekleştirilen uyum değerlendirmesi olumlu sonuçlanırsa, değerlendirmeyi yapan taraf ile ilgili veri sorumlusu veya veri işleyen arasında bağlayıcı etkiye sahip bir ***sertifikasyon sözleşmesi*** imzalanır[125]. Buradan anlaşılacağı üzere, yaptığı başvurunun olumlu sonuçlanması üzerine sertifikalı hale gelen veri sorumlusu veya veri işleyen, hem GVK Tüzüğü'ne hem de tarafı olduğu sertifikasyon sözleşmesine uygun davranmakla yükümlüdür.

GVK Tüzüğü, Resital 100 düzenlemesinde, sertifikasyonun varlığı ile, sertifikasyon kapsamında giren ürün ve/veya hizmetin sağladığı güvenlik standartları hakkında kişisel verisi işlenen ilgili kişilerin hızlı bir şekilde bilgilendirilebildiğine ve bu sayede sertifikasyonun şeffaflığı artırdığına değinilmektedir. İlgili kişilerin belirtilen şekilde bilgilendirmesinin bir sonucu olarak, sertifikasyondan faydalanan taraf ile verisi işlenen taraf arasında bilgi asimetrisi ortadan kalkar. Zira bir kimsenin kişisel verileri üzerinde gerçek anlamda kontrol sahibi olabilmesi, kişisel verilerini işleyen taraflarca yürütülen veri işleme süreçleri hakkında yeterince bilgilendirilmiş olmasına bağlıdır[126].

---

[123] Sertifikasyon sayesinde kişisel verisi işlenen ilgili kişilerin, söz konusu sürecin, ürünün ya da hizmetin veri koruma hukukuna uyumlu olduğu hususunda bilgi sahibi olması sağlanır. (Çekin (2018), s.240, p.536)

[124] Kamara & De Hert (2018), s.25; Sertifikasyonun ilgili mevzuata uyumun ispatı açısından en etkin araçlardan biri olduğu düşünüldüğünde, hesap verebilirlik ilkesi ile önemli bir ilişkisi bulunduğu açıktır. Hesap verebilirlik açısından sertifikasyona, özellikle de bulut bilişim veya nesnelerin interneti gibi alanlarda başvurulması oldukça faydalı olacaktır.

[125] A.g.e., s.31-32.

[126] Voigt & Von dem Bussche (2017), s.141.

Sertifikasyonun bu yönü itibariyle, bir sertifikasyon mekanizmasının etkin şekilde yürütülmesi için verisi işlenen kişilere yapılacak bilgilendirmenin tam, doğru ve eksiksiz olması önemlidir. Bu sebepledir ki, sertifikasyona konu edilen ürün, hizmet ve/veya veri işleme operasyonlarının ilk bakışta anlaşılır olması gerekmektedir[127]. Tıpkı şeffaflık gibi, *konuyla/süreçle ilgili*, *kaliteli*, *yönetilebilir*, *güvenilir* ve *doğru mesajı verebilir olma*[128] da sertifikasyon mekanizmasının sağlamlığı adına önemlidir.

Sertifikasyon ile sağlanan şeffaflık, hem ilgili kişiler hem de piyasadaki aktörlerin, bu araçtan faydalanan taraflara olan güveninin artması sağlar, hem de sertifika sahibi veri sorumluları veya veri işleyenlerin ticari çemberlerinin genişlemesine katkı sağlar. Dahası, sertifikalı ürün ve/veya hizmetlerin sertifikalı olmayanlardan ayrıştırılması mümkün olacağından, sertifikasyonun bir nevi pazarlama enstrümanı[129] olarak kullanılması mümkündür. Zira sertifikasyon, konu aldığı ürün ve/veya hizmetlerin tanıtılmasını sağlayarak veri sorumluları veya veri işleyenlere piyasada rekabet avantajı sağlayacaktır[130]. Öte yandan, sertifikasyonun nispeten pahalı bir araç olması ve bu araçtan yalnızca bütçesi imkân veren tarafların yararlanabilecek olmasından dolayısıyla, piyasadaki diğer şirketler karşısında elde edilen rekabet avantajının adil olmadığı düşünülebilecektir[131].

3.2.4. Onaylı Davranış Kuralları ve Sertifikasyonun Hizmet Ettiği Amaçlar

Yukarıdaki ele alındığı üzere davranış kuralları ve sertifikasyonun birçok ortak özelliği bulunur. Bu ortak özellikler daha ziyade davranış kuralları ve

[127] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.* s.24-25.
[128] Bock, K. (2016). Data protection certification: Decorative or effective instrument? Audit and seals as a way to enforce privacy. In C. Cuijpers, S. Nouwt, & B.-J. Koops (Eds.), Enforcing Privacy: Regulatory, Legal and Technological Approaches, s. 339.
[129] Lachaud (2020), s.8.
[130] EDPS. (26 Kasım 2014). Opinion of the European Data Protection Supervisor, s.24. https://edps.europa.eu/sites/edp/files/publication/14-11-26_opinion_rpas_en.pdf (Erişim Tarihi: 29.05.2023)
[131] Lachaud (2016), s.12.

sertifikasyonun hazırlık süreciyle ilgilidir. Ancak bu araçlardan faydalanmanın benzer etkiye sahip bazı sonuçları da vardır. Mesela, davranış kuralları ve sertifikasyon mekanizmaları ile GVK Tüzüğü'nde soyut olan birçok düzenleme somutlaştırılmış ve bu sayede anılan düzenlemelerin yarattığı belirsizliğin giderilmesi sağlanmıştır[132].

Bu araçlar, Komisyon tarafından güvenli ülke kararı bulunmayan hallerde üçüncü ülkelere GVK Tüzüğü, Madde 46(2)'ye göre uygun güvenceleri dâhilinde veri aktarılmasına da imkân vermektedir[133]. Bu yönleri itibariyle GVK Tüzüğü m. 47'de düzenlenen bağlayıcı şirket kuralları *(binding corporate rules – BCR)* ve GVK Tüzüğü m. 28'de anılan standart sözleşme maddelerine *(standart contractual clauses – SCC)* benzerler. Buna karşın BCR ve SCC'nin aksine, davranış kuralları ve sertifikasyonun temel fonksiyonunun AB dışı kişisel veri aktarımını hukuka uygun hale getirmek değildir.

Onaylı davranış kuralları ve/veya sertifikasyon mekanizmalarının varlığı, bu araçlardan faydalanan veri sorumlusu veya veri işleyenin yürüttüğü işleme faaliyetlerinin endüstrideki iyi uygulamalardan olduğunu belgeler[134]. Uyumun belgelenmesi veri sorumlusu veya veri işleyenin mevzuata uyum konusundaki çabasını ortaya konduğundan, onaylı davranış kuralları ve sertifikasyonun varlığı aynı zamanda bu araçlardan faydalanan taraflarca GVK Tüzüğü'nün ihlali durumunda ihlal eden tarafa idari para cezası verilirken hafifletici unsur olarak kabul edilebilecektir[135].

[132] Çekin'e göre, otoriler ile işbirliği içerisinde geliştirilen davranış kuralları ve sertifikasyon sayesinde GVK Tüzüğü'ndeki soyut hükümlerin somutlaştırılması özellikle meşru menfaat sebebine dayalı olarak veri işlenip işlenemeyeceği noktasında kolaylık sağlar. (Çekin (2018), s.233).
[133] A.g.e., s.234.
[134] Curtis & Prazeres (2021), s.305.
[135] Lachaud, E. (2019). Adhering to GDPR codes of conduct: A possible option for SMEs to GDPR certification. *Journal of Data Protection & Privacy*, 3(1), s. 49; EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.*

Burada unutulmaması gereken, gerek onaylı davranış kuralları gerek sertifikasyonun varlığı "iyi uygulama", "veri sorumlusunun/veri işleyenin çabası/eforu" gibi hususları gösterse de bu araçların ayrıştıkları önemli bir nokta vardır ki; sertifikasyonların uyumu ispat fonksiyonu varken, davranış kuralları yalnızca uyum iddiasını destekler. Bu nedenle bu iki araç birbirlerinin tamamlayıcısıdır[136]. Hal böyle iken, davranış kuralları ve sertifikasyon mekanizmalarının hizmet ettikleri uyumluluk amaçlarının farklı olduğu söylenebilecektir[137].

[136] Voigt & Von dem Bussche (2017), s.71.
[137] A.g.e., s.71.

DÖRDÜNCÜ BÖLÜM

HESAP VEREBİLİRLİK ARACI OLARAK DAVRANIŞ KURALLARI

4.1. DAVRANIŞ KURALLARININ KAPSAMI

GVK Tüzüğü'nün 40(2) maddesinde, bir sektörü temsil eden meslek birlikleri veya veri sorumlusu veya veri işleyen kategorilerini temsil eden diğer organlar tarafından hazırlanan, değiştirilen veya kapsamı genişletilen davranış kuralları içerisinde yer verilebilecek konular düzenlenmiştir. Ancak, 40. maddenin 2. fıkrasındaki (a)-(k) bentleri arasında yer verilen başlıklar sınırlı sayıda olmayıp ilgili birlik ve organlar tarafından hazırlanan davranış kuralları içerisinde bu maddede sayılanların haricinde farklı başlıklara yer verilmesi mümkündür. Zira, bu başlıklara yer verilmeden önce *"such as with regard to"* denilerek bu başlıkların örnek mahiyetinde sayıldığı vurgulanmıştır.

Davranış kurallarının sektör bakımından *tailor-made* (özel yapım) çözümler getirdiği düşünüldüğünde, veri sorumluları ve veri işleyenlerinin faaliyet gösterdiği sektöre göre bu kuralların içeriğinde farklılıklar olması kaçınılmazdır. GVK Tüzüğü Resital 98'e göre, veri sorumluları veya veri işleyenleri temsil eden birlik veya diğer organlar tarafından davranış kuralları hazırlanırken, veri işleme faaliyetlerinden kaynaklanabilecek olası riskler ile bu faaliyetlerin kişisel verisi işlenen ilgili kişilerin hak ve özgürlüklerine olası etkileri dikkate alınmalıdır. Hal böyle iken, davranış kurallarında öngörülen yükümlülüklerin bu hususların dikkate alınmasıyla kalibre edilmesi gerekebilir.

EDPB tarafından davranış kuralları özelinde yayımlanan rehberde[138] ise, davranış kurallarının sektöre uygun olarak dar veya geniş kapsamlı düzenlenebileceğinden bahsedilmiştir.

[138] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679,* s.9.

Yine bahsi geçen rehberde EDPB tarafından verilen bir örnekte, hayır kurumlarının faaliyet gösterdiği sektör için davranış kuralları hazırlanırken, bu kuralların hayır kurumlarının yürüteceği veri işleme faaliyetlerinin "adil ve şeffaf" yürütüleceğine ilişkin sektöre yönelik kurallara yer verilebileceğine değinilmiştir. Dernekler, vakıflar gibi kar amacı gütmeyen kuruluşların günümüzde kara paranın aklanması, yasal olmayan yollarla elde edilen değerleri bu kuruluşlara bağışlanması yoluyla kayıtlı ekonomiye kazandırılması gibi birçok yolla suistimal edilebildiği düşünüldüğünde, davranış kuralları içerisinde "şeffaflık" kavramının ön plana çıkması, sektör problemlerine veri koruma hukukunun ötesinde çözümler sunulabilmesi açısından da faydalı olacaktır. Bu durumu teminen, sektördeki aktörlerin yalnızca veri koruma hukuku alanında karşılaştıkları sorunların değil, diğer alanlarda da karşılaştıkları GVK Tüzüğü'nün doğru ve etkili bir şekilde uygulanmasını etkileyebilecek nitelikteki sorunlara da değinilmesi faydalı olacaktır.

EDPB'nin davranış kurallarının transfer aracı olarak kullanılmasına yönelik düzenlemeler getiren bir diğer rehberinde[139] ise, davranış kurallarının tek bir sektörden ziyade, aynı veri işleme karakteristiğini taşıyan ve ortak veri işleme süreçleri içeren birden fazla sektör bakımından da hazırlanabileceğine dikkat çekilmektedir[140]. Bundan hareketle, davranış kurallarının esasen belirli sektörlere yönelik düzenlemeler getirilmesi amacıyla öngörüldüğünü, ancak spesifik süreç veya aktörlerin ön plana çıktığı hallerde bu kuralların muhatabı ile kapsamının farklılık gösterebileceği anlaşılmaktadır.

Kapsamın geniş veya dar olduğundan bağımsız olarak, davranış kurallarının içeriğini oluştururken dikkat edilmesi gereken en önemli unsurlardan biri; bu kuralların yalnızca GVK Tüzüğü'nde yer alan maddelerin maddi bir yorumuna yer vermemesi ve davranış kurallarının GVK Tüzüğü, m.40(5)'e uygun olarak yetkili

[139] EDPB. *Guidelines 04/2021 on Codes of Conduct as tools for transfers*, s.6
[140] Buna örnek olarak, çocukların kişisel verileri bakımından davranış kuralları hazırlanması ile İK profesyonelleri birliği/federasyonu tarafından İK kodu hazırlanması verilmiştir.

veri koruma otoritesi tarafından onaylanabilmesini sağlayan imkân veren etkin mekanizmaları içermesidir[141]. İlaveten, davranış kurallarını hazırlayan taraflar, GVK Tüzüğü'nün yanı sıra, ilgili sektör açısından geçerlilik arz eden diğer uluslararası mevzuat ve standartlar[142] ile uygulanabilir ulusal mevzuat dikkate alınmalıdır.

Son olarak davranış kuralları, bölgesel kapsamına göre de "ulusal" ve "ulusötesi" davranış kuralları olmak üzere ikiye ayrılır. Ulusal davranış kuralları, yalnızca bir üye devlette yürütülecek kişisel veri işleme faaliyetlerine ilişkin olup, ulusötesi davranış kuralları birden fazla üye devletteki veri işleme faaliyetlerine ilişkin düzenlemeler içerir. Ulusötesi davranış kuralları, GVK Tüzüğü'nün 4. maddesinin 2. fıkrasında tanımlanan "sınır-ötesi işleme" faaliyetleriyle ilgili olabileceği gibi, "sınır-ötesi işleme" söz konusu olmaksızın birden fazla üye devletteki çok sayıda veri sorumlusu veya veri işleyen tarafından gerçekleştirilen veri işleme faaliyetleri ile de ilgili olabilir[143].

4.2. DAVRANIŞ KURALLARI İLE İLGİLİ AKTÖRLER

4.2.1. Kod Sahibi

Çalışmanın önceki bölümlerinde değinildiği üzere, davranış kurallarının hazırlanması, değiştirilmesi ve bu kuralların kapsamının genişletilmesi ile ilgili süreçler, belirli bir sektörü temsil eden birlikler veya sair bir organlar[144] tarafından yürütülmektedir. Birlikler veya sair organlardan her biri, EDPB rehberinde[145] "*code owner (kod sahibi)"* olarak da anılmaktadır. Bu doğrultuda, bir kod sahibi

[141] Voigt & Von dem Bussche (2017), s. 74.
[142] ISO standartları örnek olarak verilebilecektir.
[143] Örnek için bkz. EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679,* Appendix 1 – Distinction between national and transnational codes.
[144] GVK Tüzüğü'nün 40. maddesinin 2. fıkrasındaki genel nitelikli ve kapsayıcı sayılabilecek bu tanımların karşılığı ile ilgili değerlendirmeler için bkz. Çekin (2018), s.236, p.522.
[145] Bkz. EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679,* s.7.

tarafından hazırlanan taslak davranış kuralları, ilgili birlik veya organ tarafından yetkili veri koruma otoritesinin onayına sunulur[146].

4.2.2. Yetkili Veri Koruma Otoritesi

GVK Tüzüğü'nün 55. maddesi uyarınca yetkilendirilen ilgili veri koruma otoritesi, belirli bir sektörü temsil eden birlik veya sair bir organ tarafından hazırlanarak onayına sunulan davranış kurallarını değerlendirmekle yükümlüdür. Ayrıca yetkili veri koruma otoritesinin rolü davranış kurallarının değerlendirmesiyle sınırlı değildir. GVK Tüzüğü'nün 41. maddesi kapsamında onaylı davranış kurallarının izlenmesinden sorumlu olan akredite izleme makamlarına gerekli akreditasyon da yetkili veri koruma otoritesi tarafından sağlanır[147].

Birden fazla üye devletteki veri işleme faaliyetlerini kapsayan (ulusötesi) davranış kurallarının onay süreci, ulusal davranış kurallarından farklı olarak, EDPB ve Avrupa Komisyonu (Komisyon) ile ilgili üye devletlerin de sürece dâhil olmasını gerektirdiği için ilgili üye devletlerdeki veri koruma otoriteleriyle gerekli koordinasyonun sağlanması da yetkili veri koruma otoritesinin sorumlulukları arasındadır.

4.2.3. EDPB

Ulusal davranış kurallarının onay sürecinin aksine, EDPB birden fazla üye devleti ilgilendiren kişisel veri işleme süreçleri bakımından düzenleme getiren ulusötesi davranış kurallarının onay sürecinde rol oynamaktadır. Bu kapsamda EDPB, yetkili veri korumasının kendisine iletilmiş olan taslak davranış

[146] GVK Tüzüğü'nün 40(5) maddesi. Transferler İçin Tasarlanmış Davranış Kuralları ile detaylı bilgilere ilerleyen bölümlerde yer verilecektir.
[147] Yetkili veri koruma otoritelerinin izleme kuruluşlarını akredite etmesi yasal bir zorunluluk olmamakla birlikte, akreditasyon işleminin yetkili veri koruma otoritelerine düşen yükü azaltacağından hareketle pratikte akreditasyon işlemiyle karşılaşmasının oldukça mümkün olduğuna dair görüş için bkz. Voigt & Von dem Bussche (2017), s.75-76.

kurallarının uygun olduğu yönündeki görüşünü, GVK Tüzüğü madde 40(7) ve 64(1)-(b) uyarınca değerlendirir.

EDPB, yetkili veri koruma otoriteleri tarafından iletilen davranış kurallarının GVK Tüzüğü'ne uyum açısından asgari gereksinimleri karşılayıp karşılamadığını değerlendirilmekle birlikte, üye devletlerin uygulamalarında tutarlılık sağlanabilmesi adına ilgili veri koruma otoriteleri tarafından sunulan taslakların tadil edilmesini önerebilir[148].

4.2.4. Komisyon

Bir kod sahibi tarafından yetkili veri koruma otoritesine sunulan ve yetkili veri koruma otoritesi tarafından uygun görülen taslak ulusötesi davranış kurallarının EDPB'nin görüşüne sunulması ve bu kuralların uygunluğu bakımından EDPB'nin uygunluk vermesi üzerine, anılan kurallarının Komisyon'a bildirilmesi gerekir. Yapılan bu bildirim üzerine Komisyon, ulusötesi davranış kurallarının AB içinde ***genel geçerliliğe*** sahip olduğuna karar verebilir[149]. GVK Tüzüğü'nün 40(9) maddesindeki *"may decide"* ifadesinden, yetkili veri koruma otoritesi tarafından onaylanan ve EDPB tarafından uygun bulunan davranış kuralları için Komisyon tarafından genel geçerlilik kararı verilmeme ihtimali olduğu söylenebilecektir.

[148] EDPB. (4 Temmuz 2022). *Opinion 14/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR.* https://edpb.europa.eu/system/files/2022-07/edpb_2022-14_opinion_on_bg_sas_accreditation_requirements_of_monitoring_bodies._docx_en_0.pdf (Erişim Tarihi: 29.05.2023), s.4.

[149] Genel geçerlilik kararı verilmesi durumunda ilgili karar tüm AB üye devletleri bakımından geçerli hale gelecektir.

4.3. TASLAK DAVRANIŞ KURALLARININ ONAY SÜRECİ

Bir kod sahibi tarafından hazırlanan taslak kuralların onaylı hale gelmesi[150] için izlenmesi gereken adımlar, söz konusu davranış kurallarının "ulusal" veya "ulusötesi" davranış kuralları olması bakımından farklılık gösterecektir. Davranış kurallarının onay sürecinin ilk aşamaları, kuralların ulusal veya ulusötesi oluşuna bakılmaksızın, büyük oranda paralellik göstermektedir. Davranış kurallarının ulusal ve ulusötesi oluşuna göre onay prosedürünün ayrıştığı temel noktalar ise; yetkili veri koruma otoritesinin bulunduğu ülke dışındaki (diğer) üye devletlerdeki veri koruma otoriteleri ile EDPB ve Komisyon'un sürece dâhil olduğu hallerdir. Başka bir ifadeyle, davranış kurallarının tek bir üye devlet yerine birden fazla üye devleti ilgilendirdiği durumlarda, davranış kurallarının uygunluğu ile ilgili değerlendirme yalnızca GVK Tüzüğü'nün 55. maddesi kapsamında yetkilendirilmiş yetkili veri koruma otoritesi tarafından yürütülmeyecektir.

GVK Tüzüğü'nün 40. maddesinin 6. fıkrası ulusal davranış kurallarının onay prosedürünü düzenlerken, aynı maddenin 7. fıkrası ise ulusötesi davranış kurallarının onaylanması için öngörülen gerekliliklere yer vermektedir.

4.3.1. Taslak Davranış Kurallarının İbrazı

Ulusal ve ulusötesi niteliği haiz olup olmadığına bakılmaksızın tüm taslak davranış kuralları, belirli bir sektörü temsil eden birlik veya diğer organlar tarafından hazırlanır. Hazırlanan bu kurallar, GVK Tüzüğü madde 40(5) uyarınca yetkili veri koruma otoritesine elektronik veya fiziki ortamda yazılı olarak sunulur. Bunun üzerine, yetkili veri koruma otoritesi tarafından kod sahibine başvurusunun alındığına dair bir bilgilendirme yapılır.

[150] Daha önceden GVK Tüzüğü'ne uygun olarak onaylanmış davranış kurallarında herhangi değişiklik yapılması gereken hallerde, söz konusu kuralların gözden geçirilmesi, yeniden değerlendirilmesi, onay için sunulması ve bu esnada bu bölümde yer verilen onay prosedürünün izlenmesi gerekecektir.

Ulusötesi davranış kuralları söz konusu olduğunda ayrıca, yetkili veri koruma otoritesi diğer tüm veri koruma otoritelerine taslak davranış kurallarının ibrazına dair bir bildirim yapacak ve bu bildirimde tanımlama ve referans kolaylığı sağlayacak göze çarpan ayrıntılara yer verecektir. Buna bildirime karşılık, veri koruma otoritelerinin her birinin GVK Tüzüğü'nün 4. maddesinin 22. fıkrasında tanımlandığı kapsamda "ilgili veri koruma otoritesi" olup olmadığı konusunda yetkili veri koruma otoritesine dönüş yapması gerekir[151].

4.3.2. Taslak Davranış Kurallarının Kabul Edilebilirlik Bakımından Değerlendirilmesi

Yetkili veri koruma otoritesi tarafından (ulusal veya ulusötesi olduğu fark etmeksizin) davranış kurallarına yönelik bir değerlendirmeye başlandığında, ilk olarak taslak davranış kurallarının kabul edilebilirlik kriterlerini[152] karşılayıp karşılamadığı değerlendirilir. Bir nevi ön kontrol mahiyetindeki bu aşamanın olumsuz sonuçlanması halinde başvuru süreci sona erecektir. Sona eren bir başvuru sürecinin kaldığı yerden devam etmesi söz konusu olmadığından, kabul edilebilirlik kriterlerinin sağlanması üzerine kod sahibi tarafından yeni bir başvuru yapılması gerekir. Ulusal davranış kurallarının kabul edilebilirlik kriterlerini karşıladığının tespiti halinde ise, yetkili veri koruma otoritesi tarafından davranış kurallarının içeriği bakımdan tam teşekkülü bir değerlendirmeye geçilir ve içerik değerlendirmesine geçildiği konusunda kod sahiplerine bilgi verilir[153].

Yapılan kapsamlı değerlendirme esnasında, taslak kuralların yerel mevzuatta öngörülen şartları[154] karşılayıp karşılamadığına ilişkin bir kontrol yapılır. Davranış kurallarının içeriğine yönelik değerlendirmelerin olumsuz sonuçlanması durumunda başvuru süreci sona erer. Değerlendirmenin olumlu sonuçlanması ise

[151] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.18.
[152] Bu kriterler, çalışmanın devam eden kısımlarında detaylı olarak açıklanacaktır.
[153] A.g.e., s.17.
[154] A.g.e., s.17.

bu kuralların içerik itibariyle uygun olduğu anlamına gelir. Davranış kurallarının onaylanabilmesi için, bu kuralların uygun bulunması yeterli olmayıp bu kuralları hazırlayan ve code owner *(kod sahibi)* olarak da anılan ilgili birlik veya organların da belirli şartları yerine getirmesi gerekir.

Diğer taraftan, ulusötesi davranış kurallarının kabul edilebilirlik kriterlerini karşıladığının yetkili veri koruma otoritesi tarafından tespiti halinde, bu husus kod sahibi olarak hareket eden taraflara bildirilecektir. İçeriğe yönelik değerlendirme yapılacak bu aşamada, yetkili veri koruma otoritesi ile diğer üye devletlerdeki ilgili veri koruma otoriteleri arasında iş birliği başlayacaktır[155]. Görüldüğü üzere, ulusötesi davranış kurallarının "kabul edilebilirlik kriterleri" bakımından değerlendirilmesi aşamasında ilgili veri koruma otoriteleri sürece dâhil olmazken, içeriğe yönelik bir inceleme yapılacağı aşamada yetkili veri koruma otoritesi ile ilgili veri koruma otoriteleri davranış kuralları hakkında istişare edecektir. Bu durumun sebebi, kabul edilebilirlik kriterlerinin EDPB tarafından yayımlanan rehberlerde tüm üye devletler açısından aynı şekilde düzenlenirken, davranış kurallarının içeriğinin diğer üye devletlerdeki ulusal mevzuat açısından farklı sonuçlar doğurabilecek olması olabilir.

4.3.2.1. Taslak Davranış Kurallarının Kabul Edilebilirlik Kriterleri ve Onay Şartları

Davranış kurallarının içeriğine bakımından detaylı bir analiz ve kontrol yapılmadan önce yetkili veri koruma otoritesi tarafından kabul edilebilirlik kriterleri gözden geçirilir. Bu kriterlerin kontrolü sayesinde daha efektif bir değerlendirme yapılması ve zaman kaybının önüne geçilmesi sağlanmaktadır.

Taslak davranış kurallarının kabul edilebilir olup olmadığının tespitinde, yetkili veri koruma otoritesi tarafından dikkate alınan başlıklar: **(i)** Açıklayıcı Beyan ve

[155] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.19.

Destekleyici Belgeler; **(ii)** Temsil Yetkisi; **(iii)** Maddi Kapsam; **(iv)** Bölgesel Kapsam; **(v)** Yetkili Veri Koruma Otoritesine Başvuru; **(vi)** Mekanizmaların Gözetimi; **(vii)** İzleme Kuruluşu; **(viii)** Danışma; **(ix)** Ulusal Mevzuat; **(x)** Dil; ve **(xi)** Kontrol Listesi, olarak belirtilmiştir.

Bu başlıklar çerçevesinde, taslak davranış kurallarının "kabul edilebilir *(admissible)*" sayılarak onay sürecinin bir sonraki aşamasına geçebilmesi için dikkate edilmesi gereken hususlar ise EDPB tarafından açıklanmıştır. Bu bağlamda, aşağıdaki yer verilen detaylara dikkat edilmesi suretiyle EDPB'nin beklentilerini karşılamak mümkün olacaktır:

(i) Açıklayıcı Beyan ve Destekleyici Belgeler

Taslak davranış kurallarının kabul edilebilirlik şartlarını sağlayabilmesi için hazırlanan davranış kurallarıyla ilgili açıklayıcı, net ve öz beyanlarda bulunulması gerekli görülmektedir. Bir beyanın aynı anda hem yeterince açıklayıcı hem de öz olabilmesi, yapılan açıklamanın saflığın bozabilecek bilgilere yer verilmemesi ile sağlanır. Esasen EDPB bu dengenin nasıl kurulacağı konusunda yönlendirmelerde bulunmuş, sunulacak beyanların taslak davranış kurallarının amacı, kapsamı ve GVK Tüzüğü'ne uyumun temini bakımından bu kuralların sağlayacağı faydaya ilişkin açıklamalara yer verilmesi gerektiğini ifade etmiştir.

EDPB'nin konuya ilişkin rehberinde, açıklayıcı beyanlarda hangi hususlara değinileceğinden bahsederken beyanların belirtilen kapsamda yapılmasının başvuru sürecini hızlanmasına destek olacağı *(assist)* belirtilmiştir[156]. Burada EDPB'nin 'assist' kelimesini tercih etmesi açıklayıcı beyanların kapsamı konusunda esnek bir yaklaşımı olmadığı şeklinde yorumlanabilecekse bile, hemen ardından *"in providing the requisite clarity …"* ifadesi kullanıldığı görülür. Burada EDPB'nin 'requisite' kelimesini tercih etmesi dikkat çekici olup

[156] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.11, p.20.

esnekliğini tekrar sorgulatmaktadır. Açıklayıcı beyanların yanı sıra, bu beyanları ve başvuruyu destekleyici tüm belgelerin de yapılan başvuru dahlinde sunulması beklenmektedir.

(ii) Temsil Yetkisi

Davranış kurallarının uygunluk değerlendirmesine tabi tutulabilmesi için, bu kuralların veri sorumluları veya veri işleyenleri GVK Tüzüğü'nün 40(2) maddesi uyarınca temsil etmeye yetkili kod sahipleri tarafından hazırlanması ve sunulması gerekir. Bunun için üyelerini temsil konusunda ehil olduğunun kod sahibi tarafından yetkili veri koruma otoritesi nezdinde gösterilmesi gerekir. Bir kod sahibinin temsile yetkili kabul edilebilmesi için EDPB tarafından herhangi bir eşik öngörülmediğinden[157], temsil yetkisine ilişkin değerlendirme yapılırken ilgili sektör ve dinamiklerine bağlı olarak farklı parametrelerin dikkate alınacağı anlaşılmaktadır. Ancak her halükarda, temsil edebilirliğin kod sahibi tarafından somut unsurlarla (üye sayısı, sektör ve ilgili veri işleme faaliyeti bakımından sahip olduğu deneyim vb.) ortaya konması gerekir. İlaveten, kod sahibi gerek üyelerinin ihtiyaçlarını gerek de davranış kurallarının etkin uygulaması için ilgili sektör hakkında yeterli bilgi ve anlayışa sahip olduğunu göstermelidir[158].

(iii) Maddi Kapsam

Taslak davranış kurallarının çerçevelediği tüm veri işleme faaliyetlerini ve ilgili faaliyetlerin karakteristiği ile ilgili açık ve net bilgiler içermesi, ayrıca işleme faaliyetlerinin daha etkili yürütülmesi için hazırlanan bu kuralların öngördüğü pratik mekanizmalar ve/veya çözümlere yer verilmesi gerekmektedir.

[157] Lachaud (2019), s.51.
[158] A.g.e., s.51; EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.11-12.

Diğer taraftan, taslak davranış kurallarına konu veri işleme faaliyetlerin hem veri sorumlusu hem de veri işleyen olarak hareket eden taraflarca yürütülebileceğinden, davranış kurallarının bunlardan hangisi tarafından yönetildiği belirtilmelidir[159].

(iv) Bölgesel Kapsam

Davranış kurallarının ulusal veya ulusötesi olarak hazırlanması mümkün olduğundan sunulan taslak kuralların hangi nitelikte olduğunun belirtilmesi ve bölgesel kapsamına ilişkin bilgi verilmesi önemlidir. Bölgesel kapsamı belirtilirken, davranış kuralların hangi yargı bölgelerinde uygulanması öngörülüyor ise tüm ilgili ülkelere yer verilmelidir.

Ulusötesi davranış kurallarının tabi olduğu değerlendirme süreci ulusal davranış kurallarından farklı olduğundan, davranış kuralları birden fazla üye devletteki işleme faaliyetleriyle ilgili olarak hazırlanmış ise tüm ilgili veri koruma otoritelerinin de başvuruda belirtilmesi gerekir[160].

(v) Yetkili Veri Koruma Otoritesine Başvuru

Davranış kurallarının GVK Tüzüğü'nün 55. maddesi kapsamında yetkilendirilen veri koruma otoritesine sunulması gerekir. Aksi halde kabul edilebilirlik şartları sağlanmamış olacaktır. Ulusötesi davranış kuralları söz konusu olduğunda ise birden fazla AB ülkesinin yargı alanına girileceğinden, hangi otoritenin yetkili veri koruma otoritesi kabul edileceğinin belirlenmesi ve bu otoriteye başvuru yapılması gerekecektir[161].

---

[159] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.12.
[160] A.g.e., s.12.
[161] Ulusötesi davranış kuralları için yetkili veri koruma otoritesinin seçimiyle ilgili rehberlik sağlanması adına EDBP tarafından ilgili rehberinin ekinde yönlendirmeler yapıldığı görülür. (A.g.e., Annex-2.)

(vi) Mekanizmaların Gözetimi

Katılma sözleşmesi ile davranış kurallarını kabul eden veri sorumlusu veya veri işleyenlerin GVK Tüzüğü'ne bu kurallara uygun davranıp davranmadığını gözeten mekanizmaların oluşturulması ve bu mekanizmalara davranış kurallarında yer verilmesi gerekmektedir. EDPB, bahsi geçen gözetim mekanizmasının özel sektör veya kamu kuralları olup olmadığına bakılmaksızın tüm davranış kuralları açısından kurgulanması gerektiğinin altını çizmiştir[162]. Bu halde, kamunun sürece dâhil olmasının ilgili mevzuata uyum sağlanması ve sürdürülmesi açısından tek başına yeterli güvenceyi vermediği düşünülmüş olabilir.

(vii) İzleme Kuruluşu

GVK Tüzüğü'nün 41. maddesi uyarınca davranış kuralları kapsamında yetkili veri koruma otoritesi tarafından akredite edilmiş bir izleme kuruluşu atanması gerekir[163]. Bu doğrultuda, davranış kurallarının 'kabul edilebilirlik' olduğunun söylenebilmesi için özel sektör veya kamu için hazırlanmış olan bu kuralların içerisinde izleme kuruluşunun işlevini yerine getirebilmesi için gerekli birtakım mekanizmalar bulunmalıdır[164].

(viii) Danışma

Kod sahibi tarafından davranış kurallarının hazırlanması, değiştirilmesi veya kapsamının genişletilmesi aşamalarında, GVK Tüzüğü Resital 99 uyarınca, davranış kurallarının içeriği hakkında, ilgili paydaşlara (mümkün olması halinde

---

[162] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.12.

[163] Uygulamadaki bir örnekte, davranış kuralların kapsamında henüz akredite edilmiş bir sertifikasyon kuruluşu belirlenmiş olmamasına rağmen ilgili kuralların onaylı hale geldiği görülür. O halde izleme kuruluşunun belirlenmemiş olmasının tek başına taslak davranış kurallarının reddi için yeterli olmadığını, ancak davranış kurallarının teknik olarak onaylanmasına rağmen geçerli etki doğuracak şekilde kullanılabilmesi için akredite izleme kuruluşunun da adreslenmesinin zorunlu olduğu söylenebilir. Bahsi geçen örnek, çalışmanın 4.6. numaralı başlığı altında ele alınacaktır.

[164] A.g.e., s.12-13

kişisel verisi işlenen ilgili kişiler dâhil) danışılır. Bu doğrultuda, hazırlanan taslak davranış kurallarının paydaşlarla istişare edildiğini göstermesi ve gerçekleştirilen istişarenin kapsamına ana hatlarıyla yer vermesi gerekmektedir. Ancak istişarenin kapsamının belirtilmesi tek başına yeterli olmayıp ilgili paydaşların görüşlerinin kod sahibi tarafından ne şekilde değerlendirdiği de belirtilmelidir. Fizibilite eksikliği vb. sebeplerle istişare gerçekleştirilemediği hallerde bu hususun da yapılan başvuru kapsamında makul gerekçeleriyle birlikte açıklanması beklenecektir[165].

(ix) Ulusal Mevzuat

Davranış kurallarının ilgili ulusal mevzuatta yer alan düzenlemelere uygun olduğu kod sahibi tarafından teyit edilmelidir. Bu teyit gerekliliğinin tüm taslak davranış kuralları için geçerli olduğu anlaşılmakla birlikte, ulusal mevzuat ile özel olarak regüle edilen sektörler ve/veya veri işleme faaliyetleri bakımından ayrıca vurgu yapılmıştır[166].

(x)Dil

Ulusal davranış kurallarının yetkili veri koruma otoritesi tarafından öngörülen dil gerekliliklerine uygun olarak, ulusötesi davranış kurallarının ise hem yetkili veri koruma otoritesi tarafından öngörülen dilde hem de İngilizce dilinde hazırlanıp sunulması gerekmektedir[167].

Birden fazla üye ülkeyi ilgilendiren davranış kurallarının evrensel dil olarak kabul edilen İngilizce dilinde de sunulması ile hedeflenen, ulusötesi davranış kurallarının değerlendirilmesinde yetkili veri koruma otoritesi ile ilgili veri koruma otoriteleri arasındaki iş birliğinin desteklenmesi/kolaylaştırılması olabilir.

[165] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.13.
[166] A.g.e., s.13.
[167] A.g.e., s.13.

(xi) Kontrol Listesi

Taslak davranış kurallarının bir sonraki değerlendirme aşamasına geçip geçmeyeceği konusunda nihai karar yetkili veri koruma otoritesi tarafından verilecekse bile, başvuru yapılmadan önce başvuruda sunulacak bilgi ve belgelerde eksiklik olmadığına ilişkin kontrollerin Kontrol Listesi[168] üzerinden yapılması gerekir. Bu sayede yetkili veri koruma otoritesinin işi kolaylaşacağı gibi, yapılan başvuruların tam olsa kabul edilebilir olacak iken bilgi/belge eksikliği sebebiyle reddedilme ihtimali de ortadan kalkacaktır.

Yukarıda detaylarına yer verilen kabul edilebilirlik kriterlerinin yanı sıra, davranış kurallarının onaylanabilmesi için bu kuralları hazırlayan ilgili birlik veya diğer organlarca mevcudiyeti ortaya konulması gereken diğer hususlar, başka bir deyişle sağlanması gereken şartlar[169], aşağıdaki şekildedir:

- **(i)** Davranış kurallarının GVK Tüzüğü'nün daha kolay uygulanmasına imkân sağlaması
- **(ii)** Davranış kuralları içerisinde GVK Tüzüğü'nün uygulanması bakımından açık, net ve pratik[170] çözümlere yer verilmesi
- **(iii)** Davranış kuralları sayesinde bu kuralların ilgili olduğu sektör veya işleme faaliyeti bakımından mevcut bir soruna ilgili tüm paydaşlar açısından efektif bir çözüm getirilmesi
- **(iv)** Davranış kurallarının kişisel verilerin işlenmesi ve bireylerin hak ve özgürlükleri ile ilgili risklerin azaltılması için yeterli nitelikte önlemler içermesi

---

[168] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* - Annex-3.

[169] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.14

[170] EDPB'ye göre, taslak davranış kurallarının, açık ve net olmanın yanı sıra, somut ve test edilebilir (uygulanabilir) niteliği haiz olması gerekmektedir. Bununla birlikte, EDPB tarafından, davranış kurallarının GVK Tüzüğü'nün ilgili maddelerinin patik ve etkin bir uygulanmasıyla sınırlı olmadığına dikkat çekildiği görülmektedir. Bu doğrultuda, davranış kuralları hazırlanırken, bu kurallarının ilgili olduğu sektör veya işleme faaliyeti hakkında daha önceden EDPB tarafından verilmiş olan kararların da dikkate alınması beklenmektedir. (A.g.e., s.15-16).

(v) Davranış kurallarına uygun davranıldığının takibi için etkin izleme mekanizmalarının bulunması

4.3.3. Ulusötesi Kuralların İçeriği Bakımından İlgili Veri Koruma Otoriteleri İle İşbirliği Yapılması

Veri koruma otoriteleri arasında iş birliğinin varlığından bahsedebilmek için, birden fazla veri koruma otoritesinin mevcudiyeti kaçınılmazdır. Birden fazla veri koruma otoritesinin varlığı yalnızca ulusötesi davranış kuralları açısından söz konusu olacağından, bu başlık altında yer verilen açıklamalar yalnızca ulusötesi davranış kurallarının onay süreci bakımından dikkate alınmalıdır.

Bilindiği üzere, davranış kurallarının kabul edilebilirlik kriterlerini karşıladığının tespiti üzerine, bir sonraki aşamaya geçilecek ve içeriğe yönelik değerlendirme yapılacaktır. Bu aşamada yetkili veri koruma otoritesi ile diğer üye devletlerdeki ilgili veri koruma otoriteleri arasında iş birliği başlayacaktır. Yetkili veri koruma otoritesi, AB üyesi devletlerdeki tüm veri koruma otoritelerine yapacağı bir bilgilendirme ile davranış kurallarının onay süreciyle ilgili olan veri koruma otoritelerinin hangileri olduğunu belirtecektir. Bunun üzerine ilgili veri koruma otoriteleri tarafından, gönüllülük esasına dayalı olarak, taslak davranış kurallarının esasa ilişkin değerlendirilmesi mümkün olacak ve bu bağlamda yetkili veri koruma otoritesine yardım etmek üzere "ortak değerlendirmeci" talep edilebilecektir. Talep edilecek "ortak değerlendirmeci" sayısı en fazla iki olup bu değerlendirmecilerden, ilk gelenlere öncelik tanınmak suretiyle yetkili veri koruma otoritesi tarafından bir seçim yapılacaktır.

Yetkili veri koruma otoritesi ile iş birliği içerisinde hareket edecek ortak değerlendirmeciler, seçildikleri tarihten itibaren 30 gün içerisinde taslak davranış kurallarıyla ilgili yorumlarını yetkili veri koruma otoritesine iletir. Taslak davranış kurallarının, GVK Tüzüğü madde 63'te belirtilen prosedür kapsamında yetkili veri koruma otoritesi tarafından EDPB'nin görüşüne sunulup sunulmayacağı

konusunda nihai karar alma yetkisi yetkili veri koruma otoritesine ait olmakla birlikte, yetkili otorite tarafından yapılacak değerlendirme esnasında ortak değerlendirmecilerin kendisiyle paylaştığı yorumlar da dikkate alınır[171].

Nihai kararını veren yetkili veri koruma otoritesinin taslak davranış kurallarına yönelik değerlendirmelerinin olumsuz sonuçlanması halinde, başvuru süreci sona erer. Böyle bir durumda, ilgili veri koruma otoritelerine de davranış kurallarının reddedildiğine ilişkin bilgilendirme yapılması gerekmektedir[172]. Görüldüğü üzere, bu bildirim, diğer bildirimlerden farklı olarak, yalnızca davranış kuralları onay süreciyle ilgili olduğu kabul edilen veri koruma otoritelerine yapılır. Zira yetkili veri koruma otoritesi tarafından ortak değerlendirmeci seçim süreci işletilmeden önce AB üye devletlerindeki tüm veri koruma otoritelerine yapılan bildirim ile, ilgili veri koruma otoritelerinin hangileri olduğu açıklanmaktadır. Yapılan değerlendirmeler sonucunda yetkili veri koruma otoritesinin davranış kurallarını uygun bulması halinde ise, bu kurallar yetkili veri koruma otoritesi tarafından EDPB'nin görüşüne sunulur.

4.3.4. Taslak Davranış Kuralların Onaylanması

Taslak mahiyetindeki ulusal davranış kurallarının kabul edilebilirlik kriterleri ile çalışmanın kabul edilebilirlik kriterlerini içeren ilgili alt başlığında öngörülen ilave şartları taşıdığının tespiti üzerine, yetkili veri koruma otoritesi davranış kurallarının yerel mevzuata uygun olup olmadığının tespiti için bir değerlendirmeye başlar. Yapılan değerlendirme kapsamında davranış kurallarının yerel mevzuata uygun olduğunun görülmesi halinde, davranış kuralları GVK Tüzüğü madde 40(5) uyarınca yetkili veri koruma otoritesi tarafından onaylanır. Aynı madde tahtında, onaylanan davranış kurallarının yetkili veri koruma otoritesi tarafından kamuoyuna açık bir şekilde yayımlanması gerektiği de düzenlenmiştir.

[171] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.17.
[172] A.g.e., s.19.

Çalışmanın önceki kısımlarında yer yer değindiğimiz üzere, ulusal davranış kurallarının onaylanması prosedürü ulusötesi davranış kurallarında farklıdır.

Ulusal davranış kurallarının yolculuğuysa, yetkili veri koruma otoritesinde başlar, devam eder ve sonlanır. Bu yolculuğun aşamaları, baştan sona sırasıyla; taslak kuralların ibrazı, kabul edilebilirlik değerlendirmesine tabi tutulması, yerel mevzuata uygunluk değerlendirmesine tabi tutulması ve son olarak davranış kurallarının onaylanması ve kamu açık olarak ilan edilmesidir.

Ulusal davranış kuralları aksine, ulusötesi davranış kuralları ile ilgili onay prosedürü ise yalnızca yetkili veri koruma otoritesi nezdinden yürütülmez[173]. EDPB ve Komisyon da sürece dâhil edilir. Bu bağlamda, ulusötesi davranış kurallarının yetkili veri koruma otoritesi tarafından EDPB'ye sunulması üzerine EDPB'nin değerlendirmesi başlar. EDPB, taslak davranış kurallarının (veya mevcut davranış kuralların değiştirilmesi veya kapsamının genişletilmesi ile ilgili düzenlemelerin) GVK Tüzüğü'ne uyumlu olup olmadığı ya da 40. maddenin 3. fıkrasında atıfta bulunulan durumda[174], davranış kurallarının "uygun güvenceler" içerip içermediğini değerlendirir.

Yapılan değerlendirmenin sonunda EDPB, davranış kurallarında yapılması gereken değişikliklere ilişkin görüşünü yetkili veri koruma otoritesiyle paylaşabileceği gibi, davranış kurallarının onaylanması konusunda destekleyici

[173] Voigt & Von dem Bussche (2017), s.74.

[174] Burada bahsi geçen; GVK Tüzüğü'nün bölgesel kapsamını düzenleyen 3. maddesine tabi olmayan, başka bir deyişle AEA bölgesi dışındaki üçüncü ülkelerde bulunan, veri sorumluları veya veri işleyenlerin davranış kurallarına uyma taahhüdü verdiği hallere ilişkindir. Zira code owner (kod sahibi) olarak anılan taraflarca hazırlanan davranış kurallarına, yalnızca GVK Tüzüğü'nün 3. maddesinde sayılan veri sorumluları veya veri işleyenlerin değil, aynı zamanda GVK Tüzüğü'nün bölgesel kapsamı içerisinde kalmayanlar tarafından da kişisel verilerin aktarılması bakımından GVK Tüzüğü'nün 46(2) maddesinin (e) bendi uyarınca bağlı kalınması mümkündür. Ancak GVK Tüzüğü'nün 40(3) maddesi, üçüncü ülkelerdeki veri sorumlusu veya veri işleyenlerin onaylı davranış kurallarına katılabilmesi için birtakım şartlar getirmiştir. Buna göre; ilgili veri sorumlusu veya veri işleyen tarafından, sözleşme veya yasal olarak bağlayıcılık teşkil eden sair enstrümanlar aracılığıyla, GVK Tüzüğü'nün 46(1) maddesi uyarınca "yeterlilik kararı bulunmayan hallerde üçüncü ülkelere kişisel veri aktarılabilmesi için alınması gereken önlemler"in uygulanacağına ilişkin, bağlayıcı ve uygulanabilir taahhütler verilmesi zorunludur.

görüş de paylaşabilir. Davranış kurallarının GVK Tüzüğü'ne uyumlu olduğunun veya GVK Tüzüğü'nün 40. maddesinin 3. fıkrasında atıfta bulunulan durumda davranış kurallarının "uygun güvenceler" içerdiğinin tespit edildiği hallerde, EDPB tarafından bir destekleyici görüş paylaşılır. Davranış kurallarına ilişkin destekleyici görüş paylaşılması üzerine yetkili veri koruma otoritesi ulusötesi davranış kurallarını onaylar ve bu hususta davranış kuralları ile ilgili veri koruma otoritelerini bilgilendirir.

EDPB tarafından destekleyici görüş paylaşılmayan durumlarda ise, EDPB ilgili davranış kurallarında yapılması gereken değişikliklere ilişkin görüşünü yetkili veri koruma otoritesine iletecektir.

4.3.5. Onaylı Davranış Kurallarının Komisyon'a Sunulması

Ulusötesi davranış kurallarının GVK Tüzüğü'ne uygun olduğunun veya bu kuralların GVK Tüzüğü madde 40/3'te atıfta bulunan AEA dışında kalan ülkelere (başka bir ifadeyle, üçüncü ülkelere) aktarım yapılan hallerde yeterli uygun güvencelerden olduğunun EDPB tarafından tespiti üzerine, EDPB konuya ilişkin destekleyici görüşünü Komisyon'a iletmekle yükümlüdür. GVK Tüzüğü'nün 40. Maddesinin 8. paragrafı gereğince Komisyon'a yapılacak bu bildirime istinaden, Komisyon[175] tarafından, kendisine ibraz edilen davranış kurallarının Avrupa Birliği içerisinde **"genel geçerliliğe"** sahip olduğu yönünde bir karar vermesi[176] mümkündür. İlgili maddede Komisyon'un genel geçerlilik kararı vermesi bakımından *"may decide*" ifadesi kullanıldığı görülmektedir. Bu ifadeden hareketle, EDPB tarafından destekleyici bir görüş sunulmuş olmasına

[175] Komisyon'un inceleme usulü için bkz. GVK Tüzüğü, madde Article 93(2).

[176] GVK Tüzüğü madde 40/9 uyarınca, bu karar uygulama tasarrufu[176] yoluyla verilecektir. Uygulama tasarrufları ("implementing acts"), Avrupa Birliği nezdinde bağlayıcı niteliği haiz olan yasama tasarruflarının, tüm üye devletlerde yeknesak uygulanmasına yönelik ayrıntıları içeren yasama dışı düzenlemelerdir. Detaylı bilgi için bkz. https://www.consilium.europa.eu/en/council-eu/decision-making/implementing-and-delegated-acts/#:~:text=An%20implementing%20act%20is%20a,of%20legally%20binding%20Union%20acts

bakılmaksızın, Komisyon tarafından davranış kurallarının genel geçerliliğe sahip olmadığı yönünde de karar verilebilecektir.

GVK Tüzüğü'nün 40/9 maddesi uyarınca, genel geçerliliğe sahip olduğuna karar verildiği onaylı davranış kuralları Komisyon tarafından yayımlanır. Bununla birlikte Komisyon, onaylı tüm davranış kurallarını bir sicilde toplar ve bunları uygun yollarla kamuoyuna açıklar.

4.4. ONAYLI DAVRANIŞ KURALLARININ İZLENMESİ

Davranış kurallarının onaylı hale gelebilmesi için, bu kurallarına katılan üyelerin GVK Tüzüğü'ne uyumluluğun etkili ve sürekli bir şekilde izlenmesine imkân veren, GVK Tüzüğü gereklerinin ihlali halinde ise, söz konusu ihlalin ortadan kaldırılması için ilgili üye tarafından alınması gereken aksiyonları içeren düzenlemelere yer vermesi gerekir. Başka bir deyişle, davranış kurallarının onaylı hale gelebilmesi için, davranış kuralları hazırlanırken bu kurallara uyumluğu izleyip takip etmeye yetkili izleme kuruluşları ile ilgili düzenlemelere yer verilmesi şarttır. Onaylı davranış kurallarının izlenmesinden sorumlu olan ve "izleme kuruluşu" olarak adlandırılan organ, GVK Tüzüğü'nün 41(1) maddesinde düzenlenmiştir. Bu düzenlemeye göre, GVK Tüzüğü'nün 40. maddesinde öngörülen gereklilikler doğrultusunda onaylanmış olan davranış kuralları, kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan ve davranış kurallarına uyumluluğun izlenmesi amacına yönelik olarak yetkili veri koruma otoritesi tarafından akredite edilen bir kuruluş tarafından izlenebilir. İzleme kuruluşu, bir organı/komiteyi ifade edilebileceği gibi birden fazla organı/komiteyi de ifade edebilir.

4.4.1. İzleme Kuruluşunun Özellikleri

Veri sorumlusu veya veri işleyen tarafından kabul edilmiş olan davranış kurallarına bağlılık taahhüdü tek başına yeterli görülmemektedir. Zira GVK

Tüzüğü, bu bağlılığın sürekli olarak devam etmesi ve bu sürekliliğin ortaya konması adına ayrıca bir izleme mekanizması öngörmüştür. Bu mekanizmanın en önemli aktörü, davranış kurallarına uygun davranılıp davranılmadığını gözetmekten sorumlu izleme kuruluşudur.

İzleme kuruluşunun davranış kurallarına katılan ilgili veri sorumlusu veya veri işleyen bünyesinde dâhili olarak veya haricen kurulması mümkündür. Burada önem arz eden husus, izleme kuruluşunun bu kuralları hazırlayan ilgili birlik veya diğer bir organ -yani kod sahibi- nezdinde değil, kod sahibi tarafından hazırlanan kurallara uygun davranmayı taahhüt eden veri sorumluları veya veri işleyenler -yani birlik üyeleri- nezdinde kurulması gerektiğidir. Öte yandan, dâhili veya harici izleme kuruluşlarından hangisinin kullanılacağı konusunda karar verme yetkisi davranış kurallarını oluşturan ilgili birlik veya organda olmaya devam edecektir[177].

Gerek özel sektörde faaliyet gösteren kuruluşlar gerek kamu kuruluşları için hazırlanan davranış kurallarının, bu kurallarına uygunluğun izlenmesi için bazı etkili mekanizmalar getirmesi gerektiği görülür zira bunun aksine bir düzenleme ilgili mevzuatta yer almamaktadır. Ancak EDPB tarafından hazırlanan yönlendirici rehbere bakıldığında, yalnızca özel (kamu-dışı) kuruluşlar için öngörülenler mekanizmaların GVK Tüzüğü'nün 41. maddesindeki gerekliliklere uygun olarak kurgulanmasının zorunlu olduğu anlaşılmaktadır[178]. O halde; kamu kuruluşları tarafından kabul edilen davranış kurallarına uygunluğun takibinin bakımından da bir izleme mekanizmasının gerekli görüldüğü, ancak bu hususta özel sektörde faaliyet gösteren kuruluşlara kıyasla kamu kuruluşlarına bir miktar daha esneklik sağlandığı düşünülebilecektir.

[177] Bkz. EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.21.
[178] A.g.e., s.12-13.

4.4.2. İzleme Kuruluşunun Yetkileri

GVK Tüzüğü uyarınca davranış kurallarına uygun davranılıp davranılmadığının takibinden sorumlusu olan izleme kuruluşu, yetkili veri koruma otoritesi tarafından akredite edilmiş olmalıdır. Dolayısıyla, yetkili veri koruma otoritesi tarafından GVK Tüzüğü'nün 41(1) maddesinde belirtilen kapsamda akredite edilmeyen kuruluşların izleme faaliyetlerinin yürütülmesi bakımından yetkili olduğunu söylemek mümkün olmayacaktır.

Davranış kurallarının veri sorumlusu veya veri işleyen tarafından ihlal edildiğinin tespiti halinde, izleme kuruluşlarının sahip olduğu yetkiler GVK Tüzüğü'nün 41(4) maddesinde düzenlenmiştir. Buna göre; yetkili izleme kuruluşu tarafından davranış kurallarının ihlal edildiğinin tespit edilmesi durumunda, izleme kuruluşu uygun güvencelere tabi olarak ilgili veri sorumlusu veya veri işleyen hakkında gerekli gördüğü şekilde işlem yapabilecektir. Bu işlemler eğitim veya uyarı verilmesiyle sınırlı kalabileceği gibi, davranış kurallara katılan ilgili veri sorumlusu veya veri işleyenin davranış kurallarını hazırlayan birlik veya sair organ nezdindeki üyeliğinin askıya alınması veya ilgili veri sorumlusu veya veri işleyenin davranış kurallarından çıkarılmasına kadar gidebilir[179]. GVK Tüzüğü'nün 41. maddesinin 4. fıkrasında, davranış kurallarının ihlali halinde izleme kuruluşu tarafından 'gerekli olan' aksiyonların alınacağı düzenlediğinden, veri sorumlusu veya veri işleyen hakkında yapılacak işlem veya alınacak aksiyonlar ile ilgili kararların akredite izleme kuruluşunun takdirinde olduğu anlaşılmaktadır. Aynı fıkranın devam cümlesinde, izleme kuruluşu tarafından alınan aksiyonların gerekçeleri hakkında yetkili veri koruma otoritesine bilgilendirme yapılacağı düzenlenmiştir. Buradan, alınan aksiyonların makul gerekçelere dayanıp dayanmadığına ilişkin yetkili veri koruma otoritesinin değerlendirilmesine veya teyidine başvurulmadığı anlaşılmaktadır.

[179] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.24.

4.4.3. İzleme Kuruluşunun Akredite Edilmesi

GVK Tüzüğü'nün 41. maddesi kapsamında bir izleme kuruluşunun varlığından söz edilebilmesi için, izleme kuruluşunun yetkili veri koruma otoritesi tarafından akredite edilmiş olması şarttır. Akreditasyon için; yetkili veri koruma otoritesi tarafından hazırlanan ve EDPB tarafından onaylanmış akreditasyon şartlarının karşılanması gerekir.

Yetkili veri koruma otoritesi tarafından hazırlanan akreditasyon şartları taslak niteliğini haiz olup bu şartların izleme kuruluşunun akreditasyon sürecinde uygulanmasından önce, GVK Tüzüğü'nün 63. maddesinde anılan "tutarlılık mekanizması" gereğince EDPB tarafından onaylanması beklenmektedir[180]. Hazırlanan akreditasyon şartları, AB üye devletlerindeki veri koruma otoriteleri arasında farklılık gösterebilecekse EDPB onayının öngörülmesi ile birlikte, bu şartlar arasında tutarsızlık olmasının önüne geçilmiştir.

4.4.3.1. Akreditasyon Kriterleri

GVK Tüzüğü'nün 41. maddesinin 1. ve 2. fıkraları uyarınca bir izleme kuruluşunun akredite edebilmesi için **(i)** bağımsız olması; **(ii)** davranış kurallarının konusu ile ilgili uygun bir uzmanlık seviyesine sahip olması; **(iii)** görev ve sorumluluklarının çıkar çatışması yaratmayacak olması; ve **(iv)** gerekli prosedür ve yapıların kurgulamış olması *(veri koruma otoriteleri ile iletişim, şeffaf şikayet yönetimi, gözetim/izleme ve izleme kuruluşunun statüsü ve kaynakları ile ilgili düzenlemeler dahil)* gerekmektedir.

Bir izleme kuruluşunun akredite edilebilmesi için yukarıdaki şartları eksiksiz olarak sağlaması ve akreditasyon süresi boyunca sağlanmaya devam etmesi beklenir. Görüldüğü üzere ilgili kriterlerin bir kısmı izleme kuruluşunun sahip

[180] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.21.

olması gereken niteliklere ilişkin iken, diğerleri ise izleme kuruluşunun kontrolünde yürütülecek süreçler bakımından davranış kurallarında yer verilen mekanizmaların etkili olmasıyla ilgilidir. İzleme kuruluşlarının GVK Tüzüğü'ne uygun akreditasyonu için aranan bu kriterler, aşağıda ilgili başlıklar altında detaylı olarak ele anılacaktır.

4.4.3.1.1. İzleme Kuruluşunun Bağımsız Olması

İzleme kuruluşunun "bağımsız" olmasından kasıt; izleme kuruluşunun, davranış kurallarına katılan veri sorumluları veya veri işleyenler ile davranış kurallarının geçerli olduğu ilgili meslek, endüstri veya sektöre karşı tarafsız olmasıdır[181]. Bununla birlikte, pratikte bağımsızlıktan söz edilebilmesi için izleme kuruluşunun tarafsız olmanın yanı sıra, izleme kuruluşunun herhangi bir talimata bağlı olmaksızın hareket edebilmesi ve bağımsızlığını zedeleyebilecek her türlü üçüncü taraflar müdahalesinden korunması gerekmektedir[182].

Bağımsızlık; yalnızca izleme kuruluşu akredite edilene kadar değil, akreditasyon sonrasında da mevcut olmalıdır. Bu bağlamda, izleme kuruluşunun tarafsız ve bağımsız konumunu olumsuz etkileme riski olan hususlar izleme kuruluşu tarafından devamlı olarak değerlendirilmeli ve böyle bir riskin tespiti halinde riskin bertaraf edilebilmesi için gerekli tüm aksiyonlar alınmalıdır[183].

Bütçe ve finansman yönetimi, personel/üye atanması, karar alma süreçleri gibi konuların organizasyonun diğer alanlarından ayrışmış olması da izleme kuruluşunun bağımsızlığını ortaya koyabilecek yöntemler arasındadır. Bu bağlamda EDPB, bir izleme kuruluşunun görev ve sorumluluklarını yerine getirirken finansal destek alması halinde, başlı başına bu durumu izleme

[181] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.21.
[182] İzleme kuruluşunun bağımsızlık bakımından GVK Tüzüğü'nde düzenlenen Veri Koruma Görevlisi (DPO) ile benzerlik gösterdiği söylenebilir.
[183] A.g.e., s.22.

kuruluşunu finansal istikrara sahip olmadığı ve/veya yeterli kaynaklara sahip olmadığı dolayısıyla da bağımsız olmadığı şeklinde yorumlamaz.

4.4.3.1.2. İzleme Kuruluşunun Uzmanlık Sahibi Olması

İzleme kuruluşunun, davranış kurallarının ilgili olduğu sektör veya veri işleme faaliyeti ile yürürlükte olan kişisel veri koruma mevzuatı bakımından, görev ve sorumluluklarını etkili bir şekilde yerine getirebilecek düzeyde bilgi ve tecrübeye sahip olması gerekmektedir. Bunun yanı sıra, akreditasyon kriterlerine uygunluğu değerlendirilen izleme kuruluşunun personellerinin de davranış kurallarına uygunluğu izlenme usulleri hakkında operasyonel deneyime ve eğitime sahip olması gerekir[184].

4.4.3.1.3. Çıkar Çatışması İmkanı Bulunmaması

İzleme kuruluşunun, görev ve sorumluluklarıyla bağdaşmayan ve çıkar çatışması olarak değerlendirilebilecek her türlü eylemden kaçınması ve bu tür eylemlerden kaçınabilmek adına gerekli önlemleri alması gerekmektedir[185]. Örneğin; izleme kuruluşunun herhangi bir üçüncü taraftan talimat alması, görev ve sorumluluklarıyla bağdaşmamaktadır. Bu yönüyle, bağımsızlık ile ilgili kriter ve çıkar çatışması ile ilgili kriter arasında bir korelasyon olduğu söylenebilir.

4.4.3.1.4. Gerekli Prosedür ve Yapıların Mevcut Olması

İzleme kuruluşunun akredite edilebilmesi için GVK Tüzüğü'ne uyumlu davranılmasına imkan veren ve hatta buna hizmet eden çeşitli prosedür ve yapıların bulunması gerekir. Bu prosedür ye yapılar; veri koruma otoriteleri ile

[184] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.23.
[185] A.g.e., s.22.

iletişim, şeffaf şikayet yönetimi, gözetim/izleme süreçleri ve izleme kuruluşunun statüsü ve kaynakları[186] gibi çok çeşitli konuları düzenleyebilecektir. Her bir konu özelinde dikkat edilmesi gereken hususlar, aşağıda ayrı ayrı ele alınacaktır.

İzleme kuruluşunun, *"ilgili veri sorumluları veya veri işleyenlerin davranış kurallarının uygulanması bakımından gerekli yeterliliğe sahip olup olmadığını"* değerlendirme sorumluluğu vardır. Bu doğrultuda, izleme kuruluşu tarafından üyelerin yeterliliği hakkında değerlendirme yapılabilmesi için etkili prosedür ve yapılar mevcut olmalıdır[187]. Zira gerekli yeterliliğe sahip olmadığı değerlendirilen veri sorumluları/veri işleyenlerin davranış kurallarından faydalanması mümkün olmayacaktır. Diğer taraftan, izleme kuruluşunun etkili bir yönetişim yapısına sahip olması gerekmektedir. Ayrıca, davranış kuralları formüle edilirken ilgili izleme kuruluşunun GVK Tüzüğü, m. 41(4) kapsamındaki rolünü yerine getirmek için uygun statü ve yetkinliklere[188] sahip olduğunun gösterilmesi önemlidir.

İzleme kuruluşları tarafından, veri sorumları veya veri işleyen tarafından *davranış kurallarına uygun davranılmasının sağlanması, uygunluğun izlenmesi ve davranış kurallarının nasıl işlediğinin düzenli bir şekilde gözden geçirilmesi* gerekir. Bu adımların zincir halkaları gibi birbirlerini tamamladığı düşünüldüğünde, yalnızca bir halkanın dahi yeterli ölçüde ele alınmaması, GVK Tüzüğü'ne eksiksiz bir şekilde uyum sağlanamaması sonucunu doğurabilir. Bunun önüne geçebilmek adına, izleme kuruluşunun, davranış kurallarına uyumun temini için etkili prosedür[189] ve yapılar oluşturması gerekir.

---

[186] Burada kast edilen izleme kuruluşunun görevlerini yerine getirebilmek için yeterli personel ve kaynaklara sahip olması gerektiğidir.

[187] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.23.

[188] Bu ifadeden kasıt, izleme kuruluşunun GVK Tüzüğü'nün 41(4) maddesi kapsamındaki rolünü yerine getirebilmesi ve Madde 83(4)-(c) uyarınca para cezasına hükmedilmesi anlamına gelmektedir.

[189] Bir veri sorumlusu veya veri işleyenin davranış kurallarına aykırı hareket ettiği hallerde izleme kuruluşuna "düzeltici önlemler" alma yetkisi (davranış kurallarını askıya alma, kuralların dışına çıkan taraflara duruma göre eğitim, uyarı verme veya aykırılığı gidermesi için kesin mehil verme, ilgili tarafları üst yönetime raporlama veya davranış kurallarından çıkarma vs.) verilmiş olması, EDPB'ye prosedürlerin 'etkili' olduğu şeklinde yorumlanacaktır. (EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.24)

Davranış kurallarının yürürlükte olan mevzuat ve/veya bilgi teknolojilerindeki gelişmelere rağmen güncel ve uygulanabilir kalmasını teminen *gözetim mekanizması* oluşturulması da oldukça önemlidir. Her hâlükârda izleme kuruluşları tarafından prosedür hazırlanırken davranış kurallarına konu olan sektör ve/veya veri işleme faaliyeti özelinde değerlendirme yapılmalı ve bu kapsamda tespit edilen olası risklerin bertafını ya da minimazyonunu sağlayan mekanizmalara yer verilmelidir[190].

İzleme kuruluşunun sorumluluk alanındaki konuların veri sorumlusu veya veri işleyenleri etkileyen boyutları olduğu gibi, üçüncü tarafları etkileyen boyutları da bulunur. Dolayısıyla mevcut prosedür ve yapılar; davranış kurallarına ile ilgili şikâyetlerin ne şekilde ele alınacağına dair net düzenlemeler *ile şikayet sürecinin tarafsız ve şeffaf yürütülmesini* temin eden mekanizmalar da içermelidir[191]. Bununla birlikte, izleme kuruluşu ve yetkili veri koruma otoritesi arasında davranış kurallarının gereği gibi uygulanması adına, taraflar arasındaki olası iletişimler için etkin bir iletişim mekanizmasının kurulması sağlanmalıdır[192].

4.4.4. İzleme Kuruluşunun Akreditasyonunun Kaldırılması

Nasıl ki davranış kurallarına uygun davranmadığının tespiti halinde izleme kuruluşunun veri sorumlusu veya veri işleyenler hakkında işlem yapması ve bu kapsamda davranış kurallarını askıya alması veya iptal etmesi mümkün olabiliyor ise; aynı şekilde davranış kurallarının uygulanmasından sorumlu akredite izleme kuruluşuna verilen yetkinin de belli koşullarda ortadan kaldırılması mümkündür. İzleme kuruluşuna verilen akreditasyonun hangi şartlarda kaldırılacağı GVK Tüzüğü'nün 41(5) maddesinde ele almaktadır. İlgili maddeye göre, akreditasyon

[190] Bu mekanizmalara EDPB tarafından verilen örneklerden bazıları; rastgele veya habersiz denetimler, yıllık teftişler, düzenli raporlama ve anketlerin kullanımıdır. Bkz. A.g.e., s.23.
[191] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, s.24.
[192] A.g.e., s.25.

kriterlerinin sağlanamaması veya sağlanamamaya başlanması, izleme kuruluşuna verilen akreditasyonun kaldırılması için yeterli olacaktır. Bununla birlikte, akreditasyon şartlarını sağlayıp sağlamadığına bakılmaksızın, izleme kuruluşu tarafından GVK Tüzüğü'nün ihlal edilmesi halinde de bu kuruluşa verilen akreditasyon yetkili veri koruma otoritesi tarafından kaldırılır.

4.5. YURT DIŞINA VERİ TRANSFERLERİ BAKIMINDAN DAVRANIŞ KURALLARI

Davranış kuralları, başlangıçta salt GVK Tüzüğü'nün 40. maddesinin 2. paragrafı uyarınca kişisel veri transferleri ile ilgili düzenlemeler içermeyecek şekilde hazırlanabileceği gibi[193], aynı maddenin 3. fıkrası kapsamında doğrudan transferlere ilişkin düzenleme içerecek şekilde (transferlere yönelik davranış kuralları şeklinde) de hazırlanabilir. Bununla birlikte, başlangıçta kişisel verilerin transferleriyle ilgili herhangi bir düzenleme içermeyecek şekilde hazırlanan GVK Tüzüğü Kuralları'nın[194] kapsam bakımından genişletilerek içerisine veri transferlerine ilişkin düzenlemeler eklenmesi suretiyle oluşturulması da mümkündür[195].

GVK Tüzüğü'nün 5. bölümü (Madde 44 - Madde 50 arası) kişisel verilerin üçüncü ülkelere[196] ve uluslararası organizasyona aktarılabilmesinin şartlarını düzenlemektedir. Madde 44'e göre, üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri transferi yapılabilmesi için Komisyon tarafından verilen bir yeterlilik kararı olması gerekir. Komisyon tarafından verilen bir yeterlilik kararı[197] bulunmayan hallerde kişisel verilerin üçüncü ülkelere ve uluslararası

[193] Bu şekilde hazırlanan kurallar, çalışmanın devam eden kısımlarında "GVK Tüzüğü Kuralları" olarak anılacaktır.
[194] "GVK Tüzüğü Kuralları" ile ilgili açıklama için bkz. dn.192.
[195] Özetle, ister GVK Tüzüğü Kuralları şeklinde oluşturulup sonradan içerisinde veri transferleriyle ilgili ekleme yapılmış olsun ister de başlangıçta transferlere ilişkin düzenleme içerecek şekilde hazırlanmış olsun, kişisel verilerin üçüncü ülkelere aktarımı bakımından düzenleme öngören davranış kuralları "Transferler İçin Tasarlanan Davranış Kuralları" olarak anılabilecektir.
[196] GVK Tüzüğü'nün bölgesel kapsama ilişkin 3. maddesine göre Tüzüğe tabi olmayan ülkelerdir.
[197] Bkz. GVK Tüzüğü m. 45.

organizasyona hangi şartlarda aktarılabileceği GVK Tüzüğü'nün 46. maddesinde düzenlenmiş olup bu madde düzenlenen hallerde veri aktarımlarının gerçekleştirilebilmesi için birtakım uygun güvencelerin bulunması zorunlu kılınmıştır. Aynı maddenin 2. fıkrasının (e) bendinde ise, yetkili veri koruma otoritesinden ayrıca bir izin alınmaksızın üçüncü ülkelere veya uluslararası organizasyonlara veri aktarımı yapılması için alınması gereken güvenceler arasında; *"yetkili veri koruma otoritesi tarafından onaylanan ve Komisyon tarafından AB içinde* ***genel geçerliliği*** *olduğuna karar veren davranış kuralları ile birlikte ilgili kişilerin hakları da dâhil olmak üzere uygun güvenlik önlemlerinin alınacağına dair üçüncü ülkedeki veri sorumluları veya veri işleyen tarafından verilen bağlayıcı ve uygulanabilir taahhütler"* sayılmıştır. Nitekim, GVK Tüzüğü'nün 40(3) maddesinde de, yetki veri koruma otoritesi tarafından onaylanan ve Komisyon tarafından AB içinde *genel geçerliliği* olduğuna karar veren davranış kurallarına, yasal olarak bağlayıcı ve uygulanabilir taahhütler vermeleri kaydıyla, üçüncü ülkelerde bulunan veri sorumluları veya veri işleyenler tarafından da tabi olunabileceği belirtilmektedir. Transferler İçin Tasarlanan Davranış Kuralları[198], genellikle AB üyesi birden fazla devlet tarafından üçüncü ülkere yapılacak aktarımları düzenlediğinden, bu kurallar çoğunlukla "ulusötesi" niteliğini haiz olacaktır. Transferler İçin Tasarlanan Davranış Kuralları'nın "ulusötesi" olarak nitelendirilmesinin bir diğer sebebi ise, bu kuralların *genel geçerliliğe* sahip olmak zorunda olması, dolayısıyla kuralların onay aşamasında EDPB ve Komisyon'un da sürece dâhil olmasıdır[199].

Üçüncü ülkede yerleşik bir veri alıcısının (veri ithalatçısının), GVK Tüzüğü'nün 40(3) maddesindeki koşulları sağlamak suretiyle Transferler İçin Tasarlanan Davranış Kuralları'na katıldığı senaryoda, bu kurallar tahtında GVK Tüzüğü'ne uygun bir aktarımdan bahsedilebilmesi için, AEA'da yerleşik veri ihracatçısı tarafından Transferler İçin Tasarlanan Davranış Kuralları'na bağlılık

[198] "Transferler İçin Tasarlanan Davranış Kuralları" ile ilgili açıklama için bkz. dn.189.
[199] EDPB. *Guidelines 04/2021 on Codes of Conduct as tools for transfers*, s.7.

taahhüdü verilmesi aranmaz[200]. Başka bir ifadeyle, GVK Tüzüğü'ne uygun davranılabilmesi için üçüncü ülkede bulunan bir veri alıcısının Transferler İçin Tasarlanan Davranış Kuralları'na katılmış olması gerekirken, kişisel verilerin üçüncü ülkedeki veri alıcısına aktarımı sağlayan GVK Tüzüğü'ne tabi veri sorumlusu veya veri işleyenler tarafından davranış kurallarına bir bağlılık taahhüdü verilmesi zorunlu değildir[201]. Burada en önemli kriter; üçüncü ülkelerde bulunan veri sorumluları veya veri işleyenler tarafından veri transferi esnasında davranış kurallarında yer alan yükümlülüklere uygun davranacaklarının bağlayıcı ve uygulanabilir taahhüt altına alınması gerektiğidir.

Kişisel verilerin GVK Tüzüğü kapsamında üçüncü ülkelerdeki veri sorumluları veya veri işleyenlere aktarılmasına imkân sağlayan davranış kurallarının, benzer fonksiyona sahip bağlayıcı şirket kurallarına (BCR) veya standart sözleşme maddelerine (SCC) kıyasla daha efektif çözümler sunduğu söylenebilir. Zira GVK Tüzüğü madde 47 kapsamındaki bağlayıcı şirket kurallarının aksine, davranış kurallarını kullanan kuruluşların veri transferlerinin çerçevesini çizebilmek adına aynı grup içinde yer almaları şart değildir. Bununla birlikte davranış kuralları, SCC'lerde olduğu gibi yalnızca sözleşme içerisinde belirtilen spesifik veri işleme süreci için değil, tekrarlanan süreçler için de koruma getirmektedir[202].

4.5.1. Transferler İçin Tasarlanan Davranış Kurallarının Onaylanması

Öncelikle belirtmek gerekir ki, davranış kuralları ile ilgili çalışmanın önceki kısımlarındaki bilgiler, bu başlık altında aksine bir düzenlemeye yer verilmediği takdirde, Transferler İçin Tasarlanan Davranış Kuralları bakımından da geçerli kabul edilmelidir.

[200] Yine de, grup şirketlerinden AEA sınırları dâhilindeki bir şirket tarafından üçüncü ülkede bulunan diğer bir şirkete veri transferinin belirtilen şartlar dâhilinde yapılması mümkün olacaktır. Bkz. EDPB. *Guidelines 04/2021 on Codes of Conduct as tools for transfers,* s.6
[201] A.g.e., s.6
[202] A.g.e., s.7

Daha evvel değinildiği üzere, Transferler İçin Tasarlanan Davranış Kuralları başlangıçta *transferlere yönelik davranış kuralları* (GVK Tüzüğü madde 40(3)) şeklinde hazırlanabileceği gibi, ilk olarak GVK Tüzüğü Kuralları olarak hazırlanıp sonradan bu kuralların kapsamının kişisel veri transferlerini içerecek şekilde genişletilmesi suretiyle de oluşturulabilecektir.

Davranış kurallarının içerisinde kişisel veri transferine ilişkin düzenlemelere yer verilen her iki halde, bu kurallar önce yetkili veri koruma otoritesi tarafından değerlendirilir ve yapılan değerlendirme sonucunda uygun bulunması durumunda yetkili veri koruma otoritesi tarafından EDPB'nin görüşüne sunulur[203]. Bu kapsamda EDPB, kendisine iletilen taslak davranış kuralları ile yetkili veri koruma otoritesinin olumlu görüşünü GVK Tüzüğü madde 40(7) ve 64(1)-(b) uyarınca değerlendirir.

Davranış kurallarının içeriğinin EDPB tarafından uygun görülmesi halinde, EDPB bu kuralları destekleyici görüşüyle birlikte Komisyon'a iletilir. Komisyon, transferler için tasarlanan davranış kurallarının *genel geçerliliği* olup olmadığı konusunda karar vermeye yetkili mercidir.

Transferler İçin Tasarlanan Davranış Kuralları'nın onaylanması için ulusötesi davranış kurallarının onaylanmasına ilişkin usul izlenmekle birlikte, üçüncü ülkelere kişisel veri aktarımı için kullanılacak davranış kurallarının Komisyon tarafından bu kuralların *genel geçerliliğe* sahip olduğuna karar verilmesi zorunludur[204].

[203] Her ne kadar "transferler için tasarlanmış davranış kuralları" bir üye devlet tarafından AEA bölgesi dışına yapılacak veri aktarımlarının çerçevesini çizebilecekse de, bu kurallar çoğunlukla birden fazla üye devlet tarafından gerçekleştirilecek veri aktarımlarını düzenler. Bu nedenle, "transferler için tasarlanmış davranış kuralları ağırlıklı olarak "ulusötesi kurallar" niteliğini haiz olur.

[204] EDPB. *Guidelines 04/2021 on Codes of Conduct as tools for transfers,* s.10; Lachaud (2019), s.5.

4.5.2. Transferler İçin Tasarlanan Davranış Kurallarına Uyumun İzlenmesi

EDPB'nin Transferler İçin Tasarlanan Davranış Kuralları özelinde hazırladığı rehberiyle[205], davranış kuralları bakımından genel çerçeveyi çizen EDPB rehberi[206] içerisindeki izleme kuruluşunun akreditasyonu ile ilgili düzenlemelere ek yükümlülükler getirilmekte ve kimlerin izleme kuruluşu olabileceğine dair birtakım detaylara yer verilmektedir. Bu doğrultuda, Transferler İçin Tasarlanan Davranış Kuralları'na uygunluğun gözetiminden sorumlu izleme kuruluşlarının AEA'da kurulu olma şartı yoktur. İzleme kuruluşunun AEA dışında yerleşik olduğu bu gibi durumunda, izleme kuruluşunun bağlı kuruluş merkezinin AEA sınırları içinde bulunması veya izleme faaliyetlerine ilişkin nihai kararların alındığı yerin AEA içinde olması gerekir[207].

AEA'da yerleşik bir izleme kuruluşu, GVK Tüzüğü'nün 41. maddesi kapsamındaki görev ve sorumluluklarını AEA'de kurulu olmayan ancak bağımsız ve uzmanlığa sahip üçüncü bir kuruluşa taşere edebilecektir. Böyle bir durumda, taşeron kuruluşun da izleme kuruluşunun tabi olduğu akreditasyon gerekliliklerini eksiksiz bir şekilde karşılaması şarttır. Dahası, taşeron kuruluşun sağlayacağı hizmetlerin de AEA'da yerleşik olması dolayısıyla izleme kuruluşu tarafından etkin bir şekilde kontrol edilmesi gerekir. Zira izleme kuruluşu ile taşeron kuruluş arasında kurulan sözleşmesel ilişkisi[208] kapsamında ne sorumluluk ne de izleme faaliyetleri ile ilgili karar alma yetkisi taşeron kuruluşa geçer[209]. Bu bağlamda, taşeron tarafından yürütülen izleme faaliyetleri de dâhil ancak bunlarla sınırlı olmaksızın, izleme kuruluşunun sorumluluğunda olan tüm izleme faaliyetleri ile ilgili olarak hesap verecek taraf, izleme kuruluşudur. O halde, izleme kuruluşunun

[205] EDPB. *Guidelines 04/2021 on Codes of Conduct as tools for transfers.*
[206] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*.
[207] EDPB. *Guidelines 04/2021 on Codes of Conduct as tools for transfers*, s.9.
[208] İzleme kuruluşu ve taşeron firma arasında imzalanacak olan ana sözleşmede, gizliliğin ve veri güvenliğinin temini için gerekli her türlü düzenlemeye yer verilmelidir. Ayrıca taşeronun sözleşme kapsamında elde edeceği kişisel verileri kendi alt işverenlere aktarması söz konusu olacak ise, ilgili üçüncü tarafların da veri güvenliğine ilişkin gerekli önemleri alması sağlanmalıdır. Bkz. A.g.e., s.9.
[209] A.g.e., s.9.

izleme faaliyetlerini taşere edeceği kuruluş ile imzalayacağı sözleşmede, taşeron tarafından, yürütülecek izleme faaliyetlerinin gereği gibi ifa edilmediği hallerde izleme kuruluşunun kendisine rücu edileceğine dair taahhütlere yer verilmesi faydalı olacaktır.

4.6. GVK TÜZÜĞÜ TAHTINDA ÖRNEK DAVRANIŞ KURALLARI

AB kişisel veri koruma hukukunda kendisine yer bulan davranış kurallarının temelleri 95/46 sayılı Direktif ile atılmış olup GVK Tüzüğü ile davranış kurallarının tekrar teşvik edildiği görülmektedir[210]. GVK Tüzüğü'nün 40(6) maddesi kapsamında hâlihazırda sicile kaydedilmiş olan onaylı davranış kurallarına bakıldığında[211], bu kuralların oldukça sınırlı sayıda olduğu görülür. Bunun en temel sebebinin 95/46 sayılı Direktif döneminde yetkili veri koruma otoriteleri ve endüstri aktörleri arasında mevcut olan anlaşmazlıklar olduğu düşünülmektedir[212]. GVK Tüzüğü'nün yürürlüğe girerek davranış kuralları ile ilgili daha açık düzenlemeler getirmesi ve EDPB tarafından davranış kuralları ile ilgili yönlendirici rehberlerin yayımlanmasıyla birlikte bu anlaşmazlıkların ortadan kalkmaya başladığı, dolayısıyla -gidişata bakıldığında- hesap verebilirlik araçlarından davranış kurallarının kullanımının gün geçtikçe artacağı tahmin edilmektedir. Hâlihazırda sicile kayıtlı kuralların birçoğunun ulusal davranış

[210] Uygulamada GVK Tüzüğü yürürlüğe girmeden önce kabul edilen davranış kurallarına da mevcut olup bunlara örnek olarak Almanya'nın Federal Veri Koruma Yasası'na dayanılarak Alman Sigorta Birliği (GDV) tarafından hazırlanan "Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft *(Kişisel Verilerin Alman Sigorta Endüstrisi Tarafından İşlenmesine İlişkin Davranış Kuralları)*" gösterilebilecektir. İlgili davranış kurallarının GVK Tüzüğü referanslarını içeren güncellenmiş versiyonuna erişim için: https://www.gdv.de/resource/blob/90408/c391b1dd04b41448fdb99918ce6d03bf/download-code-of-conduct-data.pdf (Erişim Tarihi: 11.07.2023)

[211] GVK Tüzüğü'nün yürürlüğe girmesinden önce davranış kuralları ile ilgili birtakım düzenlemeler 95/46 sayılı Direktif'te yer aldığından, esasında AB çapındaki ilk davranış kurallarının FEDMA'ya ait "European Code of conduct for the use of personal data in direct marketing" isimli kurallar olduğu söylenebilir. (Konuyla ilgili açıklamalar için bkz. Vander Maelen, C. (2021). First of many? First GDPR transnational code of conduct officially approved after EDPB opinions 16/2021 and 17/2021. *European Data Protection Law Review*, 7(2). s.230) Bu kuralların GVK Tüzüğü'nden önce kabul edilmesi sebebiyle ilk kez ilgili tüzük ile getirilen sicile kayıt sürecinin bir parçası olmadığı anlaşılmaktadır.

[212] Vander Maelen (2021), s.231.

kuralları olduğu, bunlardan yalnızca iki tanesinin ulusötesi davranış kurallarından olduğu görülmektedir[213]. Yalnızca ulusötesi davranış kurallarının birden fazla AB üyesi devlette yürütülecek veri işleme faaliyetleriyle ilgili olması dolayısıyla, gerçek anlamda AB çapında kabul edilebilecek uygulamadaki davranış kuralları sınırlıdır.

Hâlihazırda sicile kayıtlı olan ulusötesi davranış kurallarına bakıldığında sırasıyla SCOPE Europe tarafından Belçika Veri Koruma Otoritesi'ne yapılan başvuru kapsamında sunulan EU Cloud Code ile Fransa Veri Koruma Otoritesi'ne yapılan başvuru Cloud Infrastructure Service Providers Europe'un onaylanarak kamuya açıklandığı görülür. Anılan davranış kurallarının her ikisi bulut bilişim endüstrisindeki hizmet sağlayıcı veri işleyenlere yönelik hazırlanmıştır. Yine, onaylı ulusötesi davranış kurallarından her ikisinin de AB dışına veri aktarımı için transfer aracı olarak –en azından şimdilik- kullanılamayacağı[214] görülmektedir. Buna karşılık, ilgili davranış kuralları kapsamları itibariyle farklılaşmaktadır.

Cloud Infrastructure Service Providers Europe'un (CISPE), EU Cloud Code'dan daha sonra onaylanmasına rağmen, daha sınırlı bir kapsamı vardır. Eu Cloud Code, bulut bilgi işlemini ifade eden Hizmet Olarak Altyapı (IaaS), Hizmet Olarak Yazılım (SaaS) ve Hizmet Olarak Platform (PaaS) gibi çeşitli hizmet modellerini içerirken[215], CISPE kapsamında yalnızca Hizmet Olarak Altyapı (IaaS) ile sınırlı düzenlemeler öngörülmüştür. Ayrıca her ikisinin de onaylı hale gelebilmek için tabi oldukları usul aynı olsa da, yürürlükleri bakımından önemli bir farkları vardır.

---

[213] EDPB. (n.d.). Our documents. https://edpb.europa.eu/our-work-tools/documents/our-documents_en?f%5B0%5D=all_topics%3A125&f%5B1%5D=all_topics%3A896 (Erişim Tarihi: 29.05.2023)

[214] Konuyla ilgili EDPB görüşü için bkz. International Association of Privacy Professionals (IAPP). (10 Mayıs 2021). What's behind the EU's new cloud code of conduct? *IAPP News.* https://iapp.org/news/a/whats-behind-the-eus-new-cloud-code-of-conduct/ (Erişim Tarihi: 29.05.2023)

[215] EDPB. (2021). Opinion 16/2021 on the Draft Decision of the Belgian Supervisory Authority Regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe. s.4. https://edpb.europa.eu/our-work-tools/our-documents/opinion-board/article-64/working-draft-opinion-162021-draft-decision_en (Erişim Tarihi: 29.05.2023)

Bildiğini üzere, onaylı davranış kurallarının kullanılabilmesi için bu kurallara uygun davranılıp davranılmadığını gözetecek bir izleme kuruluşu bulunması gerekir. EU Cloud Code onaylanıp sicilde ilan edilmeden evvel, ilgili kurallara uyumun izlenmesi için izleme kuruluşu belirlenmiştir. Belirlenen bu kuruluş hâlihazırda akredite edilmiş olduğundan, EU Cloud Code doğrudan kullanılabilecektir[216]. Bunun aksine, CISPE kapsamında henüz GVK Tüzüğü'ne uygun olarak belirlenmiş bir izleme kuruluşu bulunmaması dolayısıyla davranış kuralları sicile kaydolmuş olsa bile, bu kuralların derhal kullanması mümkün olmamıştır.

Gerek EU Cloud Code gerek CISPE'nin nispeten yeni kullanılan araçlar olması sebebiyle ilgili davranış kurallarının avantaj veya dezavantajlarına dair şimdilik yeterli bilgi olmamakla birlikte, gönüllü hesap verebilirliği sağlayan bu kuralların yetkili veri koruma otoritelerinin iş yükünü hafifleteceği düşünülmektedir[217]. Buna karşılık, onaylı ulusötesi davranış kuralları ile ilgili bazı eleştiri ve endişelere sahip tarafların da olduğu görülür[218]. Diğer taraftan, Komisyon'un, özellikle bulut bilişim gibi önemli miktarda verinin işlendiği veya sağlık sektörü gibi hassas verilerin işlendiği endüstrilerde ulusötesi davranış kurallarının çoğalması yönünde bir temennisi olduğu anlaşılmaktadır[219].

[216] Vander Maelen (2021), s.228.
[217] A.g.e., s.230.
[218] Detaylar için bkz. The Privacy Company. (2021, Nisan). New EU code of conduct for cloud providers: Not a GDPR party. *The Privacy Company Blog.* https://www.privacycompany.eu/blogpost-en/new-eucode-of-conduct-for-cloud-providers-not-a-gdpr-party (Erişim Tarihi: 29.05.2023)
[219] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.* s.21, dn. 72.

BEŞİNCİ BÖLÜM

HESAP VEREBİLİRLİK ARACI OLARAK SERTİFİKASYON

5.1. SERTİFİKASYON KAPSAMI

GVK Tüzüğü'nün 42. maddesinde, sertifikasyon mekanizmalarının veri sorumluları ve veri işleyenler tarafından yürütülen işleme faaliyetlerinin GVK Tüzüğü'ne uygunluğunu göstermek amacıyla ve mikro, küçük ve orta ölçekli işletmelerin özel ihtiyaçlarının dikkate alınması suretiyle oluşturulacağı düzenlenmiştir. Ayrıca GVK Tüzüğü'nde sertifikasyon kapsamına detaylı bir şekilde yer verilmemekle birlikte, mevcut düzenlemeler doğrultusunda sertifikasyonun geniş bir kapsama sahip olabileceği söylenebilecektir. Bununla birlikte, hesap verebilirlik araçlarından sertifikasyondan, GVK Tüzüğü'ne tabi olan veri sorumluları veya veri işleyenler ile Madde 46(2)-(f)'de atıfta bulunulan koşulların sağlanması kaydıyla GVK Tüzüğü'ne tabi olmayan veri sorumluları veya veri işleyenler de yararlanabilecektir[220]. Bu anlamda hesap verebilirlik araçlarından sertifikasyon ile davranış kurallarının benzeştiği ve GVK Tüzüğü'nün bölgesel kapsamına girmeyen veri sorumluları veya veri işleyenleri de resme dâhil edebildiği görülmektedir.

Geçerli bir sertifikasyondan söz edilebilmesi için bir sertifikasyon başvurusu almış ve sertifikasyon sağlamak üzere GVK Tüzüğü ile yetkilendirilmiş olan kuruluşların, onaylı sertifikasyon kriterlerine dayanan bir sertifikasyon şeması kapsamında uyum değerlendirmesi gerçekleştirmesi ve bu değerlendirmenin olumlu sonuçlanmasının ardından sertifikasyon düzenlemiş olması gerekir**.**

Sertifikasyon şeması; *"veri sorumluları ve veri işleyenler tarafından yürütülen bir veya birden fazla veri işleme operasyonunun ve/veya faaliyet*

[220] İlgili madde için bkz. GVK Tüzüğü, m.42(2).

gösterilen bir veya birden fazla sektörün hedef alınması suretiyle oluşturulan şema[221]*"* olarak tanımlanabilecektir. Sertifikasyon şemalarının kapsamının net, pratik, izlenebilir olması ve katma değer sağlaması[222] oldukça önemlidir. Nitekim kapsamı net olmayan bir sertifikasyon şemasına yönelik etkin bir uygunluk değerlendirmesi yapılması mümkün olmayacaktır. Sertifikasyon şeması bakımından vazgeçilmez olan üç ana element vardır ki, bunlar: **(i)** değerlendirme hedefi (ToE), **(ii)** sertifikasyon kriterleri ve **(iii)** değerlendirme sürecidir[223].

Değerlendirme hedefi (ToE), değerlendirmeye konu olan bir ürün ve/veya sistem ya da bir sistemin veya ürünün parçası ile bunlarla ilgili tüm dokümantasyonu ifade eder[224]. Değerlendirme hedefi (ToE) ile bir sertifikasyon şemasının kapsamını karıştırmamak gerekir. ToE, sertifikasyon şeması tahtında yürütülen sertifika projelerinin içeriğine bağlı olarak farklılaşır, böylece her bir sertifikasyon projesi özgün bir niteliğe sahip olur. ToE'de, sertifikasyona konu veri işleme operasyonlarından hangilerinin olduğu ile söz konusu operasyonlarının değerlendirilmesi esnasında dikkate alınması gereken ana bileşenlerden[225] hangilerinin değerlendirmeye konu olup olmadığının açıkça belirtilmesi gerekir. Ayrıca ToE'de yer alan veri işleme operasyonları, veri işleme

[221] EDPB, sertifikasyon şemalarını, hedeflenen veri işleme operasyonları ve/veya sektörlerinin bir veya birden fazla (çeşitli) olması göre "general certification scheme" ve "specific certification scheme" olarak ayrı ayrı tanımlamıştır. Bkz. EDPB. (6 Nisan 2021). *Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment.* s.3. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_certification_criteria_assessment_formatted_en_0.pdf (Erişim Tarihi: 29.05.2023)

[222] A.g.e, s.7.

[223] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,* s.17.

[224] National Institute of Standards and Technology. (n.d.). Target of Evaluation. NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/target_of_evaluation (Erişim Tarihi: 29.05.2023)

[225] Bahsi geçen ve sertifikasyona konu olan veri işleme operasyonlarının değerlendirilmesi esnasında (her hâlükârda ve uygulanabilir olduğu ölçüde) dikkate alınması gereken üç ana bileşen; **(i)** işlenen kişisel veriler, **(ii)** kişisel verilerin işlenmesi için kullanılan donanım ve yazılımlar ve **(iii)** kişisel veri işleme operasyonlarıyla ilgili süreç ve prosedürlerdir. (EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,* s.15-16)

faaliyetleriyle doğrudan bağlantılı ihtiyaçlara sahip olmalı ve kişisel verilerin güvenliğinin anlaşılır bir şekilde sağlanmasına yardımcı olmalıdır. Her hâlükârda TOE yanıltıcı olmamalı ve GVK Tüzüğü, m.42 kapsamında düzenlenen sertifikasyon ile sertifika sahiplerinin üçüncü kişiler nezdinde ortaya koyduğu 'uyumluluk iddiası' ile uyumlu olmalıdır. TOE kapsamında hangi veri işleme operasyonlarının olduğu ve üç temel bileşenden (kişisel veriler, donanım ve yazılımlar, süreç ve prosedürler) hangilerinin değerlendirilip değerlendirilmeyeceği ise açıkça belirtilmelidir[226].

Sertifikasyon şemasının çeşitli veri işleme operasyonları ve/veya birden fazla sektör ile ilgili 'genel sertifikasyon şeması' olarak ya da münferit bir veri işleme operasyonu ve/veya belirli bir sektör ile ilgili 'spesik sertifikasyon şeması' olarak hazırlanması mümkündür.

Spesifik sertifikasyon şeması söz konusu olduğunda, değerlendirme hedefleri (ToE) bu sertifikasyon şeması içerisinde halihazırda tanımlanmış olabilir. Başka bir deyişle, önerilen sertifikasyon şemasının kapsamına bakıldığında, ToE'nin anlamlı bir şekilde daraltılması ve belirli bir özellik veya tek bir veri işleme faaliyetinin sertifikasyona konu edilmesi mümkün değil ise, sertifikasyon şemasının kapsamı ve ToE özdeş olacaktır[227]. ToE'nin yanı sıra sertifikasyon şemasında bulunması gereken iki diğer ana bileşen, çalışmanın ilerleyen kısımlarda detaylı olarak açıklanacağından burada ayrıca ele alınmamıştır.

5.2. SERTİFİKASYON-AKREDİTASYON ARASINDAKİ İLİŞKİ VE GENEL HATLARIYLA AKREDİTASYON

Sertifikasyon düzenlenmesi ile akreditasyon sağlanması birbirinden farklı konular olup 'sertifikasyon' süreci GVK Tüzüğü çerçevesinde kişisel veri işleme

[226] *EDPB. Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,* s.17.
[227] A.g.e., s.17.

faaliyetleri yürüten veri sorumluları veya veri işleyenlerin hesap verebilirlik araçlarından sertifikasyondan yararlanması anlamına gelirken, 'akreditasyon' ise bir kuruluşun veri sorumlusu veya veri işleyen başvuruculara geçerli bir sertifikasyon sağlayabilmek üzere yetkilendirilmesidir. GVK Tüzüğü'nün 42(5) maddesi göre sertifikasyon düzenleme yetkisi, ilgili veri sorumlusu veya veri işleyenin bulunduğu AB üyesi devletteki yetkili veri koruma otoritesi veya GVK Tüzüğü'nün GVK Tüzüğü'nün 43(1) maddesi kapsamında akredite edilmiş sertifikasyon kuruluşlarına aittir.

5.2.1. Sertifikasyon Kuruluşlarının Akredite Edilmesi

5.2.1.1. Akreditasyon Kavramı

GVK Tüzüğü'nde akreditasyon kavramının tanımı yer almazken, tüzüğün 43 maddesinin 1. fıkrasında atıf yapılan ürünlerin akreditasyonu ve pazar gözetimi için gerekliliklerin belirlenmesi hakkındaki 765/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü ("765/2008 sayılı Tüzük")[228] ile ISO/IEC 17011[229] standartlarında akreditasyon kavramın tanımlandığı görülmektedir. 765/2008 sayılı Tüzük'ün 2. maddesinin 10. fıkrasındaki tanıma göre akreditasyon; *"Bir uygunluk değerlendirme kuruluşunun, belirli bir uygunluk değerlendirme faaliyetini yürütebilmek için, uyumlaştırılmış standartlardaki gereklilikleri (ve uygulanabilir olduğunda, ilgili sektörel şemalarda belirtilenler dâhil olmak üzere herhangi ek gereklilikleri) karşıladığının ulusal bir akreditasyon kuruluşu tarafından tasdik edilmesi"* anlamına gelmektedir. Öte yandan, ISO/IEC 17011 uyarınca akreditasyon; *"belirli uygunluk değerlendirme görevlerini yerine*

[228] European Union. (2008). Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. *EUR-Lex.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0765&from=EN (Erişim Tarihi: 29.05.2023)

[229] ISO. (2017). ISO/IEC 17011:2017(en) *Conformity assessment - Requirements for accreditation bodies accrediting conformity assessment bodies* https://www.iso.org/obp/ui/en/#iso:std:iso-iec:17011:ed-2:v1:en (Erişim tarihi: 29.05.2023)

getirme yetkinliğinin resmi olarak gösterilmesini sağlayan bir uygunluk değerlendirme kuruluşuna ilişkin üçüncü taraf tasdiki" anlamına gelir[230].

Ayrıca, her ne kadar GVK Tüzüğü'nde akreditasyon tanımı yer almasa da, EDPB tarafından yayımlanan rehberde GVK Tüzüğü kapsamında akreditasyonun ne anlama geldiğiyle ilgili bir açıklama yapılmıştır. Yapılan açıklamaya göre akreditasyon; *"bir sertifikasyon kuruluşunun, ISO/IEC 17065:2012 ve yetkili veri koruma otoritesi ve/veya Kurul (EDPB) tarafından belirlenen ek gerekliliklerin dikkate alındığı ve bunlara uyulduğunun tespit edilmesi kaydıyla ulusal akreditasyon kuruluşu ve/veya yetkili veri koruma otoritesi tarafından GVK Tüzüğü Madde 42 ve 43 kapsamında sertifikasyon sağlamaya yetkili olduğunun tasdik edilmesi"* şeklinde ifade edilmektedir.[231] Özetle, GVK Tüzüğü anlamında akreditasyon, bir sertifikasyon kuruluşunun GVK Tüzüğü kapsamında geçerli bir sertifika sağlamaya yetkili hale gelmesi olup bu fonksiyon De Hert ve Kamara tarafından *'certifying certifier'* olarak tanımlanmıştır[232].

GVK Tüzüğü'nün 43(1) maddesinde, sertifikasyon kuruluşlarını akredite etmeye yetkili taraflara yer verilmiştir. Madde 43(1)(a)'ya göre akreditasyon, kendi gereklilikleri temelinde yetkili veri koruma otoriteleri tarafından sağlanabileceği gibi, Madde 43(1)(b) kapsamında ve ISO/IEC 17065:2012 standartları[233] ile yetkili veri koruma otoritesi tarafından öngörülen akreditasyon gereklilikleri temelinde ulusal akreditasyon kuruluşu tarafından da sağlanabilecektir.

---

[230] EDPB. (4 Haziran 2019). *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, s.8. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf (Erişim Tarihi: 29.05.2023)

[231] EDPB. *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, s.8.

[232] Kamara & De Hert (2018), s. 18.

[233] ISO. (2012). ISO/IEC 17065:2012(en) *Conformity assessment - Requirements for bodies certifying products, processes and services.* https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en (Erişim tarihi: 29.05.2023)

5.2.1.2. Akreditasyon Gereklilikleri

Bir sertifikasyon kuruluşunun akredite edilebilmesi için, akreditasyon sağlamaya yetkili kuruluşun aşağıda sayılan GVK Tüzüğü'nün 43(2) maddesindeki akreditasyon gerekliliklerini sağladığını ortaya koyması zorunludur. Bahsi geçen gereklilikler aşağıda belirtilmiştir:

a) Sertifikasyon konusunda bağımsızlığını ve uzmanlığını[234] yetkili veri koruma otoritesini tatmin edecek ölçüde göstermiş olması

b) GVK Tüzüğü'nün 42(5) maddesinde atıfta bulunulan ve yetkili veri koruma otoritesi tarafından onaylanan sertifikasyon kriterlerine riayet etmeyi taahhüt etmiş olması

c) Sertifika (belge), veri koruma mührü ve işaretinin verilmesine, düzenli aralıklarla gözden geçirilmesine ve geri çekilmesine ilişkin usuller oluşturmuş olması

d) Sertifikasyon ihlalleri veya veri sorumlusu veya veri işleyen tarafından uygulanmış veya uygulanmakta olan sertifikasyon yöntemine ilişkin şikayetleri ele almak için yerleşik prosedürler ve yapılar oluşturmuş olması

e) Görev ve vazifelerinin çıkar çatışmasına neden yetkili veri koruma otoritesini tatmin edecek ölçüde göstermiş olması

---

[234] Akredite sertifikasyon kuruluşu tarafından yürütülen uygunluk değerlendirmesi kapsamında sertifikasyon faaliyetlerinin bir kısmı ilgili laboratuvarlar, denetçiler gibi üçüncü kuruluşların desteğiyle sertifikasyon kuruluşu adına gerçekleştirilebilecektir. Nasıl ki sertifikasyon kuruluşunun akredite edilebilmesi için uzmanlığını ortaya koyması bekleniyorsa, sertifikasyon faaliyetlerinin yürütülmesi sırasında destek veren üçüncü kuruluşlardan yararlanıldığı bu gibi hallerde, bahsi geçen kuruluşların da sertifikasyon kuruluşundan beklenen uzmanlığa sahip olması gerekmektedir. (EDPB. *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* s.12.) GVK Tüzüğü'nün sertifikasyon kuruluşu adına faaliyetlerinin bir kısmını gerçekleştiren üçüncü tarafların akredite edilmesine cevaz verdiğini gösteren bir düzenleme bulunmamaktadır. Dolayısıyla, akredite sertifikasyon kuruluşu ile üçüncü taraf arasında hukuki ilişki kurulmadan evvel üçüncü tarafın yetkinliğinin sertifikasyon kuruluşu tarafından kontrol edilmesi gerekeceğini ve bu konu özelinde birtakım koruyucu hükümlerin taraflar arasında imzalanacak sözleşmede öngörülmesi gerekeceği söylenebilir. Zira sertifikasyon faaliyetlerinin bir kısmını yürütmekle sorumlu ilgili üçüncü tarafların sertifikasyon kuruluşu 'adına' hareket ettiği esnada yeterli ve gerekli uzmanlığa sahip olmadığı hallerde, sertifikasyon kuruluşunun akredite olabilmek için sağlamakla yükümlü olduğu uzmanlık şartının varlığı korunmak istenen menfaatlerin korunamamasına sebep olacaktır.

5.2.1.2.1. Ek Akreditasyon Gereklilikleri

Değerlendirme sürecinin ulusal akreditasyon kuruluşu tarafından yürütüleceği durumlarda GVK Tüzüğü'ne uygun bir akreditasyon için; GVK Tüzüğü'nün 43(2) maddesinde sayılan akreditasyon gerekliliklerine ilave olarak ISO/IEC 17065:2012 standartları ile yetkili veri koruma otoritesi tarafından hazırlanan ek akreditasyon gerekliliklerinin de dikkate alınması gerekir. Bu doğrultuda EDPB, ek akreditasyon yükümlülüklerin hazırlanması kapsamında yetkili veri koruma otoritelerine rehberlik sağlamak amacıyla yapısal ve metodolojik anlamda birtakım önerilerde bulunulmuştur[235].

Ek akreditasyon gereklilikleri hazırlanırken, GVK Tüzüğü'nün 43(2) maddesinde düzenlenen akreditasyon gerekliliklerinin temel alınması gerektiğiunutulmamalıdır. Bu doğrultuda yetkili veri koruma otoritesinin hazırlayacağı ek akreditasyon gereklilikleri, akreditasyon değerlendirme sürecinin bir parçası haline gelmeden önce EDPB ile bu gerekliliklere ilişkin iletişim kurulması gerekir[236]. Geçerlilik kazanan ek akreditasyon gereklilikleri ile GVK Tüzüğü madde 43(2)'te öngörülen ana akreditasyon gereklilikleri ve ISO/IEC 17065:2012 standartlarının birlikte dikkate alınması suretiyle gerçekleştirilecek değerlendirmenin olumlu sonuçlanması halinde, sertifikasyon kuruluşu akredite edilecektir.

Bir sertifikasyon kuruluşunun ulusal akreditasyon kuruluşu tarafından akredite edilebilmesi için dikkate alınması gereken tüm gereklilikler ve standartlar arasında, teşbih yerindeyse, normlar hiyerarşisi vardır. Bu hiyerarşiye göre, piramidin en üstünden en aşağısına doğru sırasıyla GVK Tüzüğü, ISO/IEC 17065:2012 standartları ve ek akreditasyon gereklilikleri vardır. Yani, ek

[235] Detaylar için bkz. EDPB. *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679)* – Annex1, s.13.
[236] A.g.e. (Annex 1), s.13.

akreditasyon gerekliliklerinin ISO/IEC 17065:2012'ye aykırılık teşkil edecek şekilde düzenlenmemesi, ISO/IEC 17065:2012 standartlarının ise GVK Tüzüğü'nde öngörülen şartları zayıflatmaması veya tamamıyla ortadan kaldırmaması gerekir[237].

5.2.1.3. Akreditasyonun Sağlanması ve Geri Çekilmesi

Sertifikasyon kuruluşunun GVK Tüzüğü Madde 42 ve 43 kapsamında sertifikasyon sağlamaya yetkili olduğunun değerlendirilmesi halinde, ilgili kuruluşa akreditasyon sağlanır. İlgili sertifikasyon kuruluşuna sağlanan akreditasyon süresiz olmayıp GVK Tüzüğü'nün 43. maddesinin 4. fıkrası uyarınca en fazla beş yıl süreyle verilir. Ayrıca aynı maddenin 7. fıkrasına göre, akredite sertifikasyon kuruluşu tarafından akreditasyon gerekliliklerinin karşılanmadığı veya artık sağlanmadığının tespit edildiği hallerde ya da GVK Tüzüğü'nün ilgili sertifikasyon kuruluşu tarafından ihlal edildiği hallerde, sağlanan akreditasyon yetkili veri koruma otoritesi veya ulusal akreditasyon kuruluşu tarafından geri çekilebilecektir.

5.3. SERTİFİKASYON VE AKREDİTASYON İLE İLGİLİ AKTÖRLER

Yukarıda açıklandığı üzere, sertifikasyon ve akreditasyon süreçleri arasında bir ilişki olup[238] sertifikasyon ve akreditasyon ile ilgili aktörlerin GVK Tüzüğü'nden doğan görev ve yetkileri yer yer kesişebilmektedir[239]. Bu sebepledir ki; bu kısımda yer verilen açıklamalar, sertifikasyon ve akreditasyon sürecindeki tüm süjeler ile bu süjelerin birbiriyle benzeştiği veya ayrıştığı durumları da kapsayacaktır.

---

[237] EDPB. *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* s.13-14.

[238] Çalışmanın 5. bölümünün "5.2. Sertifikasyon-Akreditasyon Arasındaki İlişki ve Genel Hatlarıyla Akreditasyon" alt başlığı altındaki açıklamalara bakınız.

[239] Örneğin, akredite sertifikasyon kuruluşu, sertifikasyon için başvuruda bulunan veri sorumluları veya veri işleyenlere sertifika sağlayabileceği gibi aynı anda sertifikasyon şeması hazırlayan taraf, yani scheme owner, da olabilir.

5.3.1. Şema Sahibi

Sertifikasyon şeması hazırlayan taraf, yani şema sahibi *(scheme owner),* uygunluk değerlendirmesinde dikkate alınacak sertifikasyon kriterleri ile usuli gerekliliklerini belirleyen kuruluştur. ISO/IEC 17065:2012[240] standartlarına göre şema sahibi, belirli bir sertifikasyon şeması geliştirmekten ve yürütmekten sorumlu kişi veya kuruluş olup sertifikasyon kuruluşunun kendisi, bir devlet kurumu, ticaret birliği, bir grup sertifikasyon kuruluşu veya diğerler tarafların şema sahibi olabileceği düzenlenmiştir.

GVK Tüzüğü'nde şema sahibi tanımlanmamakla birlikte EDPB tarafından yayımlanan rehberde konuya bir anlamda açıklama getirilmiştir. EDPB'nin tanımına göre 'şema sahibi'; *sertifikasyon kriterleri ile uygunluk değerlendirilmesinde dikkate alınacak gereklilikleri belirleyen tanımlanabilir kuruluş*u ifade eder[241]. EDPB, uygunluk değerlendirmesini yürüten sertifikasyon sağlamaya yetkili kuruluş ile sertifikasyon şemasını hazırlayan ve geliştiren kuruluşların aynı olabileceği gibi, bunların farklı kuruluşlar da olabileceğini belirtmiştir[242]. GVK Tüzüğü kapsamında kimlerin şema sahibi olabileceği konusunda EDBP'nin kapsayıcı ancak nispeten muğlak bir yorum yaptığı görülmektedir.

ISO'nun şema sahibine ilişkin tanımı ile EDPB tarafından yapılan açıklamalar birlikte değerlendirildiğinde, kimlerin şema sahibi olabileceği konusunda bir çıkarım yapmak mümkündür. Bu doğrultuda, sertifikasyon şemalarının kimler tarafından hazırlanacağı ve/veya yöneteceği konusunda GVK Tüzüğü'nün esnek

[240] ISO. (2012). ISO/IEC 17065:2012(en) *Conformity assessment - Requirements for bodies certifying products, processes and services.* Terms and Definitions. https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en:term:3.9 (Erişim Tarihi: 29.05.2023)
[241] EDPB. Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679), s.6, p. 8.
[242] EDPB. (14 Şubat 2023). *Guidelines 07/2022 on certification as a tool for transfers (Version 2.0),* s.8.https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (Erişim Tarihi: 29.05.2023)

çeşitli modellere izin verdiği kabul edilebilecektir[243]. Bahsi geçen farklı sertifikasyon modellerine göre;

a) Sertifikasyon şemaları, akredite sertifikasyon kuruluşları tarafından hazırlanır ve yönetilir[244].

b) Sertifikasyon şemaları, yetkili veri koruma otoritesi tarafından hazırlanır ve yönetilir.

c) Sertifikasyon şemaları, yetkili veri koruma otoritesi tarafından hazırlanır ancak değerlendirme sürecinin tamamı veya bir kısmı üçüncü şahıslara devredilir.

d) GVK Tüzüğü'nde aksi öngörülmediği için, sertifikasyon şemaları piyasadaki üçüncü taraflarca- yani özel şema sahiplerince- hazırlanır.

Özetle, sertifikasyon şemalarının akredite sertifikasyon kuruluşları, yetkili veri koruma otoritesi veya "özel şema sahipleri *(private scheme owners)*" tarafından hazırlanabileceği söylenebilir.

5.3.2. Sertifikasyon Kuruluşu

GVK Tüzüğü'nün 43(2) ve 43(3) maddeleri sertifikasyon kuruluşlarının akredite edilebilmesi için birtakım kriterler ve gereklilikler öngörmüş olup bunların eksiksiz olarak yerine getirilmesi, ilgili sertifikasyon kuruluşunun akredite edilmesi için zorunludur. Akredite sertifikasyon kuruluşları, GVK Tüzüğü 42(5) maddesinde sertifikasyon düzenlemeye yetkili taraflar arasında sayılmıştır. Bu kuruluşların akreditasyonu GVK Tüzüğü'nün 43. maddesine uygun olarak gerçekleştirmesi gerekmekle birlikte, maddenin ilk fıkrasının girişinde *"Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58..."* denilmek suretiyle sertifikasyon sağlamaya

[243] Lachaud (2020), s.12; EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.7.

[244] Bu modelde, söz konusu hazırlık ve yönetim süreci yetkili veri koruma otoritesi tarafından yakından izlenir.

yetkili kuruluşların yetkilerinin sınırları çizilmiştir. Atıf yapılan maddeler yetkili veri koruma otoritesinin görev ve yetkilerini düzenler.

Akredite sertifikasyon kuruluşları, sertifikasyon şemasına ve Madde 42(5) kapsamında onaylanmış olan sertifikasyon kriterlerine göre uygun olarak sertifikasyon sağlanmasından/düzenlenmesinden sorumludur. Bunun yanı sıra, anılan sertifikasyon kuruluşunun, ilgili veri sorumluları ve veri işleyenler tarafından GVK Tüzüğü'ne uyumluluğun gözden geçirilmesi/denetlenmesi, GVK Tüzüğü'nde belirtilen şartların sağlandığı hallerde sertifikasyonun uzatılması veya sertifikasyonun geri çekilmesi ve bu konularda yetkili veri koruma otoritesine bilgi verilmesi gibi başkaca yetki ve sorumlukları da vardır[245]. İlave olarak, akredite sertifikasyon kuruluşları tarafından sertifikasyon kriterlerinin tasarlanması da mümkündür. Yani akredite sertifikasyon kuruluşları 'sertifikasyon sağlayıcı' olabileceği gibi, 'şema sahibi' de olabilmektedir.

GVK Tüzüğü'nün 58(2) maddesinde yetkili veri koruma otoritesine yer tanınan düzeltici yetkilerin ilgili taraflar üzerinde etkili bir şekilde kullanılabilmesi için akredite edilmiş sertifikasyon kuruluşlarının, AEA içerisinde bir kuruluşa sahip olması gerekir. Akredite sertifikasyon kuruluşu olabilmek için AEA içerisinde bir kuruluşa sahip olmak gerekse de, denetim faaliyetlerinin ilgili sertifikasyon kuruluşu adına gerçekleştirilmek üzere AEA dışındaki yerel uzman veya kuruluşlara taşere edilmesi mümkündür. Bu durumda AEA dışındaki uzman veya kuruluşu tarafından akredite sertifikasyon kuruluşu 'adına' hareket edilmesi söz konusu olduğundan, sertifikasyon düzenlenip düzenlenmeyeceği konusunda karar verme yetkisinin tamamen veya kısmen AEA dışındaki taşerona devredilmesi söz konusu olmayacaktır.

EDPB tarafından dikkat çekilen bir diğer husus ise; sertifikasyon kuruluşlarının AEA dışında bir taşerondan faydalandığı hallerde, denetim faaliyetlerinin bir

[245] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.11.

bölümünün taşere edildiği ilgili uzman veya kuruluşların ISO 17065 standartları ile yetkili veri koruma otoritesi tarafından belirlenen ek akreditasyon gereklilikleri doğrultusunda değerlendirilmesi gerektiğidir. EDPB'nin bu yaklaşımının, akredite olmaya hak kazanmış bir sertifikasyon kuruluşu adına faaliyet gösteren üçüncü bir tarafın da, benzer akreditasyon standartlarını taşıdığının teminine yönelik olduğu anlaşılmaktadır.

5.3.3. Ulusal Akreditasyon Kuruluşu

Ulusal akreditasyon kuruluşu, ISO/IEC 17065:2012 standartları ile yetkili veri koruma otoritesi tarafından düzenlenen ve 765/2008 sayılı Tüzük'te öngörülen mevcut akreditasyon sözleşmelerini tamamlayıcı nitelikteki ek akreditasyon gereklilikleri tahtında[246], sertifikasyon kuruluşlarını akredite etmeye yetkilidir. Buna karşın, GVK Tüzüğü'nün, akreditasyonun yetkili veri koruma otoritesi tarafından gerçekleştirildiği hallerde, ulusal akreditasyon kuruluşu tarafından gerçekleştirildiği hallere nispetle daha az şart koştuğu görülmektedir[247]. Zira GVK Tüzüğü'nde akreditasyon sürecinin yetkili veri koruma otoritesi tarafından yürütülmesi kapsamında ISO/IEC 17065:2012 standartları ile ek akreditasyon gereklilikleri uyarınca hareket edilmesi şartına yer verilmemiştir.

Yine, GVK Tüzüğü ile ilgili olmayan sertifika programları için ISO/IEC 17065:2012 temelinde mevcut akreditasyona sahip bir sertifikasyon kuruluşunun, akreditasyon kapsamını GVK Tüzüğü'nde düzenlenen sertifikasyonu kapsayacak şekilde genişletmek istediği ve bu akreditasyonun GVK Tüzüğü madde 43(1)(b) uyarınca ulusal akreditasyon kuruluşu tarafından sağlanacağı senaryoda; mevcutta ISO/IEC temelli akreditasyona sahip sertifikasyon kuruluşunun da yetkili veri koruma otoritesi tarafından belirlenen ek gereklilikleri karşılaması gerekecektir[248].

[246] EDPB. *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* s.10.
[247] A.g.e., s.10
[248] EDPB. *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* s.10

5.3.4. Yetkili Veri Koruma Otoritesi

Yetkili veri koruma otoritesi, tıpkı akredite sertifikasyon kuruluşları gibi hem sertifikasyon sağlayıcı hem de şema sahibi *(scheme owner)* olarak hareket edebilir. Ayrıca yetkili veri koruma otoritesi, akredite sertifikasyon kuruluşlarının aksine, sertifikasyon kriterlerinin onaylanması[249] bakımından da yetki ve sorumluluklara sahiptir. Öyle ki, Avrupa Veri Koruma Mührü için başvurulmadığı hallerde yetkili veri koruma otoritesi tarafından onaylanan sertifikasyon kriterlerinden yararlanılacaktır.

Diğer taraftan, yetkili veri koruma otoritesi, sertifikasyon kuruluşlarına akreditasyon sağlanması bakımından da yetkilidir. Ancak bunun için ilgili üye devletlerin yerel mevzuatının yetkili veri koruma otoritesinin akreditasyon sağlamasına imkân vermesi gerekir[250]. GVK Tüzüğü'nün 43(1) maddesinde, sertifikasyon kuruluşlarının ilgili maddenin (a) ve (b) bentlerinde sayılan taraflardan biri veya her ikisi tarafından akredite edilebileceğinin üye devletlerce belirlenebileceği düzenlenmiştir[251]. Başka bir deyişle, sertifikasyon kuruluşunun akredite edilmesi bakımından yetkili olan organ veya organların tayin edilmesi üye devletlerin takdirine bırakılmıştır. Dolayısıyla ilgili üye devletlerin yerel mevzuatın imkân verdiği takdirde ve sınırda, ulusal akreditasyon kuruluşu tek başına veya yetkili veri koruma otoritesi ile birlikte akreditasyon sağlaması mümkün olacaktır. Üye devletlere böyle bir seçim yetkisi tanınması, AB düzeyinde uyumlaştırılmamış uygulamaların ortaya çıkabileceği gerekçesiyle *De Hert ve Kamara* tarafından eleştirilmektedir[252]. Kaldı ki, akreditasyon sağlamaya

[249] Sertifikasyon kriterleri hem akredite sertifikasyon kuruluşu hem de yetkili veri koruma otoritesi tarafından tasarlanabilecekse de, söz konusu kuruluşlardan yalnızca yetkili veri koruma otoritesi sertifikasyon kriterlerin onaylanması bakımından yetkilidir.
[250] EDPB. *Guidelines 07/2022 on certification as a tool for transfers* ,s.8.
[251] Bkz. madde GVK Tüzüğü m. 43 & EDPB. *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* s.9.
[252] Kamara & De Hert (2018), s.19; Kamara ve De Hert tarafından eleştirilen bir durumun pratikte bir örneği olarak, Lüksemburg ve Fransız veri koruma otoritelerinin GVK Tüzüğü'nün 42(5) maddesi bakımından kendi yorumları yaptıkları ve uygunluk değerlendirmesinin gerçekleştirilmesi bakımından akredite sertifikasyon kuruluşlarını yetkilendirerek bu karışıklığı giderecek çözümler yaratmaya çalıştıkları görülmüştür. (Lachaud (2020), s.4)

yetkili tarafların deneyim açısından kıyaslanması halinde de, yetkili veri koruma otoritesinin ulusal akreditasyon kuruluşuna kıyasla çoğunlukla daha deneyimsiz kalması ve kaynak sıkıntısı çekmesi kaçınılmazdır. Zira yetkili veri koruma otoritesinin, akreditasyon sürecinin yürütülmesi ile ilgili olanların dışında, GVK Tüzüğü kapsamında birçok görev ve yetkisi vardır[253].

GVK Tüzüğü'nde yetkili veri koruma otoritesinin hem sertifikasyon sağlamaya yetkili olması hem de geçerli bir sertifikasyon sağlayabilmesi için akredite olması gereken bir sertifikasyon kuruluşunu akredite etmeye yetkili olmasının öğretide birtakım endişeler doğurduğu görülür. Bu endişelerin temelinde, ilgili veri koruma otoritesinin niteliği gereği birbiriyle çatışan yetkilerini bağımsız ve objektif şekilde kullanıp kullanamayacağı sorusu yatmaktadır. Yetkili veri koruma otoritesinin hem sertifikasyon sağlayıcı hem de akreditasyon sağlayıcı şapkalarına sahip olmasının, öğretide De Hert ve Kamara tarafından[254] eleştirildiği görülür. Hatta benzer bir endişe Lauchard tarafından da dile getirilmiştir.

Lauchard'a göre, GVK Tüzüğü'nün lafzına bakıldığında akreditasyon süreci yalnızca ulusal akreditasyon kuruluşu tarafından gerçekleştirilse dahi, akreditasyonla ilgili nihai kararın yetkili veri koruma otoritesi tarafından verileceği anlamı çıkmaktadır. Dolayısıyla akreditasyon sürecinin yalnızca ulusal akreditasyon kuruluşu tarafından yürütüleceği bir senaryoda, ilgili kuruluş ile yetkili veri koruma otoritesi arasındaki süreçlerin nasıl yürütüleceği konusunda GVK Tüzüğü'nde düzenlemeye yer verilmemesi belirsizlik yaratmaktadır[255]. Bu sebepledir ki, sertifika sağlayanın yetkili veri koruma otoritesi olduğu senaryolarda sertifikasyon mekanizmasına duyulan güven azabilecektir. Zira yetkili veri koruma otoritesinin, GVK Tüzüğü'nün 42(4) maddesi çerçevesinde hareket ederken 'sertifikasyon sağlamaya yetkili kuruluş' şapkasını, 43(1)-(a) maddesi çerçevesinde ise 'akreditasyon sağlamaya yetkili kuruluş' şapkasını

[253] Kamara & De Hert (2018), s.19
[254] A.g.e., s.30-31.
[255] Lachaud (2020), s.6.

takarak hareket etmesi gerekse dahi, pratikte tam bir ayrışma yapılamaması muhtemeldir. Öğretideki endişeleri tamamen giderip gidermeyeceği tartışmaya açık olmak birlikte, EDPB'nin ilgili rehberinde[256] çıkar çatışmasına sebep olabilecek hallerde yetkili veri koruma otoritesi tarafından güçler ayrılığı ilkesine uygun davranılması gerektiğine değinildiği görülmektedir.

Son olarak, yetkili veri koruma otoritesinin, GVK Tüzüğü m.43(4) ile mevcut bir sertifikasyona uyumluluğun gözden geçirilmesi/denetlenmesi, tüm şartların sağlanması halinde sertifikasyonun yenilenmesi veya şartların gerçekleştirilmediğinin tespiti halinde, sertifikasyonun geri çekilmesi konularında da yetkilendirildiği görülmektedir.

5.3.5. EDPB

AEA genelinde geçerli bir sertifikasyondan söz edilebilmesi için ilgili sertifikasyon kriterlerinin EDPB tarafından onaylanması gerekmektedir. EDPB tarafından onaylanan sertifikasyon kriterlerine dayanan bu sertifikasyon, GVK Tüzüğü'nün 42(5) maddesinde 'Avrupa Veri Koruma Mührü' olarak adlandırılmıştır. Dolayısıyla EDPB sertifikasyon kriterlerinin onaylanması bakımından yetkilidir. Bunun dışında EDPB, tüm sertifikasyon mekanizmaları, veri koruma mühürleri ve işaretlerinin ortak bir sicilde toplanması ve kamuya açık hale getirilmesinden sorumludur[257].

EDBP, sertifikasyon kuruluşlarının akreditasyonu için öngörülen gerekliliklerin onaylanmasından ve Komisyon'a yetkili veri koruma otoritesinin akreditasyon gereklilikleri hakkında vermiş olduğu kararlara yönelik görüş verilmesinden sorumludur.

[256] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.* s.10.
[257] Bkz. GVK Tüzüğü, madde 70(1)(o).

5.3.6. Komisyon

GVK Tüzüğü'nin 43(8) maddesi uyarınca Komisyon, sertifikasyon gerekliliklerinin belirlenmesi bakımından GVK Tüzüğü, m.92'ye uygun olarak yetki devrine dayanan tasarruflarda (delegated acts) bulunmaya yetkilidir. Ayrıca, aynı maddenin bir sonraki fıkrası uyarınca Komisyon, veri koruma belgelendirme mekanizmaları (sertifika), mühürleri ve işaretlerinin teşvik edilmesi ve tanınması için teknik standartları ortaya koyan uygulama tasarrufları (implementing acts) kabul edebilir.

5.4. SERTİFİKASYON KRİTERLERİ VE GEREKLİLİKLERİ

Sertifikasyon kriterleri, sertifikasyon şemasının oldukça önemli ve ayrılmaz bir parçasıdır. Sertifikasyon kriterlerinin kimler tarafından hazırlanabileceği GVK Tüzüğü'nde açıkça belirtilmemiş olup 42. maddede bu kriterlerinin hangi otoriteler tarafından onaylanacağına değinilmekle yetinilmiştir[258]. EDPB tarafından yayımlanan yönlendirici rehberde[259] ise 'sertifikasyon kriterlerini hazırlayan ve bunları onaya sunmayı arzu eden' ifadesi kullanılarak sertifikasyon kuruluşları ile şema sahipleri (scheme owners) anılmıştır[260].

GVK Tüzüğü'nde 'sertifikasyon kriterleri' ve 'sertifikasyon gereklilikleri' olmak üzere iki ayrı kavrama yer verildiği görülse de bu iki kavram da tanımlanmamıştır. De Hert ve Kamara'ya göre, Madde 42(5)'de öngörülen sertifikasyon kriterleri ile Madde 43(8)'de öngörülen sertifikasyon gereklilikleri birbirinden farklı ve fakat birbirini tamamlayıcıdır[261].

---

[258] GVK Tüzüğü kapsamında yetkili veri koruma otoritelerine sertifikasyon şemaları hazırlama imkânı verilirken, kendi sertifikasyon kriterlerini belirlemeleri bakımından ilgili otoritelere açıkça bir yetki verilmemesi eleştirilmiştir (Lachaud (2020), s.4)

[259] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, Annex-2.

[260] GVK Tüzüğü kapsamında yetkili veri koruma otoritesine (supervisory authority) kendi sertifikasyon şemalarını hazırlama imkânı verilmiş iken, kendi sertifikasyon kriterlerini belirlemeleri konusunda açık bir düzenleme getirilmemesi eleştirilmiştir Bkz. Lachaud (2020), s.4.

[261] Kamara & De Hert (2018), s.24

Avrupa Ağ ve Bilgi Güvenliği Ajansı *(European Union Agency for Cybersecurity)* tarafından 2017 yılında yayımlanan veri koruma alanındaki sertifikasyonlara ilişkin tavsiyeleri içeren rehberde, ISO ve IEC tarafından önerilen terminolojinin aksine, GVK Tüzüğü'nde maddi gereklilikler ile prosedürel gerekliliklerin ayrı ayrı tanımlandığı belirtilmiş ve maddi gerekliliklerin 'sertifikasyon kriterlerini' prosedürel gerekliliklerin ise 'sertifikasyon gerekliliklerini' karşıladığı ifade edilmiştir[262]. O halde, sertifikasyon kriterleri ile sertifikasyon gereklilikleri birbirinden farklı olup yapılan başvuru kapsamında geçerli bir sertifikasyon sağlanabilmesi için sertifikasyon kriterlerinin karşılanması yeterli olmayacak, sertifikasyon gerekliliklerinin de yerine getirilmesi beklenecektir.

5.4.1. Sertifikasyon Kriterlerinin Belirlenmesi

GVK Tüzüğü'nün 42. maddesi kapsamında sertifikasyon kriterleri[263] hazırlanırken, bilgi güvenliğini konu alan ancak GVK Tüzüğü'nün kapsamına girmeyen sertifikasyon mekanizmaları ile mühürlerin aksine, GVK Tüzüğü'ndeki gerçek kişilerin temel haklarının korunmasına yönelik düzenlemeler getiren esaslara dayanılması gerekmektedir[264]. GVK Tüzüğü kapsamında hazırlanacak sertifikasyon kriterlerinin asgari olarak tüzük gerekliliklerini içermesi gerekmekle birlikte, bu kriterlerin GVK Tüzüğü'nde öngörülen düzenlemelerin ötesi geçecek şekilde hazırlanması da mümkün olabilmektedir.

Sertifikasyon kriterlerinin hazırlanması ve bu kriterlerin onaylanması esnasında dikkate alınması gereken hususlar hakkında EDPB'nin rehberlik sağladığı görülmektedir. Bu doğrultuda sertifikasyon kriterleri; (i)yeknesak, doğrulanabilir ve hedef kitle ile alakalı olmalı, tür ve boyutundan bağımsız olarak tüm

[262] Kamara, I., & Burnik, J. (2017). Recommendations on European data protection certification. *European Union Agency For Network and Information Security,* s.10.
[263] Değerlendirme kriterleri olarak da tanımlanabilecektir.
[264] Kamara & De Hert (2018), s.22; EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.21.

kuruluşlara uygulanabilecek düzeyde esnek ve ölçeklenebilir bir yapıda olmalı, hacmine bakılmaksızın her türlü veri işleme operasyonunun gerektirdiği teknik ve idari tedbirlerin tanımlanmasına izin vermeli, veri işleme operasyonlarına ilişkin gerçekleştirilecek uygunluk değerlendirmesini kolaylaştırmalı ve her hâlükârda dikkate alması gereken ilgili tüm standartlarla[265] gerekli olduğunda uyum içinde çalışmalıdır[266]. Bunların dışında, değerlendirmeye konu başvurunun desteklenmesi adına sertifikasyon kriterlerinin hazırlığı aşamasında başkaca unsurlar[267] da dikkate alınacaktır[268].

Genel sertifikasyon şemalarının birbirinden farklı veri işleme operasyonları ve/veya sektörler ile ilgili düzenlemeler getirebileceği düşünüldüğünde, sertifikasyon kriterleri bu gibi farklılıklar arasında denge kurulmasına imkân sağlayabilmelidir[269]. Dolayısıyla genel sertifikasyon şeması söz konusu olduğunda, sertifikasyon kriterlerinin anılan farklılıkların gerektirdiği önlemleri barındırabilecek esneklikte olması gerekir. Ayrıca sertifikasyon kriterlerinin, veri işleme operasyonlarının gerektirdiği uygun ve yeterli teknik ve idari tedbirlerin tanımlanmasına imkân sağlaması, bu tedbirlerin alınması için yeterli garantilerin sağlanıp sağlanmadığı konusunda sertifikasyon sağlayan kuruluşun nesnel bir değerlendirme yapmasına imkân vermesi ve ilgili kişilerin hak ve özgürlüklerine yönelik riskleri olasılık ve derece bazında ortaya koyması önemlidir[270].

---

[265] Örnek olarak ISO standartları ile ulusal düzeydeki standartların verildiği görülmektedir.

[266] Detaylar için bkz. EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.20.

[267] Bahsi geçen diğer unsurlar aşağıda belirtildiği gibidir:

- 6. Madde uyarınca işlemenin yasallığı;
- 5. Madde uyarınca veri işleme ilkeleri;
- 12-23. Maddeler uyarınca ilgili kişilerin hakları;
- 33. Madde uyarınca veri ihlallerini bildirme yükümlülüğü;
- 25. Madde uyarınca tasarım gereği ve varsayılan olarak veri koruma yükümlülüğü;
- Uygulanabilir olması halinde, Madde 35(7)(d) uyarınca bir veri koruma etki değerlendirmesinin yapılıp yapılmadığı;
- 32. Madde uyarınca uygulamaya konulan teknik ve organizasyonel önlemler

[268] Bahsi geçen unsurlar, uygun olduğu ölçüde ve ilgili veri işleme operasyonları ile sertifikasyonun kapsamına bağlı olarak dikkate alınacaktır. (EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.15)

[269] Kamara & De Hert (2018), s.23.

[270] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.21; Kamara & De Hert (2018), s.23.

5.4.2. Sertifikasyon Kriterlerinin Onaylanması

GVK Tüzüğü Madde 42(5)'e göre sertifikasyon kriterleri, Avrupa Veri Koruma Mührü söz konusu olan haller haricinde, yetkili veri koruma otoritesi tarafından onaylanacaktır. Bu bağlamda EDPB'nin yetkili veri koruma otoritelerinin sertifikasyon kriterleri ile ilgili taslak kararları hakkında görüş bildirme yetkisi mevcut olup bu yetki AB genelindeki uygulamalarda tutarlılığın sağlanmasını temin eder[271]. Diğer taraftan, Avrupa Veri Koruma Mührü'nün söz konusu olduğu hallerde ise, sertifikasyon kriterlerinin EDPB tarafından onaylanması gerekmektedir. Sertifikasyon kriterlerinin yetkili makamlarca onaylanması, söz konusu kriterlerin kullanılabilmesi için zorunlu olan ve bağlayıcı etkili bir işlemdir[272].

5.4.2.1. Avrupa Veri Koruma Mührü İçin EDPB Onayı

GVK Tüzüğü'nün 42(5) maddesinin son cümlesine göre, sertifikasyon kriterlerinin EDPB tarafından onaylanması ile ortak bir sertifikasyon olan Avrupa Veri Koruma Mührü verilebileceği düzenlenmiştir. Ancak Avrupa Veri Koruma Mührü'nün söz konusu olduğu hallerde dahi, sertifikasyon kriterlerinin onaylanması için doğrudan EDPB'ye başvurmak mümkün olmayıp önce yetkili veri koruma otoritesine başvurulması gerekir. Eğer yapılan başvuru kapsamında yetkili veri koruma otoritesi tarafından sertifikasyon kriterlerinin EDPB tarafından onaylanabilir olduğuna dair bir değerlendirme yapılır ise, EDPB'ye bir taslak sunulması gerekir[273].

Sertifikasyon şemasının tüm üye devletlerde kullanılmaya uygun olarak düzenlenmesi ve sertifikasyon şemasında yer alan sertifikasyon kriterleri bakımından EDPB tarafından GVK Tüzüğü'nün 63. maddesindeki tutarlılık

[271] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.6.
[272] Kamara & De Hert (2018), s.2.
[273] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,* s.13, p.36.

mekanizması çerçevesinde bir tutarlılık kararı alınması kaydıyla, AB düzeyinde sertifikasyon düzenlenmesi mümkün olacaktır.

5.4.2.2. Yetkili Veri Koruma Otoritesi Onayı

Yetkili veri koruma otoritesi, hem sertifikasyon kriterlerinin onaylanması hem de başvuru sahibi veri sorumluları veya veri işleyenleri uygunluk değerlendirmesine tabi tutarak bu değerlendirmenin olumlu sonuçlandığı hallerde sertifikasyon düzenlenmesi konusunda yetkilidir. Bu halde EDPB ise, sertifikasyon kriterleri ile ilgili olarak yetkili veri koruma otoritesi tarafından verilen taslak kararlar hakkında görüş verebilir.

Geçerli bir sertifikasyondan söz edilebilmesi için sertifikasyonun onaylı sertifikasyon kriterlerine uygun olarak düzenlenmesi zorunlu olup yetkili veri koruma otoritesinin hem sertifikasyon kriterlerinin onaylanması hem de sertifikasyon düzenlenmesi konusunda yetkili olması, *'function creep'* etkisine (başka bir ifadeyle, işlev sürünmesine) yol açabilecektir[274]. Böyle bir sonuçtan kaçınılması için sertifikasyon sürecindeki farklı görevlerin aynı aktöre verilmemesi gerektiği vurgulansa da, GVK Tüzüğü'nün 42. ve 43. maddelerine göre bazı aktörlerin üst üste binen ve çıkar çatışması yaratan görevleri bakımından ilgili mevzuatta herhangi bir değişikliğe gidilmemiştir.

Eleştirilere konu olan bir diğer konu[275] ise; GVK Tüzüğü'nün 63. maddesinde öngörülen tutarlılık mekanizması çerçevesinde, AB genelinde sunulan Avrupa Veri Koruma Mührü haricindeki sertifika (belge), veri koruma mührü veya işaretlerin, diğer üye devletlerde tanınmasını zorunlu kılan bir mekanizma bulunmamasıdır. GVK Tüzüğü'nün bu konuda açıklık getirmemesi, veri sorumlusunun faaliyet gösterdiği üye devletlerin tamamında sertifikasyon

[274] Rodrigues, R., Barnard-Wills, D., De Hert, P., & Papakonstantinou, V. (2016). The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology*, 30(3), s.262.
[275] Kamara & De Hert (2018), s.21.

sürecinden geçmesi anlamına gelebilecektir. Avrupa Veri Koruma Mührü niteliğini haiz olmayan uyum tasdikinin tüm üye devletlerde kabul görmemesi riski olduğundan, esasında önemli bir uyum ve hesap verebilirlik aracı olan sertifikasyonun bu anlamda zayıf bir yönü olduğu değerlendirilmiştir[276].

Son olarak, bir yetkili veri koruma otoritesinin ulusal girişimi kapsamında ilgili sertifikasyon kriterlerinin benimsenmesine öncülük etmesi ve diğer üye devletlerin bu kriterleri benimsemek istemesi halinde ise[277], EDPB Usul Kuralları'nın[278] 10.4. maddesi uyarınca onaylı sertifikasyon kriterlerine sahip ilgili üye devlete EDPB tarafından verilen görüşe dayanılabilecek ve diğer üye devletler tarafından EDPB'ye başvuru yapılmasına gerek kalmaksızın sertifikasyon kriterleri kabul edilebilecektir[279].

5.4.3. Sertifikasyon Kriterlerinin Değiştirilmesi

Zaman içerisinde bilgi teknolojileri alanında yaşanan gelişmeler, yasal düzenlemelerdeki değişiklikler dâhil ancak bunlarla sınırlı olmamak üzere, sertifikasyon kriterlerinin hazırlandığı esnada öngörülemeyecek ancak bu kriterlerin yeterliliğini sınayabilecek birtakım sebeplerden ötürü sertifikasyon kriterlerinde değişikliğe gidilmesi gerekebilir[280].

---

[276] Bkz. Kamara & De Hert (2018), s.21; Privacy Bridges. (2015). EU and US Privacy Experts in Search of Transatlantic Privacy Solutions, 37th International Privacy Conference Amsterdam. https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf (Erişim Tarihi: 29.05.2023)

[277] Şema kriterleri ile geçerli yerel mevzuatın dikkate alınması esastır.

[278] EDPB. (25 Mayıs 2018 & 6 Nisan 2022). European Data Protection Board Rules Of Procedure (Version 8). https://edpb.europa.eu/system/files/2022-04/edpb_rules_of_procedure_version_8_adopted_20220406_en.pdf (Erişim Tarihi: 29.05.2023)

[279] EDPB. (6 Nisan 2021). *Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment,* s.16, p. 66 https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_certification_criteria_assessment_formatted_en_0.pdf (Erişim Tarihi: 29.05.2023)

[280] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, s.22.

5.5. SERTİFİKASYON PROSEDÜRÜ

5.5.1. Uygunluk Değerlendirme ve Onay Süreci

GVK Tüzüğü'ne uygun şekilde bir sertifikasyon düzenlenmesi için (başvuru kapsamında talep edilen sertifikasyonun Avrupa Veri Koruma Mührü olup olmamasına göre) yetkili veri koruma otoritesi veya EDBP tarafından onaylanmış olan sertifikasyon kriterleri temelinde bir değerlendirme yapılmış olması gerekir[281]. Bu doğrultuda gerçekleştirilecek uygunluk değerlendirme süreci aşağıdaki sistematiği[282] takip etmelidir:

1) Veri sorumlusu veya veri işleyen tarafından, işleme faaliyetleri sertifikasyon mekanizmasına sunularak akredite sertifikasyon kuruluşuna veya uygun olduğu hallerde[283] yetkili veri koruma otoritesine bir başvuru yapılır.

2) Yapılan başvuru, sertifikasyon sağlamaya kuruluş tarafından değerlendirme sürecinin yürütülmesi için gereken tüm bilgi ve işleme faaliyetlerini içerir. Bu kapsamda değerlendirmenin nesnesine *(object of certification)* yer verilir. Değerlendirme nesnesi bir ürün veya sistem olabileceği, bir süreç veya prosedür veya bir sistem veya prosedür için bir kavram olabilecektir[284]. Değerlendirme nesnesinin ardından değerlendirme hedefinin yani ToE'nin açıklamasına yer verilir.

3) Sertifikasyon sağlamaya yetkili kuruluş tarafından ilk olarak başvuruya ilişkin resmi kontrol yapılır, bu bir nevi usulî kontrol mahiyetindedir. Bu aşamada başvurucu tarafından yer verilen ToE açıklamasının kabul edilebilir olup olmadığı, ayrıca veri sorumlusu veya veri işleyen tarafından

[281] Lambert, P. (2017). Understanding the New European Data Protection Rules (1st ed.). Auerbach Publications. https://doi.org/10.1201/9781315115269

[282] Tüm süreci gösteren tablo için bkz. EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,* s.9.

[283] Bu ifade ile kast edilen; ilgili üye devlet tarafından yetkili veri koruma otoritesinin kendisine tek başına veya ulusal akreditasyon kuruluşu ile birlikte akreditasyon sürecini yürütme konusunda yetki verildiği hallerdir.

[284] Bock, 2016, s.341.

kendisine sunulan dokümanların güncel ve eksiksiz olup olmadığı kontrol edilir. Sertifikasyon sağlamaya yetkili kuruluş tarafından yapılan resmi (usulî) kontrolde eksiklik tespit edilmezse, ön değerlendirme sürecine geçilir.

4) Ön değerlendirme sürecinde uygulanabilir sertifikasyon kriterleri ile değerlendirme metotlarının neler olduğu değerlendirilir.

5) Ön değerlendirme aşamasını takiben, esasa ilişkin değerlendirmeye geçilerek ToE'nin sertifikasyon kriterlerini karşılayıp karşılamadığı ve başvurucu tarafından sunulan dokümantasyon içeriğinin uygun olup olmadığı kontrol edilir. Bu aşamada bir eksiklik tespit edilmemesi halinde 'doğrulama' aşamasına geçilir.

6) Doğrulama aşamasında, sertifikasyon kriterlerinin ToE tarafından karşılanıp karşılanmadığı ve dokümantasyonun gereğince yapılıp yapılmadığı doğrulanır[285].

7) Doğrulama aşamasının ardından, akredite sertifikasyon kuruluşu tarafından sertifikasyon düzenlenmesine karar verilmesi halinde, ilgili karar gerekçeleri ile birlikte, yetkili veri koruma otoritesine[286] bildirilir[287].

8) Akredite sertifikasyon kuruluşu tarafından sertifikasyon düzenlenmesine karar verilmesi ve verilen kararın yetkili veri koruma otoritesine bildirilmesi üzerine, başvurucuya geçerli bir sertifikasyon sağlanır.

9) Tüm sertifikasyon mekanizmaları ve veri koruma mühürleri ile işaretleri EDPB tarafından ortak bir sicilde toplanır ve uygun yollarla kamuoyuna açıklanır.

---

[285] Aslında bu aşamanın bir önceki aşamanın teyidi niteliğinde olduğu söylenebilecektir.

[286] GVK Tüzüğü madde 43(5) kapsamında bu bilgilendirmenin yapılacağı organ, sertifikasyon kuruluşu olarak değil "supervisory authority" olarak hareket eder.

[287] Sertifikasyon sağlamaya yetkili kuruluş tarafından verilen kararın GVK Tüzüğü madde 43(5) yetkili veri koruma otoritesine (supervisory authority) bildirilmesi gerekmekle birlikte, verilen kararın yetkili veri koruma otoritesi tarafından reddedilip reddedilemeyeceğine ilişkin GVK Tüzüğü'nde düzenleme getirilmediğine Lauchard tarafından dikkat çekilmiştir. Ancak 14 Şubat 2023'te kabul edilen 'Guidelines 07/2022 on certification as a tool for transfers Version 2.0' başlıklı EDPB rehberinde, sertifikasyon sağlamaya yetkili kuruluş tarafından sertifikasyon düzenlenebilmesi için yetkili veri koruma otoritesinin iznine ihtiyacı duyulmadığı açıkça belirtilmiştir.

5.5.2. Sertifikasyonun Gözden Geçirilmesi

Yetkili veri koruma otoriteleri, sertifikasyon prosedürünün çeşitli aşamalarında aktif olarak yer alması ve bu çerçevede sertifikasyon sürecinin gidişatına etki edebilmesi sebebiyle oldukça önemli bir aktördür. Mevcut ve geçerli bir sertifikasyon ile ortaya konan uyum tasdiki, yetkili veri koruma otoritesi tarafından GVK Tüzüğü, Madde 57(1)(o) uyarınca periyodik olarak gözden geçirilecektir. Bu suretle, uyumun devamlılığını destekleyen ilave bir koruma mekanizması[288] getirilmiş olup öngörülen gözden geçirme yükümlülüğü ile hesap verebilirlik ilkesine önem atfedildiği görülür.

Periyodik gözden geçirme faaliyetlerinin ilgili mevzuata uyumun devamlılığı ile sürecin şeffaflığı açısından faydası yadsınamayacak olmakla birlikte, şeffaflık unsurunun güçlendirilmesi adına, sertifikasyondan faydalanan tarafların yetkili veri koruma otoritesine belirli aralıklarla ilgili sertifikasyon gerekliliklerinin karşılandığına dair bir faaliyet raporu sunması ve bu sayede geri bildirim vermesini içeren bir mekanizma kurulması düşünülebilir[289].

5.5.3. Sertifikasyonun Yenilenmesi

Sertifikasyon, GVK Tüzüğü'nün 42. maddesi kapsamında veri sorumluları veya veri işleyenlere sağlanan sertifikasyon azami üç yıllık bir süre sağlanır. Bu bakımdan uygunluk tasdikinin süresiz olarak verilmediği, 3 yıllık azami sürenin ise üst sınır olarak öngörülüp daha kısa süreli sertifikasyonun sağlanabileceğini belirtmek gerekir. GVK Tüzüğü'nün 42(7) maddesi, ilgili sertifikasyon gerekliliklerin sağlanmaya devam etmesi şartıyla, mevcut sertifikasyonun yenilenebileceğini düzenlemektedir. Bu madde, ilk başvuruda kullanılan şekilde ve aynı şartlar altında yenilenebilecektir.

[288] Kamara & De Hert (2018), s.20.
[289] Bu tarz bir uygulamanın CNIL certification'da olduğu görülmektedir (Sümer, 2019 s.108 & EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation,* s.15).

5.5.4. Sertifikasyonun Kaldırılması

Sertifikasyonun verilmesi ve yenilenmesi ile ilgili düzenlemelerin yanı sıra GVK Tüzüğü'nün 42(7) maddesi, sertifikasyon kriterlerinin sağlanmadığı veya artık yerine getirilmediği durumlarda, sertifikasyon akredite sertifikasyon kuruluşları tarafından geri çekilecektir.

GVK Tüzüğü'nün 40. ve 41. maddelerinde düzenlenen bir diğer hesap verebilirlik aracı olan davranış kurallarından farklı olarak, sertifikasyon rejimi kapsamında *sınırlı süreli, yenilenebilir*[290] *ve geri çekilebilir* bir uyum tasdiki söz konusu olduğundan, uyumun sürekli olarak sağlanması ve bunun ortaya konması oldukça önemlidir. GVK Tüzüğü'nün 42(7) maddesinde, sertifikasyonu kaldırma görev ve yetkisi olan taraflar sayılırken *"as applicable"* ifadesi kullanılmış olup bu madde GVK Tüzüğü'nün 43(4) maddesi ile birlikte okunduğunda, 42. maddedeki ifadenin mevcut sertifikasyonu sağlayan tarafa işaret etmek için kullanılmadığı anlaşılmaktadır.

5.6. YURT DIŞINA VERİ TRANSFER ARACI OLARAK SERTİFİKASYON

GVK Tüzüğü m.46(1) gereğince, Komisyon tarafından yeterlilik kararı verilmemiş olan hallerde, kişisel verilerin üçüncü ülkelere ve uluslararası organizasyona aktarılabilmesi için birtakım uygun güvenceler bulunması ve verilerin sahibi ilgili kişilerin hakları ile bu kişilerin başvurabileceği etkili yasal yolların mevcut olması gerekir. Aynı maddenin 2. fıkrasının (f) bendine göre, madde 46(2)'de üçüncü ülkelerde bulunan veri sorumluları veya veri işleyenler tarafından uygun güvenceleri uygulamaya yönelik yasal olarak bağlayıcı ve uygulanabilir taahhütler (veri sahibi ilgili kişilerin haklarına ilişkin olanlar dâhil) verilmesi kaydıyla ve bu taahhütlere ilave olarak onaylanmış bir sertifikasyon mekanizmasının varlığı halinde, bahsi geçen uygun güvencelerin sağlanabileceği

[290] Lachaud (2020), s.7.

düzenlenmiştir. O halde, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara hukuka uygun olarak aktarılıp aktarılmadığının tespitinde 2 aşamalı bir değerlendirme yapılması gerekir. Yapılacak değerlendirmenin ilk aşaması aktarım faaliyetlerinin GVK Tüzüğü'nün genel hükümlerine uygunluğu, ikinci aşaması ise GVK Tüzüğü'nün 5. bölümündeki (Chapter V) hükümlere uygunluğu içerir.

GVK Tüzüğü'nün uygun olarak üçüncü ülkelere kişisel veri transferi gerçekleştirilmesi kapsamında sertifikasyondan faydalanılabilecek hallerde, ilgili sertifikasyonun transferler için tasarlanmış olduğu söylenebilecektir. Bu doğrultuda EDPB tarafından Transferler İçin Tasarlanan Sertifikasyon özelinde hazırlanan rehber[291], sertifikasyon ve akreditasyon süreçleri ile ilgili detaylı açıklama ve yönlendirmelerin yer aldığı diğer EDPB rehberlerinin tamamlayıcısı niteliğinde olup sertifikasyonun AB dışına- yani üçüncü ülkelere- aktarıldığı durumlarda dikkate alınması gereken ek gereklilikleri ele almaktadır[292]. Bu rehberde kişisel verileri üçüncü ülkelere aktaran AEA içerisindeki ilgili taraf "data exporter (veri ihracatçısı)", bu verilerin aktarıldığı üçüncü ülkedeki taraf ise "data importer (veri ithalatçısı)" olarak tanımlanmaktadır. Bu bakımdan hem veri ihracatçısının hem de veri ithalatçısının farklı rollerde veri sorumlusu veya veri işleyen olarak hareket etmesi mümkündür[293]. Rehber kapsamında veri ihracatçısı ve veri ithalatçısına getirilen önemli sorumluluklar, genel çerçeveyi çizmek adına aşağıda kısaca ele alınacaktır.

[291] EDPB. *Guidelines 07/2022 on certification as a tool for transfers.*
[292] A.g.e., s.3.
[293] A.g.e., s.7.

5.6.1. Transfer Taraflarının Yükümlülükleri

5.6.1.1. Veri İhracatçısının Yükümlülükleri

AEA içerisindeki veri ihracatçısı tarafından GVK Tüzüğü'nün 5. bölümünde yer alan düzenlemelere uygunluğun sağlanması gerekli[294] olup veri ihracatçısının aşağıda yer verilen hususlarda[295] gerekli kontrolleri yapması beklenir:

(i) Sertifikasyonun geçerli olup olmadığı ve süresinin dolup dolmadığı

(ii) Gerçekleştirilmek istenen spesifik veri transferinin ve transit geçişlerin[296] sertifikasyon kapsamında olup olmadığı

(iii) İleriye dönük (onward) aktarımların sertifikasyon kapsamında olup olmadığı ve yeterli dokümantasyonun sağlanıp sağlanmadığı

(iv) Sertifikasyonu düzenleyen kuruluşun, ulusal akreditasyon kuruluşu veya yetkili veri koruma otoritesi tarafından akredite edilip edilmediği

(v) Transfer aracı olarak kullanılan sertifikasyonun, söz konusu transferle ilgili üçüncü ülkede yürürlükte olan yasa ve uygulamalar ışığında etkili olup olmadığı[297]

(vi) Veri ihracatçısının veri sorumlusu olup veri ithalatçısının veri işleyen olduğu hallerde, GVK Tüzüğü Madde 28 uyarınca taraflar arasında imzalanacak veri işleme sözleşmesi kapsamında ya da veri ihracatçısı ve veri ithalatçısının her ikisinin de veri sorumlusu olduğu hallerde ise taraflar arasında imzalanacak veri paylaşım sözleşmesi kapsamında, veri transfer aracı olan sertifikasyonun kullanılacağının belirtilmesi.

---

[294] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.8.

[295] A.g.e., s.10.

[296] GVK Tüzüğü'nün 42(1) maddesi kapsamında düzenlenen sertifikasyon, çoğunlukla transit geçişleri de kapsamaktadır. Buna karşın transit geçişler, bağlama bağlı olarak ve ancak belirli durumlarda transfer aracı olarak kullanılan sertifikasyonun kapsamına dâhil olabilmektedir. A.g.e., s.9.

[297] Veri ihracatçısı, üçüncü ülkede yürürlükte olan ilgili mevzuat ve uygulamalara ilişkin olarak veri ithalatçısının belgelendirilmiş değerlendirmesi kapsamında sertifikasyon kuruluşu gerçekleştirilen doğrulamaya güvenebilecektir. Bkz A.g.e., s.10.

5.6.1.2. Veri İthalatçısının Yükümlülükleri

Kişisel verilerin GVK Tüzüğü'nün 42(2) maddesi kapsamında AEA dışındaki üçüncü bir ülkeye hukuka uygun olarak aktarılabilmesi adına uygun güvence sağlayan mekanizmalardan transfer aracı olan sertifikasyona başvurulduğu durumlarda, üçüncü ülkedeki ilgili veri sorumluları ve veri işleyenlerinin uygun güvencelerin uygulanması bakımından taahhütler verilmesi zorunludur. Bu taahhütler, yasal olarak bağlayıcı ve uygulanabilir olması koşuluyla, sözleşmeye dayalı veya diğer yasal olarak bağlayıcı araçlar aracılığıyla verilebilir. Bu taahhütler ile ilgili veri sorumlusu veya veri işleyen, yürüteceği veri işleme faaliyetlerini sertifikasyon kurallarına uygun gerçekleştirileceğini, bulunduğu ülkede hâlihazırda yürürlükte olan ilgili mevzuat ve uygulamaların taahhütlerine uymasını engellemediğini, aksi halde söz konusu değişiklikleri veri ihracatçısına bildireceğini garanti eder[298]. Unutmamak gerekir ki; verilen taahhütler üçüncü ülkedeki veri sorumlusu veya veri işleyenlerin sertifikasyona katılmasına imkân verse de, fonksiyon bakımından GVK Tüzüğü'nün 46. maddesinde bahsi geçen uygun güvenceler arasında değildir[299].

Bazı yazarlar, GVK Tüzüğü'nün 42(2) maddesi kapsamında üçüncü ülkedeki kişilerin de sertifikasyona katılmasına izin vermesini, üçüncü ülkedeki veri ithalatçısının taahhüt vermesi gerekliliğini kişisel verileri işlenen gerçek kişiler tarafından bu taahhütlerin 'icra edilebilir' olmaması nedeniyle eleştirmiştir[300]. EDPB rehberine bakıldığında bu problematik açı, *"Üçüncü ülkedeki veri sorumluları veya veri işleyenlerce verilecek taahhütler, üçüncü 'taraf lehtar' konumundaki veri sahibi gerçek kişi tarafından da bağlayıcı ve uygulanabilir olmalıdır"* yaklaşımıyla ele alınmıştır[301].

[298] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.17.
[299] A.g.e., s.16.
[300] Kamara & De Hert (2018), s.29.
[301] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.16.

5.6.2. Özel Sertifikasyon Kriterleri ile Ek Özel Kriterler

Yukarıda bahsedildiği gibi, Transferler İçin Tasarlanan Sertifikasyona ilişkin 07/2022 sayılı ilgili EDPB rehberi, sertifikasyon mekanizmasının genel hatlarını ortaya koyan 1/2018 sayılı rehberi[302] temel alır. Transferler İçin Tasarlanan Sertifikasyon özelinde hazırlanmış olan rehber ile EDPB tarafından, sertifikasyonun üçüncü ülkelere transfer aracı olarak kullanılacağı durumlarda dikkate alınması gereken hususlar bakımından rehberlik sağlanır ve üçüncü ülke transferleri için sertifikasyon mekanizmasına dâhil edilmesi gereken 'özel sertifikasyon kriterleri[303]' açıklanır.

Anılan özel kriterler içerisinde, sertifikasyon mekanizmasının kapsamı ve değerlendirme hedefi (TOE, şeffaflık ve veri sahibi ilgili kişilerin hakları, teknik ve idari tedbirler hakkında kapsamlı ve detaylı düzenlemelere[304] yer verilmelidir. Bununla birlikte EDPB, transfer aracı olan sertifikasyonun, özel sertifikasyon kriterlerine ilave olarak ilgili rehberde yer verilen ek özel sertifikasyon kriterlerini[305] de içermesi gerektiğini ifade eder.

Özel sertifikasyon kriterlerinin onay süreci, çalışmanın 5.5.1. numaralı başlığı altında açıklanan onay süreci ile aynıdır. Bu doğrultuda özel sertifikasyon kriterlerinin EDPB tarafından onaylandığı senaryoda Avrupa Veri Koruma Mührü sağlanacaktır. Sertifikasyon kriterlerinin yetkili veri koruma otoritesi tarafından onaylandığı hallerde sağlanan sertifikasyonun aksine, AB genelinde geçerliliğe sahip olan Avrupa Veri Koruma Mührü ile tüm AEA üye devletlerinden bağlayıcı ve uygulanabilir taahhütler veren üçüncü ülkelere veri transferi yapılabilecektir[306].

---

[302] EDPB. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.*
[303] Özel sertifikasyon kriterlerinin kapsamına ilişkin açıklamalar için bkz. EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.3.
[304] Özel sertifikasyon kriterlerinin içeriğine ilişkin detaylar için bkz. A.g.e., s.12-13.
[305] Rehberde 7 ana başlıkta ele alınan ek özel sertifikasyon kriterleri ile ilgili detaylar için bkz. A.g.e., s.13.
[306] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.11.

Sertifikasyon kriterlerinin onay süreçlerinden farklı olarak, özel sertifikasyon kriterleri içerik bakımından farklılık arz eder. Bu kriterler içerisinde, ilgili sertifikasyon kurallarının ihlalini engellemek adına, veri ithalatçısı tarafından gerçekleştirilen işleme faaliyeti ile veri ithalatçısının bulunduğu üçüncü ülkenin ilgili mevzuat ve uygulamaları çerçevesinde değerlendirilme yapmasına yönelik gerekliliklere yer verilecektir.

5.6.3. Uygunluk Değerlendirme Sürecinde Dikkat Edilmesi Gerekenler

Sertifikasyon kuruluşu tarafından kişisel verilerin aktarılacağı üçüncü ülkede yürürlükte olan ilgili mevzuat ve uygulamalara ilişkin olarak veri ithalatçısının belgelendirilmiş değerlendirmesine ilişkin "doğrulama" işlemi[307], sertifikasyon kriterlerinin gerektirdiği şekilde gerçekleştirmelidir. Bu bağlamda, sertifikasyon kuruluşunun gerekli değerlendirmeyi eksiksiz ve doğru şekilde gerçekleştirebilecek yetkinliğe[308] sahip olması gereklidir. Sertifikasyon kuruluşunun, ilgili mevzuat veya uygulamalarda yapılacak ve ToE kapsamına giren veri işleme faaliyetleri bakımından etkisi olabilecek değişiklikleri izlemesi de gerekir[309]. Dolayısıyla, sertifikasyonun transfer aracı olarak kullanıldığı hallerde sertifikasyon kuruluşuna getirilen sorumluluk veri ithalatçısı tarafından yapılan değerlendirmenin doğrulanması ile sınırlı olmayıp üçüncü ülke yasal düzenlemelerinin sertifikasyon kuruluşu tarafından bizzat takibini de içerecektir. İlgili mevzuat veya uygulamaların takibi GVK Tüzüğü'nün 42(2) maddesi kapsamında veri ihracatçısı tarafından yürütülen veri işleme faaliyetlerinin uygunluğunun tespiti açısından yeterli olmayabileceği için sertifikasyon kuruluşu tarafından yürütülecek sertifikasyon sürecinin olası yerinde incelemeler[310] ile desteklenmesi uygun olacaktır[311].

[307] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.10, p. 21.
[308] Örnek için bkz. A.g.e., s.11-12.
[309] A.g.e., s.12.
[310] Yerinde incelemeden kasıt, incelemenin AEA dışındaki ilgili ülkede gerçekleştirilmesi anlamına gelir.
[311] EDPB. *Guidelines 07/2022 on certification as a tool for transfers,* s.12.

5.7. GVK TÜZÜĞÜ TAHTINDA ÖRNEK SERTİFİKASYON MEKANİZMALARI

95/46 sayılı Direktif'te sertifikasyon ile ilgili düzenleme öngörülmemiş olmakla birlikte bu araçların o dönemlerde dahi bazı üye ülkelerde uygulama alanına sahip olduğu görülmekteydi[312]. GVK Tüzüğü'nün 41 ve 42. maddesi doğrultusunda düzenlenen sertifikasyon mekanizmaları ile ilgili örnekler henüz sınırlı sayıda olmakla birlikte bunların zaman içerisinde daha da artması beklenmektedir.

Şimdiye kadar EDPB tarafından AB genelindeki uygulamalarda tutarlılık sağlanabilmesi kapsamında üç ayrı sertifikasyon şeması kapsamında görüş yayımlanmıştır. Bunlardan ikisi EDPB'nin Lüksemburg Veri Koruma Otoritesi tarafından sunulan Europrivacy sertifikasyon şeması ve taslak mahiyetindeki GDPR-CARPA sertifikasyon şemasına yönelik görüşlerini içerirken, diğeri ise Alman Veri Koruma Otoritesi tarafın sunulan EuroPrise sertifikasyon şeması ile ilgilidir. 8 Şubat 2022 tarihinde GPDR-CARPA sertifikasyon kriterlerine ilişkin vermiş olduğu görüş kapsamında EDPB, GVK Tüzüğü'nün tutarsız bir şekilde uygulanması sonucu doğabileceğinden bahisle içeriğinde birtakım değişiklikler yapılmasını önermiştir[313]. Yine 19 Eylül 2022 tarihli EDPB görüşü kapsamında, EuroPriSe benzer bir yaklaşım sergileyerek sertifikasyon kriterlerinin içeriği bakımından birtakım değişiklikler önermiştir[314]. Buna karşılık, Europrivacy sertifikasyon kriterleri ile ilgili 10 Kasım 2022 tarihli görüşünde EDPB, Europrivacy sertifikasyon kriterlerinin GVK Tüzüğü'nün tutarlı şekilde uygulanması sonucu doğuracağını belirtmiş ve bunları onaylayarak Avrupa Veri

[312] Çekin (2018), s.240, p.536.
[313] EDPB. (2022). *Opinion 01/2022 on the GDPR Carpa Certification Criteria.* https://edpb.europa.eu/system/files/2022-02/opinion_01-2022_gdpr-carpa_certification_criteria_en.pdf (Erişim Tarihi: 29.05.2023)
[314] EDPB (2022). *Opinion 2022/25 on the approval of the EuroPriSe certification criteria as a European Data Protection Seal.* https://edpb.europa.eu/system/files/2022-09/edpb_opinion_2022-25_europrisecertificationcriteria_en.pdf (Erişim Tarihi: 29.05.2023)

Koruma Mührü olarak kabul edilmesine karar vermiştir[315]. Ancak henüz GVK Tüzüğü madde 42(8) kapsamında EDPB tarafından resmi olarak sicile kaydedilerek ilan edilmiş onaylı bir sertifikasyon mekanizması EDPB'nin resmi internet sitesinde[316] bulunmamaktadır. Nihayetinde, GVK Tüzüğü ile getirilen kriterlere uygun olan GDPR-CARPA sertifikasyon mekanizmasını uygulamaya alan ilk ülke Lüksemburg olmuştur[317].

[315] EDPB (2022). *Opinion 28/2022 on the approval of EuroPrivacy certification criteria as EU data protection seal.* https://edpb.europa.eu/system/files/2022-10/edpb_opinion_202228_approval_of_europrivacy_certification_criteria_as_eu_data_protection_seal_en.pdf (Erişim Tarihi: 29.05.2023)
[316] EDPB. *Ana Sayfa.* https://edpb.europa.eu/edpb_en (Erişim Tarihi: 29.05.2023)
[317] European Data Protection Board. (2022). *CNPD adopts certification mechanism under GDPR (CARPA).* https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en (Erişim Tarihi: 29.05.2023)

ALTINCI BÖLÜM

TÜRK HUKUKUNDA HESAP VEREBİLİRLİK

6.1. MUHTELİF DÜZENLEMELERDE HESAP VEREBİLİRLİK

Türk hukukunda muhtelif düzlemlerde hesap verilebilirlik ile ilgili düzenlemelere yer verildiği görülmektedir. Son yıllarda hesap verebilirlik ilkesinin önemi özellikle kamu düzeni, kamu güvenliği ve kamu yönetimi kapsamına giren konularda sıklıkla vurgulanırken, kurumsal yönetim anlayışının bir gereği olarak özel sektör aktörleri ve kamuoyunu ilgilendiren konularda da hesap verebilirlik ilkesine önem atfedildiği görülmektedir. Çalışmanın bu kısmında, Türk hukukunun kişisel verilerin korunması dışında kalan diğer alanlarında hesap verebilirlik ilkesi ile ilgili düzenleme getiren temel kaynaklar ele alınacak ve bu sayede Türk hukukunda hesap verebilirlik ilkesine ne boyutta bir önem atfedildiği değerlendirilecektir.

6.1.1. Bilgi Edinme Hakkı Kanunu

24 Ekim 2003 tarih ve 25269 sayılı Resmi Gazete'de yayımlanmasının ardından 24 Nisan 2004 tarihinde yürürlüğe giren 4982 sayılı Bilgi Edinme Hakkı Kanunu ("4982 sayılı Kanun"), ilke olarak tüm gerçek ve tüzel kişilerin bilgi edinme hakkına sahip olduğunu düzenler. 4982 sayılı Kanun içerisinde düzenlenen bilgi edinme hakkı, demokrasi anlayışı doğrultusunda devlet yönetiminde şeffaf olunmasını amacıyla Türk hukukuna kazandırılmıştır. Şeffaf ve hesap verebilir bir yönetimin temini için AB müktesebatında yapılan düzenlemeler, bu ilkenin Türk hukukunda da kendisine yer etmesine öncülük etmiştir.

6.1.2. Kamu Mali Yönetimi ve Kontrol Mevzuatı

24 Aralık 2003 tarih ve 25326 sayılı Resmi Gazete'de yayımlanan 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun ("5018 sayılı Kanun") amacı; kamu kaynaklarının etkili ve verimli şekilde edinimi ve kullanımının yanı sıra, hesap verebilirliğin ve malî saydamlığın temin edilmesi için kamu malî yönetim yapısı ile mali işlemlere yönelik düzenlemeler getirilmesidir. 5018 sayılı Kanun bağlamında hesap verebilirlik türlerinden hem yönetsel (m.11) hem de siyasi hesap verebilirliğe (m.30, m.53) rastlanmaktadır.

Kamu idarelerinin, 5018 sayılı Kanun'un 55. maddesinde tanımlanan iç kontrol sistemlerinin oluşturulması, izlenmesi ve değerlendirilmesine ilişkin dikkate alınması gereken temel yönetim kurallarını içeren Kamu İç Kontrol Standartları Tebliği içerisinde de hesap verebilirlik kavramının açıkça zikredildiği görülür[318].

6.1.3. Kolluk Mevzuatı

6713 Sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanunun Uygulanmasına Dair Yönetmelik'te hesap verebilirlik ilkesi: *"Kolluğun eylemlerinden, ihmallerinden ve verdiği emirlerden şahsen sorumlu ve sıralı amirleri ile Türkiye Büyük Millet Meclisine karşı daima hesap verebilir olmasıdır."* denilerek tanımlanmış ve hesap verebilirlik temel ilkeler arasında sayılmıştır. Yine, kolluk personelinin görevini yürütürken uyması gereken ilkelerin belirlenmesi amacıyla hazırlanan Kolluk Etik İlkeleri içerisinde hesap verebilirlik ilkesinin zikredildiği görülmektedir.

[318] Hesap verebilirlik ilkesinin, Kamu İç Kontrol Standartları Tebliği'nin 1, 2 ve 14 numaralı maddelerinde zikredildiği görülür.

6.1.4. Kamu Görevlileri Etik Mevzuatı

5176 Sayılı Kamu Görevlileri Etik Kurulu ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun ("5176 sayılı Kanun") ile kurulan Kamu Görevlileri Etik Kurulu tarafından, kamu görevlileri tarafından uyulması gereken etik davranış ilkeleri belirlenecek ve bu ilkelere uygun davranılıp davranılmadığı gözetilecektir. Gerek 5176 sayılı Kanun'da gerek de bu kanunun 3. ve 7. maddelerine dayanılarak hazırlanan Kamu Görevlileri Etik Davranış İlkeleri İle Başvuru Usul ve Esasları Hakkında Yönetmelik[319] içerisinde, kamu görevlilerinin uyması gereken etik davranış ilkeleri arasında hesap verebilirlik ilkesine yer verilmiştir. Ayrıca, ilgili yönetmeliğin yöneticilerin hesap verme sorumluluğunu düzenleyen 20. maddesinde, yönetici konumundaki kamu görevlilerinin bağlı oldukları kamu kurumlarının amaç ve politikalarına uygun olmayan işlem veya davranışlarda bulunmalarının engellenmesi için alınması gereken tedbirler açıklanarak hesap verebilirlik ilkesine somut bir görünüm kazandırılmıştır.

6.1.5. Sayıştay Kanunu

6085 sayılı Sayıştay Kanunu, kamu idarelerinin mali faaliyet, karar ve işlemlerinin etkili, verimli, hukuka ve amaca uygun olarak yürütülüp yürütülmediği ile ilgili olarak Sayıştay tarafından Türkiye Büyük Millet Meclisi ("TBMM") adına denetlenmesine ilişkin hüküm ve koşulları belirler. 6085 sayılı Sayıştay Kanunu'nun amacı, kamu idareleri tarafından ilgili süreçlerin kamuda hesap verme sorumluluğu ve mali saydamlık esasları çerçevesinde yürütülmesinin sağlanmasıdır. Hesap verme sorumluluğunun temini bakımından Sayıştay'ın TBMM adına denetim yapma hakkı, T.C. Anayasası'nın 160. maddesinden kaynaklanır. Dolayısıyla Anayasa'da hesap verme sorumluluğunun temelinin atıldığını söylemek mümkündür.

[319] 13 Nisan 2005 tarih ve 25785 sayılı Resmi Gazete'de yayımlanan Kamu Görevlileri Etik Davranış İlkeleri İle Başvuru Usul ve Esasları Hakkında Yönetmelik.

AYM'nin 4 Aralık 2014 tarih ve 2014/184 sayılı kararı ile 28 Aralık 2016 tarih ve 2016/199 sayılı kararında[320] Sayıştay'a tanınan denetim yetkisinin önemi şu ifadeler kullanılarak vurgulanmıştır: "*Sayıştay denetimi, demokratik devlet ilkesinin bir gereği olarak yürütmenin, halka ve yasama organına hesap verme sorumluluğunun işlevselleştirilmesinin en önemli araçlarındandır.".*

6.1.6. Kamu İhale Kanunu

4734 sayılı Kamu İhale Kanunu'nun 5. maddesine göre, idarenin, kamu hukukuna tâbi olan veya kamunun denetimi altında bulunan veyahut kamu kaynağı kullanan kamu kurum ve kuruluşlarının yapacakları ihalelerin saydamlığını sağlama sorumluluğu vardır. Saydamlık ve hesap verebilirliğin madalyonun iki yüzü olduğu ve bu kavramlardan birinin diğeri olmadan pek anlam ifade etmediği[321] düşünüldüğünde, 4734 sayılı Kamu İhale Kanunu'nun da hesap verebilirlik ilkesiyle ilişkili olduğu söylenebilecektir.

6.1.7. Türk Ticaret Kanunu ile Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu

14 Şubat 2011'de Resmi Gazete'de yayımlanarak yürürlüğe giren 6102 sayılı Türk Ticaret Kanunu'nda ("6102 sayılı Kanun") 'hesap verme' ibaresinin sıklıkla kullanıldığı görülmektedir. Bunun sebebi, bu kanundan önce yürürlükte olan 29 Haziran 1956 tarihli ve 6762 sayılı eski kanunda hesap verebilirlik ve şeffaflıkla ilgili yeterince düzenleme bulunmaması ve yapılan kanun değişikliği ile bu

[320]4 Aralık 2014 tarih ve Esas:2013/114, Karar:2014/184 sayılı AYM kararına erişim için: https://www.resmigazete.gov.tr/eskiler/2015/07/20150716-29.pdf (Erişim Tarihi: 29.05.2023)
28 Aralık 2016 tarihli ve Esas:2016/21, Karar:2016/199 sayılı AYM kararına erişim için: https://www.resmigazete.gov.tr/eskiler/2017/02/20170207-8.pdf (Erişim Tarihi: 29.05.2023);
[321] Küçükaycan, D. (2020). *Mali Saydamlık ve Hesap Verebilirlik Aracı Olarak: Türk Sayıştayı'nın Performans Denetimi.* Denetişim, 0(20), s.38-39. https://dergipark.org.tr/tr/download/article-file/972251 (Erişim Tarihi:29.05.2023)

kavramın Türk ticaret hukukuna kazandırılmak istenmesiydi[322]. 6102 sayılı Kanunu'nun bağlı ve hâkim şirketlerle ilgili düzenlemeleri, ticaret şirketlerine değer biçilmesi ve anonim şirketlerin genel kurul ve esas sözleşme değişiklikleri ile ilgili kısımları ve son olarak donatma iştirakine ilişkin maddelerinde hesap verme ilkesinden bahsedilmektedir.

6102 sayılı Kanun'da yer verilen hesap verebilirlik ilkesi sayesinde; mali raporlamaların hesap verebilirlik anlayışına göre yapılması, azınlık haklarının korunması, riskin erken teşhis komitesinin oluşturulması ve ticarî sır niteliğindeki bilgiler hariç olmak üzere şirket ile ilgili bilgilerin kolay erişilebilir şekilde kamuya duyurulabilmesi gibi birçok fayda sağlanmıştır[323].

Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu ("KGK") ise, Türkiye'de muhasebe ve denetim standartlarının belirlenerek kamuya şeffaf ve güvenilir finansal raporlamalar yapılmasından sorumlu, bağımsız bir kuruluştur. KGK ile 6102 sayılı Kanun arasındaki ilişkiye bakıldığında, KGK tarafından getirilen düzenlemelerin 6102 sayılı Kanun'da yer verilen hesap verebilirlik ilkesini desteklediği ve bu ilkenin şirketlerce uygulanması amacına hizmet ettiği anlaşılmaktadır. Hesap verebilirlik ilkesinin uygulanması adına KGK tarafından getirilen muhasebe standartları sayesinde finansal tablolar doğru, şeffaf ve karşılaştırılabilir olacaktır. Ayrıca, KGK tarafından belirlenen denetim standartları ile bağımsız denetim süreçlerinin etkinliği artırılmış ve bu şekilde finansal raporların güvenilir olması sağlanmıştır. Muhasebe ve denetim standartlarının belirlenmesi dışında KGK, şirketlerin hesap verebilirlik ilkesine uyumlarının sağlanmasına yönelik denetim ve gözetim faaliyetleri de yürütmeye yetkilidir.

---

[322] Ertuğrul, A. N., & Cebeci, G. (2016). Kamu hukuku ve özel hukuk çerçevesinde hesap verebilirlik kamuda uygulanabilirliği ve çözüm önerileri. *Muhasebe Bilim Dünyası Dergisi*, 18(1), s.948.

[323] Karasu, R. (2013). 6102 Sayılı Türk Ticaret Kanunu ile Anonim Şirketlerde Kurumsal Yönetim ile İlgili Getirilen Yenilikler. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 4(2), s.46 & s.56-57; Gönen, S., & Yürekli, E. (2016). 6102 Sayılı Türk Ticaret Kanunu Açısından Kurumsal Yönetim İlkelerinin Değerlendirilmesi. *Journal of Accounting, Finance and Auditing Studies*, 2(4), s.139.

6.2. TÜRK VERİ KORUMA HUKUKUNDA HESAP VEREBİLİRLİK

Türk hukukunda, kişisel verilerin korunması ile ilgili konuların yasal çerçevesi KVK Kanunu ile çizilmiştir. Bu kanun 24 Mart 2016 tarihinde TBMM tarafından kabul edilerek 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanmış ve aynı gün yürürlüğe girmiştir. KVK Kanunu'nun 4. maddesi, kişisel veri işlenmesinde uygun davranılması gereken genel ilkeleri içerir.

6.2.1. KVK Kanunu Kapsamında Hesap Verebilirlik

KVK Kanunu'nun 4. maddesinde sayılan ilkeler; **(i)** hukuka ve dürüstlük kurallarına uygun olma, **(ii)** doğru ve gerektiğinde güncel olma, **(iii)** belirli, açık ve meşru amaçlar için işlenme, **(iv)** işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve **(v)** ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ile sınırlıdır. Yani hesap verebilirlik ilkesi ne KVK Kanunu'nda ne de kişisel verilerin korunması ile ilgili ikincil mevzuatta ele alınmıştır. KVK Kanunu'nun yürürlük tarihi ile GVK Tüzüğü'nün[324] Avrupa Parlamentosu'nda onaylandığı tarih yakın olsa da, KVK Kanunu'nun hazırlık çalışmalarının yapıldığı dönemde yürürlükte olan 95/46 sayılı Direktif'in KVK Kanunu'na mehaz teşkil etmesi sebebiyle bu durum pek de beklenmedik değildir.

Mehaz 95/46 sayılı Direktif'in 6(2) maddesinde veri sorumlusunun kişisel verilerin korunması ile ilgili mevzuata uymakla yükümlü olduğu düzenlenmiş, buna karşılık 95/46 sayılı Direktif'te veri sorumlusu tarafından ilgili mevzuata uyum yükümlülüğün yerine getirildiğinin gösterilmesi gerekliliğiyle ilgili herhangi bir düzenlemeye yer verilmemiştir. Hal böyle iken; 95/46 sayılı Direktif düzenlemelerini örnek alan KVK Kanunu'nda da hesap verebilirlik ilkesi açıkça zikredilmemiştir.

[324] AB Genel Veri Koruma Tüzüğü, Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde onaylanmış olup 25 Mayıs 2018 tarihinde resmen yürürlüğe girmiştir.

6.2.1.1. KVK Kurumu'nun Hesap Verebilirlik İlkesine Yaklaşımı

Kişisel verilerin korunmasına ilişkin AB hukukundaki düzenlemelere bakıldığında, veri sorumlusunun devlet tarafından denetlenmesi unsurunun daha arka planda kaldığı söylenebilecektir[325]. Henüz Türk hukuku bu noktaya gelmemiş olmakla birlikte, KVK Kanunu'nun lafzında hesap verebilirlik ilkesine yer verilmemesine rağmen KVK Kurumu'nun internet sitesinde yayımlanan bazı karar ve duyurularda[326] hesap verebilirlik ilkesine referans verildiği ve bu ilkenin benimsendiği görülmektedir. Üstelik 10 Mayıs 2023 tarihinde KVK Kurumu'nun düzenlediği bir seminerde, şeffaflık ve hesap verebilirliğin artan öneminin tartışıldığı görülmektedir. Nitekim KVK Kanunu'ndaki bazı düzenlemelerin de hesap verebilirlik ilkesi temel aldığı söylenebilecektir[327].

GVK Tüzüğü'nün 37. maddesinde sayılan belirli şartların sağlandığı durumlarda, veri sorumlusu tarafından veri koruma görevlisi (DPO) atanması gerekli olup DPO da hesap verebilirlik ilkesine hizmet eden araçlara bir örnektir. GVK Tüzüğü'nün aksine, KVK Kanunu'nda bu tarz bir aktöre yer verilmemiştir. Hatta KVK Kurumu tarafından 6 Aralık 2021 tarihinde yayımlanan bir duyuruda[328], 06.12.2021 tarih ve 31681 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar

---

[325] Çekin (2018), s.13, p.17.

[326] Kişisel Verileri Koruma Kurumu. 2019. *"25/03/2019 tarihli ve 2019/78 Sayılı Kararı".* Karar özetine erişim için: https://www.kvkk.gov.tr/Icerik/5434/2019-78 (Erişim Tarihi: 29.05.2023); Kişisel Verileri Koruma Kurumu. 2021. *"14/10/2021 tarihli ve 2021/1051 sayılı Kararı".* Karar özetine erişim için: https://www.kvkk.gov.tr/Icerik/7261/2021-1051 (Erişim Tarihi: 29.05.2023); Kişisel Verileri Koruma Kurumu. 2021. *"3/12/2021 tarihli ve 2021/1303 sayılı Kararı".* Karar özetine erişim için: https://www.kvkk.gov.tr/Icerik/7288/2021-1303 (Erişim Tarihi: 29.05.2023); Kişisel Verileri Koruma Kurumu. 2019. *"17/12/2019 Tarihli ve 2019/387 Sayılı Kararı".* Erişim için: https://www.kvkk.gov.tr/Icerik/6749/2019-387 (Erişim Tarihi: 29.05.2023); Kişisel Verileri Koruma Kurumu. 2019. *"Dernek, Vakıf ve Sendikalara Ait İktisadi İşletmelerin VERBİS'e Kayıt Yükümlülüğü Hakkında Duyuru".* Erişim için: https://www.kvkk.gov.tr/Icerik/6990/DERNEK-VAKIF-VE-SENDIKALARA-AIT-IKTISADI-ISLETMELERIN-VERBIS-E-KAYIT-YUKUMLULUGU-HAKKINDA-DUYURU (Erişim Tarihi: 29.05.2023).

[327] Bayram, Ö. B. (2022). Bir uyum aracı olarak veri koruma etki analizinin Türk hukuku bakımından değerlendirilmesi. *Kişisel Verileri Koruma Dergisi*, 4(1), 38-53.

[328] Kişisel Verileri Koruma Kurumu. 2021. *Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu.* İlgili duyuruya erişim için: https://www.kvkk.gov.tr/Icerik/7100/Veri-Koruma-Gorevlisi-Hakkinda-Kamuoyu-Duyurusu (Erişim Tarihi: 29.05.2023)

Hakkında Tebliğ ile Veri Koruma Görevlisi Belgelendirme Programı[329] kapsamında "Veri Koruma Görevlisi" olarak adlandırılan kişilerin, GVK Tüzüğü'ndeki DPO kavramıyla karıştırılmaması gerektiği açıklanmış, ayrıca Türk mevzuatında GVK Tüzüğü'nde düzenlenen bir kavramın bulunmadığı açıkça belirtilmiştir. Öte yandan, Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ'e göre, Veri Koruma Görevlisi sıfatını haiz gerçek kişilere sertifikasyon sağlanacağından bahsedilir. Burada bahsi geçen sertifikasyonun GVK Tüzüğü'nün 42. maddesine göre sağlanan sertifikasyon arasında işlevden ziyade isim benzerliği olduğu görülmektedir. Bu sebeple, ilgili tebliğde kapsamında sağlanacak sertifikasyon ile GVK Tüzüğü'nün 42 ve 43 maddelerinde düzenlenen sertifikasyon mekanizması karıştırılmamadır.

GVK Tüzüğü'nde öngörülen önemli hesap verebilirlik araçlarında bir diğeri olan bağlayıcı şirket kuralları da KVK Kanunu'nda düzenlenmemiştir. Fakat 2020 yılının Nisan ayında KVK Kurumu tarafından sahip olduğu genel düzenleyici yetkilere dayanılarak Bağlayıcı Şirket Kurallarına ("BŞK") ilişkin bir duyuru[330] yayımlanmış[331], ayrıca bu duyuru içerisinde konuyla ilgili düzenlemeler getiren

[329] Kişisel Verileri Koruma Kurumu. 2021. *Veri Koruma Görevlisi Belgelendirme Programı.* Program detaylarına erişim için: https://kvkk.gov.tr/Icerik/7094/VERI-KORUMA-GOREVLISI-BELGELENDIRME-PROGRAMI (Erişim Tarihi: 29.05.2023).

[330] Kişisel Verileri Koruma Kurumu. 2020. *BAĞLAYICI ŞİRKET KURALLARI HAKKINDA DUYURU*. İlgili duyuru ile Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman'a erişim için: https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU (Erişim Tarihi: 29.05.2023)

[331] KVK Kurumu, kişisel verilerin korunması bakımından kamu tüzel kişiliğine sahip olan, kamu gücünü kullanan düzenleyici ve denetleyici bir makamdır. Başka bir deyişle, KVK Kanunu'nun yürütülmesi ve denetlenmesi görevi KVK Kurumu tarafından yerine getirilmektedir. Bu kurum, KVK Kurulu ve KVK Başkanlığından oluşur. KVK Kanunu'nda veri koruma görevlisi ile ilgili herhangi bir düzenleme yer almamasına rağmen, Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ ile veri koruma görevlisi hakkında düzenlemeler getirilmiştir. Bu tebliğin kanuni dayanağı KVK Kurulu'nun görev ve yetkilerini düzenleyen KVK Kanunu 22 maddesinin e bendi olup ilgili maddede KVK Kurulu'nun yetkileri arasında "Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak" sayılmıştır. Tebliğler idare hukukunun düzenleyici işlemlerinden sayılır. Yine veri koruma görevlisi konusuna benzer şekilde, KVK Kanunu'nda açıkça düzenlemeyen ve AB veri koruma hukukunda kendisine yer bulmuş ortak veri sorumlusu (joint controller) kavramının da KVK Kurulu tarafından verilen bir karara konu edildiği görülmektedir. İlaveten, KVK Kurumu'nun yayımladığı bir duyuru aracılığıyla getirilen Bağlayıcı Şirket Kuralları'na ilişkin düzenlemeler de KVK Kanunu'nda açıkça zikredilen veri aktarım araçlarından değildir. Anılan tüm bu düzenlemeler dikkate alındığında, bu işlemlerin KVK Kanunu'nun Kurum'un yetkisini düzenleyen 20. maddesi ile Kurul'un yetkisini düzenleyen

yardımcı dokümana yer verilmiştir[332]. Söz konusu yardımcı dokümana göre hesap verebilirlik ilkesi, BŞK'nın uyumluluk kriterlerinden biri olarak kabul edilir.

Yine GVK Tüzüğü'nde öngörülen temel hesap verebilirlik araçlarından olan veri koruma etki değerlendirmesi (DPIA) de KVK Kanunu'nda düzenlenme alanı bulunmamaktadır. Buna karşın, KVK Kurumu'nun "Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" adlı yayınında[333], veri işleme faaliyetlerinin hukuka uygun yürütülüp yürütülmediğinin tespitinde işleme faaliyetleri bakımından söz konusu olan riskin düzeyine göre mahremiyet etki değerlendirmesi yapılması önerilmiştir. Burada önerilerin mekanizmasının GVK Tüzüğü'ndeki DPIA eşleniği bir mekanizma olduğu söylenebilecektir[334].

---

22. maddeleri dâhilinde kalıp kalmadığı tartışılabilir. KVK Kurumu'nun KVK Kanunu ile ilgili düzenlemeler yapması ve bu konuda hukuken yetkili olması, KVK Kanunu'nun yürütülmesi ve denetlenmesi görevinin kendisine yasayla tanınmış olmasıyla açıklanabilecektir. Ancak, KVK Kurumu tarafından herhangi bir düzenleyici işlem yapılırken KVK Kanunu'nun ilgili hükümleri ve bu hükümlerde kendisine tanınan yetkilerinin sınırlarına dikkat edilmelidir. Bu doğrultuda, KVK Kurumu tarafından GVK Tüzüğü'nde yer alan ancak KVK Kanunu'nda yer düzenlenmeyen davranış kuralları ve sertifikasyon mekanizmaları gibi hesap verebilirlik araçlarına ilişkin düzenlemeler getirmesi halinde, bu düzenlemelerin KVK Kurumu'nun yetki ve görevleri dâhilinde kalıp kalmayacağı ve hukukiliği değerlendirilmelidir. Zira KVK Kurumu'nun bu konularda bir adım atması mehaz AB mevzuatına uyum açısından olumlu olsa bile, bu düzenlemelerin ilgili mevzuatta KVK Kurumu'na tanınan yetki çerçevesinde olması önemli olduğu gibi hukukun genel ilkelerine ve diğer mevzuata uygun olması gerekir. Zira KVK Kurulu'nun düzenleyici işlem yapması yetkisi Kurulun görev alanı ile Kurumun işleyişine ilişkin konularla sınırlıdır. KVK Kurumu tarafından davranış kuralları veya sertifikasyon gibi KVK Kanunu'nda ve ilgili ikincil mevzuatta yer bulmayan kavramlara ilişkin düzenlemeler yapılması, Kurum'un işleyişiyle ilgili olmadığı gibi KVK Kanunu'nun 22. maddesinde sayılan KVK Kurulu'nun görev ve yetkileri arasında da görülmeyebilir, zira bu durumda tanınan yetkilerin çok geniş yorumlandığı düşünülebilir. Bu durumda yetkisiz şekilde gerçekleştiren işlemin yok hükmü sayılması bile mümkün olabilecektir. Dolayısıyla GVK Tüzüğü'nde düzenlenen hesap verebilirlik ilkesi ve/veya davranış kuralları, sertifikasyon gibi çeşitli hesap verebilirlik araçlarının KVK Kurumu tarafından yapılan düzenlemeler ile öngörülmesi yerine, KVK Kanunu'nun bu hususlarda yapılacak düzenlemeleri içerecek şekilde güncellenmesiyle Türk hukukunun bir parçası haline getirilmesi hukuken daha doğru olacaktır. Ardından, gerekli olur ise, kanunda yer alan mekanizmaların açıklanması, detaylandırılması vb. sebeplerle KVK Kurulu tarafından bu konularda düzenleyici işlemler öngörülmesi mümkün olabilir. Hatta hesap verebilirlik araçlarının KVK Kanunu'nda kendilerine yer bulmaları üzerine, KVK Kanunu'nun 20. maddesinin c bendi kapsamında Kurum'un ulusal ve/veya uluslararası kuruluşlarla iş birliği yapma yetkisi dâhilinde, KVK Kurumu'nun standardizasyon konusunda uzmanlığa sahip olan kuruluşlarla iş birliği kurarak sertifikasyon koşulları gibi konularda çalışmalar yapması gündeme gelebilecektir.

[332] Kaya (2020), s. 1889.

[333] Kişisel Verileri Koruma Kurumu. 2022. *Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler*. Erişim için: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf s.11. (Erişim Tarihi: 29.05.2023).

[334] Bayram (2022), s.49.

KVK Kanunu'nda hesap verebilirlik ilkesiyle ilişkilendirilebilecek bir diğer husus ise, Veri Sorumluları Sicili'ne kayıt yükümlülüğüdür. Kanunun 16. maddesine göre, veri sorumlusu sıfatıyla kişisel veri işleyen gerçek ve tüzel kişilerin KVK Kurulu tarafından öngörülen istisnalara tabi olmamaları durumunda, veri işleme faaliyetlerine başlamadan önce Veri Sorumluları Sicili'ne kaydolmaları zorunludur. Bu yükümlülüğün yerine getirilmesi ile veri işleme süreçleri kayıt altında alınacaksa bile, hesap verebilirliğin önemli çıktılarından olan detaylı ve nitelikli bir kayıt tutmadan bahsetmek pek mümkün değildir[335]. Yine hesap verebilirlik ilkesi ile ilişkili olarak, KVK Kanunu ve ilgili ikincil düzenlemelerinde veri sorumluları tarafından hazırlanması zorunlu tutulmuş bazı temel politikalar kabul edilebilir[336].

Kısa bir süre önce KVK Kurumu'nun internet sitesinde toplu bir şekilde yayımlanan Şubat 2022 – Mart 2023 dönemine ait KVK Kurulu'nun verdiği karar özetlerinde[337] bakıldığında, KVK Kurulu'nun hesap verebilirlik konusundaki yaklaşımı bakımından bir karar[338] öne çıkmaktadır. 01/09/2022 tarihli ve 2022/853 sayılı bu kararda, *"bugün için kişisel verilerin korunması hukukunda veri sorumluları bakımından hâkim ilkenin hesap verebilirlik olduğunun kabul edildiği"* açıkça ifade edilmiştir. Ayrıca kararda, hesap verebilirlik ilkesinden bahsetmekle yetinilmemiş ve KVK Kurulu'nun 2020/966 sayılı İlke Kararı'na atıf yapılarak hesap verebilir olmanın ne anlama geldiği açıklanmıştır. KVK Kurulu'na göre hesap verebilirlik ilkesi, veri sorumlusuna proaktif bir özen yükümlülüğü getirmektedir.

---

[335] Öyle ki, hesap verebilirliğin Türk hukukunda GVK Tüzüğü'ndeki anılan şekliyle uygulandığı bir durumda Veri Sorumluları Sicili gibi araçlara ihtiyaç bile kalmaz. İlgili görüş için bkz. A.g.e., s.1892.

[336] A.g.e., s.1892.

[337] Kişisel Verileri Koruma Kurumu. 2023, Nisan. *Kişisel Verileri Koruma Kurulu'nun Yeni Yayımlanan Karar Özetleri.* Erişim için: https://www.kvkk.gov.tr/Icerik/7601/Kisisel-Verileri-Koruma-Kurulu-nun-Yeni-Yayimlanan-Karar-Ozetleri (Erişim Tarihi: 29.05.2023).

[338] Kişisel Verileri Koruma Kurumu. 2023, Nisan. *"Bir yasal bahis platformu tarafından ilgili kişinin e-posta adresinin işlenerek bir üyesinin kişisel verilerinin üçüncü şahıs konumundaki ilgili kişinin e-posta adresine gönderilmesi" hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/853 sayılı Karar Özeti*. https://www.kvkk.gov.tr/Icerik/7576/2022-853 (Erişim Tarihi: 29.05.2023).

Ayrıca, 01/09/2022 tarihli ve 2022/853 sayılı bu kararda özen yükümlülüğünün çerçevesi çizilirken KVK Kanunu'nda kişisel verilerin güvenliğini sağlanması için alınacak teknik ve idari tedbirler/önemlere referans verilmiş, bu bağlamda "makul" ve "gerekli" ibarelerine dikkat çekilmiştir. Bu iki ibarenin kanun koyucu tarafından getirilmesinin sebebi olarak ise "*hesap verilebilirliğin veri sorumlusunun faaliyetine bağlı olarak daralıp genişleyebilecek"* olmasını göstermiştir. O halde, KVK Kurulu tarafından da hesap verebilirlik ile risk temelli yaklaşım kavramları arasında ilişki kurulduğu ve yorum yoluyla GVK Tüzüğü düzenlemelerine yaklaşıldığı söylenebilir.

KVK Kanunu'nun kapsamındaki veri sorumlularının GVK Tüzüğü'ne benzer şekilde hesap verebilir hale geldiklerinden bahsedilebilmesi için, Türk hukukunun daha uzunca yollar katetmesi gerekir. Bununla birlikte, KVK Kurulu tarafından son dönemde verilen kararda hesap verebilirlik ilkesinin açıkça zikredilmesinin bu yönde olumlu bir adım olduğu kabul edilebilecek, hatta KVK Kanunu'nda yapılacak değişikliklerin habercisi olduğu düşünülebilecektir.

6.2.2. KVK Kanunu Reform Çalışmaları

Esasen KVK Kanunu'nda değişikliği gidilmesi bir süredir gündemdedir, fakat gerçekleştirilmesi öngörülen değişikliklerin kapsamı henüz tam anlamıyla bilinmemektedir. Öte yandan mevcut konjonktüre bakıldığında, KVK Kanunu'nda yapılacak değişikliklerin öncelikli olarak Türk veri koruma hukukunun uygulanması bakımından sıklıkla sorun ve soru işaretine yol açan özel nitelikli kişisel verilerin işlenmesi (madde 6) ile kişisel verilerin yurt dışına aktarımı (madde 9) konularını ele alması beklenmektedir.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı tarafından hazırlanarak 18 Temmuz 2019 tarihinde TBMM tarafından onaylanan 11. Kalkınma Planı'nda, doğrudan kişisel verilerin korunması mevzuatı ile ilgili olmasa dahi iyi yönetişim bakımından hesap verebilirliğin önemi vurgulanmıştır. Ayrıca 2019-2023 yıllarını

kapsayan söz konusu Kalkınma Planı, KVK Kanunu'nun GVK Tüzüğü'nün esas alınarak güncellenmesi ile ilgili genel bir hedef de koymaktadır[339]. Tıpkı Türkiye Cumhuriyeti Adalet Bakanlığı'nın hazırladığı Mayıs 2019 yayın tarihli Yargı Reformu Stratejisi ile 11. Kalkınma Planı'nda olduğu gibi, İnsan Hakları Eylem Planı'nda da kişisel verilerin korunmasıyla ilgili hedeflere yer verilmiştir. Bu hedefe göre, KVK Kanunu'nun Avrupa Birliği standartları ile uyumlu hale getirilmesi için gerekli çalışmalar yapılacaktır. Yine en son 2023 Yılı Cumhurbaşkanlığı Yıllık Programı'nda hesap verebilirlikten bahsedildiği görülmüş, fakat KVK Kanunu'ndaki genel ilkeler arasına hesap verebilirlik ilkesinin eklenmesi konusunda henüz net bir adım atılmamıştır.

Tüm bu bilgiler ışığında, KVK Kanunu'nda yakın dönemde değişikliğe gidileceği ve en azından orta veya uzun vadede hesap verebilirlik ilkesinin de normatif olarak düzenleneceği öngörülmektedir.

[339] Kaya (2020), s. 1889.

SONUÇ

Gerek AB mevzuatındaki farklı alanlarda gerek AB mevzuatının ötesine geçen çeşitli düzenlemelerde kendisine yer bulan hesap verebilirlik ilkesi, normatif anlamda ilk olarak GVK Tüzüğü sayesinde AB veri koruma hukukunun parçası haline gelmiştir. GVK Tüzüğü ile çizilen hesap verebilirlik çerçevesine göre, veri sorumlusunun ilgili mevzuattan doğan yükümlülüklerini yerine getirmenin yanı sıra ilgili mevzuata uyumluluğu da ortaya koyması gerekir. O halde hesap verebilirlik, esasında veri sorumlusunu olduğundan daha özenli davranmaya itmekte, bir nevi veri sorumlusuna artırılmış bir özen yükümlülüğü getirmektedir.

Hesap verebilirliğe hizmet edebilmesi için GVK Tüzüğü'nde çeşitli araçlar öngörülmüş olup bunlardan yalnızca birkaçı gönüllülük esasına dayanmaktadır. Gönüllü hesap verebilirlik araçlarının doğası gereği "hazırlayan" ve "faydalanan" aynı taraftır ve dolayısıyla bu araca başvuran ilgili tarafın daha fazla dâhiliyetini gerektirir. Gönüllülük esasına dayanan hesap verebilirlik araçlarının diğerlerine kıyasla daha fazla efor gerektirmesi, veri sorumlusu tarafından ortaya konan uyum eforunu da artıracaktır. Bu yönüyle gönüllülük esasına dayanan araçlar, anılan ilkeye hizmet anlamında büyük öneme sahiptir.

Onaylı davranış kuralları veya sertifikasyona katılmış tarafların GVK Tüzüğü'nü ihlal ettiği hallerde anılan hesap verebilirlik araçlarından birine veya her ikisine birden sahip olmasının, ilgili merciler nezdinde hafifletici sebep sayılabilmesi de bundandır. Bu sebepledir ki çalışma, GVK Tüzüğü'nün getirdiği gönüllü hesap verebilirlik araçlarından davranış kuralları ve sertifikasyon mekanizmalarına odaklanır. Çalışma esnasında ampirik (nicel) veya karma araştırma yöntemlerine başvurulmamakla birlikte, konunun daha net anlaşılabilmesi amacıyla davranış kuralları ve sertifikasyon mekanizmalarının uygulamada karşılaşılan bazı örneklerine -gerekli görüldüğü ölçüde- yer verilmiştir. AB mevzuatının aksine, hesap verebilirlik ilkesinin Türk veri koruma hukukunda sınırlı bir karşılığı olması sebebiyle çalışmanın son bölümünde daha

genel çerçevede değerlendirme yapılmış ve bu esnada yer yer AB mevzuatı ve Türk hukuku mukayese edilmiştir.

GVK Tüzüğü'nün yürürlüğünden sonra özellikle de son yıllarda-AB mevzuatının parçası haline gelen veya ilerleyen dönemlerde gelmesi planlanan bilişim ve teknoloji hukukuyla ilgili yasal düzenlemelerin- oldukça detaylı ve bağlayıcı düzenlemeler getirmesi, AB'de norm temelli yaklaşımın yerine ilke temelli yaklaşımın tercih edilmeye başladığı şeklinde yorumlanabilecektir. Buna karşın, ilke temelli yaklaşımdan tamamen uzaklaşılması özellikle de GVK Tüzüğü gibi AB hukukunda nispeten oturmuş bir uygulamaya sahip düzenlemeler açısından gerekmediği gibi pek beklenmemektedir de.

Davranış kuralları ve sertifikasyon arasında birbirini tamamlayıcı bir ilişki mevcuttur. Bunların geçerlilik kazanabilmesi için takip edilecek usule ilişkin süreçler benzerdir. Bunlardan her ikisi de öz-düzenleme yöntemiyle hazırlanır, ardından GVK Tüzüğü'nde öngörülen ilgili otoriteler ile iş birliği yapılarak başvuru ve onay süreçlerinin tamamlanması kaydıyla geçerlilik kazanır. İlgili otoriteler ile kurulan iş birliği sayesinde, onaylı davranış kurallarına veya sertifikasyon mekanizmalarına katılan veri sorumluları veya veri işleyenler üzerinde yetkili veri koruma otoriteleri tarafından daha etkili bir denetim gerçekleştirilmesi de mümkün olur. Bir yandan daha az maliyetle daha etkili bir denetim sağlanırken, diğer yandan veri işleme faaliyetlerinin güvenliği için daha fazla sorumluluk alınmaktadır.

GVK Tüzüğü kapsamında hesap verebilir olmak demek, ilgili mevzuata uyumu ortaya konmak demektir. Uyum kavramı tek seferlik bir işlemden ziyade bir sürece işaret ettiğinden, mevzuata uyum ve dolayısıyla hesap verebilirlikten bahsedebilmek için "süreklilik" bulunmalıdır. Davranış kuralları ve sertifikasyon bakımından bu sürekliliğin temini, izleme veya denetleme yetkisi verilen birtakım kuruluşlar tarafından takip edilir. Şüphesiz ki, uyumun sürekliliğinden ve bunun takibinden bahsedilmesi için, daha en başından ilgili mevzuata uyumun sağlanmış

olması gerekir. Dolayısıyla, mevzuata uyumluluğun gösterilmesi için hesap verebilirlik araçlarına başvurulduğu hallerde, GVK Tüzüğü'nün öngördüğü şartların yerine getirilmesi önemlidir. Davranış kuralları ve sertifikasyon, mevzuata uyumun belgelenmesi bakımından oldukça elverişli hesap verebilirlik araçlarındandır. Onaylı davranış kurallarının veya sertifikasyonun varlığı tek başına ilgili mevzuata uyumluluğu kanıtlamasa da uyumluluk iddiasının ispatı açısından bir karine yaratır.

Davranış kuralları ve sertifikasyonun her ikisinin de sektör odaklı çözümler sunması ve bu doğrultuda GVK Tüzüğü'nün 24. maddesinde öngörülen veri güvenliğine yönelik yükümlülüklerin yerine getirilmesi bakımından risk temelli yaklaşıma başvuruyu desteklemesi, veri işleme faaliyetlerinin git gide komplike hale geldiği ve bir sorunun tek doğru cevabının olmadığı çağımızın gerçekliğiyle örtüştüğünü göstermektedir. Ayrıca, temel fonksiyonu üçüncü ülkelere veri aktarımı olmasa bile, her iki aracın, GVK Tüzüğü'nde öngörülen özel başvuru prosedürlerine uyularak onaylanması halinde AB dışında veri aktarım aracı olarak kullanılması mümkündür. Özellikle dijital hizmetler gibi sınır ötesi şekilde hizmetlere başvurulduğu bu yeni yüzyılda, kişisel verilerin güvenli şekilde üçüncü ülkelere aktarılmasına imkân veren bu tip araçlardan faydalanılması gerek operasyonel gerek ticari anlamda kuruluşlara avantaj sağlayacaktır.

Davranış kuralları ve sertifikasyonun birbirlerinin tamamlayıcısı olduğu kabul edildiğinden, bu araçlardan birinin tek başına varlığı, bazen yeterli olmayabilir. Zira bu araçlardan her ikisi de uyum belgelenmesine hizmet eder, ancak bunlardan yalnızca sertifikasyon uyumu tasdik etmektedir. Davranış kuralları ise bir tasdikten ziyade, davranış kurallarını benimseyen kuruluşun veri işleme faaliyetlerini hukuka uygun şekilde gerçekleştirilmesini amaçlayan kurallar bütünüdür.

GVK Tüzüğü'nün 42 ve 43 maddeleri ile, yetkili veri koruma otoritesine hem sertifikasyon sağlama yetkisi, hem de sertifika sağlamak üzere yetkili hale

gelebilmek için akredite edilmesi gereken sertifikasyon kuruluşlarına akreditasyon sağlama yetkisi tanınması endişe vericidir. GVK Tüzüğü'nün yetkili veri koruma otoritesine tanıdığı sertifikasyon ve akreditasyon yetkileri bakımından yeterince net sınırlar çizmemiş olması çıkar çatışması yaratabilecek bir alan yaratmıştır. Ayrıca GVK Tüzüğü'nün 43. maddesinin 1. fıkrasında akreditasyon sağlanması bakımından yetkili kuruluşlar belirtilirken "biri veya her ikisi" denilerek yine belirsiz bir düzenlemeye yer verilmiştir. Sertifikasyon sürecinin gönüllülük esasına dayanan ve nispeten pahalı bir süreç olduğu düşünüldüğünde, GVK Tüzüğü'ndeki sertifikasyon ile ilgili düzenlemelerin net olması önemlidir. Aksi durumda veri sorumluları ve veri işleyenler bu araca başvurmaktan imtina edebilirler. Dahası, davranış kuralları ve sertifikasyon mekanizmalarından Komisyon tarafından hakkında genel geçerlilik kararı verilmemiş olanların tüm AB üye devletlerce geçerli kabul edilmemesi ihtimali olduğundan, mevzuata uyumun belgelenmesi için bu araçlara başvuran tarafların yeterli faydayı sağlamama ihtimali vardır. Ancak anılan tüm bu eksikliklere rağmen, davranış kuralları ve sertifikasyon, hesap verebilir olma anlamında oldukça etkili araçlardır. Teoride bu araçlar oldukça etkili gözükmekle birlikte, GVK Tüzüğü'nün GVK Tüzüğü tahtında onaylanan davranış kuralları ve sertifikasyon örnekleri ise oldukça sınırlıdır. Bu nedenle çalışmaya uygulamadan arzu edilen miktarda örnek konu edilmesi mümkün olmamıştır.

GVK Tüzüğü'nün davranış kuralları ve sertifikasyonu düzenleyen maddelerinin nasıl uygulanması gerektiği EDPB tarafından çıkarılan rehberler sayesinde netleştikçe bu konularda yapılan çalışmalar ve başvurular artmaya başlamıştır. Son yıllarda özel sektördeki kuruluşlar tarafından kişisel verilerin korunmasına atfedilen önemin de arttığı görülür. Bunun sebeplerinden, veri koruma mevzuatının ihlali nedeniyle verilen cezaların gün geçtikçe artmasıdır. GVK Tüzüğü'nün ihlali durumda ilgili kuruluşun yıllık cirosu üstünden yapılan hesaplama ile belirlenen ceza tutarları ciddi oranları bulabilmektedir. Bir diğer sebep ise, ilgili mevzuata uyumun ötesine geçerek uyumluluğun ortaya konularak piyasadaki rakipler karşısında avantaj kazanılması olabilir.

Hesap verebilirlik ilkesi, Türk veri koruma hukukunun normatif düzenlemelerinde yer almasa da, KVK Kanunu ile KVK Kurul kararı birlikte değerlendirildiğinde, benzer etkiye sahip veya bu ilkeyi anımsatan birtakım düzenlemeler olduğu görülür. Yine de hâlihazırda kişisel verilerin koruması ile ilgili Türkiye'de yürürlükte olan yasal düzenlemelerin yetersiz kaldığı görülmektedir. Teknolojinin gelişmesiyle, özellikle de kişisel verilerin odakta olduğu sosyal medya gibi mecra ve sair platformların kullanımının artmasıyla, bireylerin temel hak ve özgürlüklerinin korunması zorlaşmaktadır. Bu bağlamda kişisel verilerin güvenliğinin sağlanmasının yanı sıra, bu hususun ispatı da oldukça önemlidir. Bu sebeple hesap verebilirlik ilkesinin Türk veri koruma hukukundaki normatif düzenlemelerden biri haline gelmesi ve şeffaflık ilkesiyle desteklenmesi ümit edilmektedir. Zira, veri sorumlusuna hem iç hem de dış süreçler bakımından artırılmış bir özen yükümlülüğü getiren hesap verebilirlik sayesinde kişisel verilerin daha etkin bir biçimde korunması mümkün olacaktır.

Hesap verebilirlik ilkesinin KVK Kanunu'nda en azından orta veya uzun vadede kendisine yer bulması beklenmektedir. Türk hukukunda, özellikle de son yıllarda, bu ilke daha fazla zikredilmeye başlanmıştır. Örneğin, 11. Kalkınma Planı içerisinde 'hesap verebilirlik' kavramından bahsedildiği görülmektedir. Benzer şekilde 2023 Yılı Cumhurbaşkanlığı Yıllık Programı'nda da hesap verebilirlik kavramı anılmıştır. Bu kavramın kişisel verilerin korunması temelinde değilse bile iyi yönetişim temelinde anılmış olması dahi hesap verebilirlik ilkesine önem atfedildiğinin göstergesidir. Hükümet nezaretinde yürütülen çalışmalarının yanı sıra, KVK Kurulu tarafından verilen kararlarda da hesap verebilirlik ilkesinden bahsedildiği görülür. Özellikle son dönemlerde KVK Kurulu kararlarına da sıklıkla konu olan bu ilkenin KVK Kurumu tarafından da benimsendiği açıktır. Dolayısıyla, tüm bunlar hesap verebilirlik ilkesinin Türk veri koruma hukukuna kazandırılacağının habercisi olabilir.

2019-2023 yıllarını kapsayan 11. Kalkınma Planı ile sırasıyla 2019 ve 2021 yıllarında yayınlanan Yargı Reformu Stratejisi ve İnsan Hakları Eylem Planı

içerisinde, KVK Kanunu'nun AB müktesebatı çerçevesinde gözden geçirilmesi ve Avrupa Birliği standartlarına uyumlaştırması ile ilgili hedeflere yer verildiği ve bu kapsamda KVK Kanunu'nun GVK Tüzüğü dikkate alınarak güncellenmesinin planlandığı görülmektedir. Günümüzde kişisel verilerin korunması bakımından AB mevzuatı ile uyumlu hale gelinmesi için birtakım çalışmalar yapıldığı ve kanun değişikliği önerilerinin çeşitli kurum ve kuruluşların görüşüne sunulduğu bilinmekle birlikte, henüz normatif anlamda bir değişiklik gerçekleştirilememiştir. Uzun süredir gündemde olan mevzuat değişikliğinin öngörülenden daha uzun sürmesinin COVID-19 pandemisi dâhil olmak üzere birçok küresel ve/veya ulusal boyutlu sebebi olabilir.

GVK Tüzüğü'nün dikkate alınması suretiyle KVK Kanunu'nda yapılacak değişikliklerin kapsamı ve detayı şu aşamada tam anlamıyla öngörülemese de, piyasadaki aktörlerin olası değişiklikler bakımından tahminleri vardır, zira KVK Kanunu'nda değişiklik yapılması bir süredir gündemdedir. Nitekim Türk veri koruma mevzuatında yapılacak değişiklerin, mevzuatı GVK Tüzüğü'ne ne ölçüde uyumlu hale getirmesine ihtiyaç olduğu da tartışmaya açıktır. KVK Kanunu'nun mehaz AB veri koruma mevzuatından çok daha kısa bir ömrü olduğu düşünüldüğünde, KVK Kanunu'nun GVK Tüzüğü'ne tamamen paralel hale getirilmesi halinde uzun soluklu ve zorlu bir adaptasyon ve implementasyon sürecine girilmesi pek muhtemeldir. Bununla birlikte, KVK Kanunu'ndaki mevcut düzenlemelerden bazılarının hâlihazırda uygulamada ciddi güçlükler yarattığı yadsınamaz bir gerçektir. Üstelik oldukça sıkı şartlara tabi yurt dışı aktarımlarını ortadan kaldırmak veya minimize edebilmek adına veri sorumluları tarafından ciddi külfetler (maliyetlerin yüksek olması, güvenlik imkanlarının daha düşük olması, kullanım zorluğu ve daha az esneklik sağlayan imkanları vb.) göze alınsa ve yerel (lokal) alternatifler kullanılmak istense bile, olağan hayat akışında yurt dışı aktarımının sıfırlanamayacağı durumlar[340] vardır. Öte yandan, 1 Ocak 2002 tarihinde yürürlüğe girmiş olan 4721 sayılı Türk Medeni Kanunu'nun 2.

[340] Örneğin, iş hayatının ayrılmaz parçası haline gelen Microsoft Outlook, Teams, Google vb. e-posta ve anlık ileti uygulamalarının kullanımı dolayısıyla kişisel veriler yurt dışına aktarılmış olur.

maddesinde düzenlenen dürüstlük kuralına aykırılığın yargı fonksiyonunu ifa eden mahkemeler tarafından dahi son çare (*ultima ratio*) olarak değerlendirdiği düşünüldüğünde, yürütme organı olarak hareket eden KVK Kurumu'nun dürüstlük kuralına aykırılığı gerekçe göstererek yüksek cezalar vermesi hukuk güvenliğinin eksikliği olarak değerlendirilebilir. Bu bağlamda, Türk hukukunda da hukuk güvenliğinin tesisine hizmet eden davranış kuralları ve/veya sertifikasyon gibi araçlara er ya da geç ihtiyaç duyulacağı düşünülmektedir.

Özellikle KVK Kanunu'ndaki özel nitelikli kişisel verilerin işlenmesi şartlarını düzenleyen 6. madde ile kişisel verilerin yurt dışına aktarımını düzenleyen 9. maddenin birçok veri sorumlusunu zorunlu olarak risk almaya itmesi ve mevcut düzenlemelerin yeterince alternatif sunmaması, KVK Kanunu'nda bu konularda öncelikli olarak değişikliğe ihtiyaç duyulmasına sebep olmaktadır. Öte yandan, KVK Kanunu'nun uygulamada en çok tartışma ve sorun yaratan bu iki maddesinde AB düzenlemelerine paralel bir düzenlemeye gidilse dahi, KVK Kanunu'nun GVK Tüzüğü ile kıyaslandığında birçok yönden sınırlı kalmaya devam edeceği tartışmasızdır.

Günden güne yeni teknolojilerin ortaya çıktığı ve veri işleme faaliyetlerinin karmaşıklaştığı bu çağda, veri işlemenin faaliyetlerinin hukuka uygun gerçekleştirilmesi kadar, işleme faaliyetleri bakımından uyumluluğun ortaya konması oldukça önem arz eder. Zira bu sayede veri sorumluları, gerek yetkili otoriteler/makamların gerek de verisi işlenen ilgili kişilerin karşısına hazırlı çıkabilecektir.

Kişisel veriler hangi hukuki sebebe dayanılarak işlenirse işlensin, tüm işleme faaliyetlerinin genel ilkelere uygun yürütülmesi zorunludur. O halde, KVK Kanunu'ndaki genel ilkeler arasına 'hesap verebilirlik' ilkesinin eklenmesi, veri sorumlularının ilgili mevzuata uyum için daha fazla efor sarf etmesini gerektireceğinden bu ilkenin varlığı veri güvenliğinin sağlanmasına hizmet edecektir. Kısacası, AB mevzuatının lafzından ziyade ruhuna yaklaşabilmek adına

dahi hesap verebilirlik ilkesinin normatif düzlemde kabulüne ihtiyaç vardır. Buna karşılık, hesap verebilirlik ilkesini uygulamak için getirilen temel araçlardan bilhassa davranış kuralları ve sertifikasyon, kişisel verilerin korunması bakımından paydaşlarına en esnek ve isabetli çözümler sunsa bile henüz mahremiyet bilincinin yeterince gelişmediği Türkiye açısından nispeten daha az öncelikli bir ihtiyaçtır. Özetle, hesap verebilirlik GVK Tüzüğü'ndeki her görünümüyle olmasa bile ilkesel anlamda Türk veri koruma mevzuatına kazandırılması gereken oldukça önemli bir kavramdır.

KAYNAKÇA

Basılı Kaynaklar

Alhadeff, J., van Alsenoy, B., & Dumortier, J. (Eylül, 2011). *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions.* In D. Guagnin, L. Hempel, C. Ilten, et al. (Eds.), Managing Privacy through Accountability s. 49-82.

Aktan, C. C., Dileyici, D., & Vural, İ. Y. (2006). *Kamu Maliyesinde Çağdaş Yaklaşımlar* (1. Baskı)

Balcı, A., Nohutçu, A., Öztürk, N. K., & Coşkun, B. (2013). *Kamu Yönetiminde Çağdaş Yaklaşımlar: Sorunlar, Tartışmalar, Çözüm Önerileri, Modeller, Dünya ve Türkiye Yansımaları* (3. Baskı).

Bayram, Ö. B. (2022). Bir uyum aracı olarak veri koruma etki analizinin Türk hukuku bakımından değerlendirilmesi. *Kişisel Verileri Koruma Dergisi*, 4(1), 38-53.

Berber, L. K. & Bilgili, A. C. (2020, Ocak). Çapraz Etkileşim: Mahremiyete İlişkin Mevzuat ve Mahremiyet Standartları Arasındaki İlişki. *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku. Marmara Hukuk Bilimsel Toplantılar Serisi - 1*. On İki Levha Yayıncılık.

Bock, K. (2016). Data protection certification: Decorative or effective instrument? Audit and seals as a way to enforce privacy. In C. Cuijpers, S. Nouwt, & B.-J. Koops (Eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, s. 335-356.

Buckley, M. R., Beu, D. S., Frink, D. D., Howard, J. L., Berkson, H., Mobbs, T. A., & Ferris, G. R. (2001). Ethical issues in human resources systems. *Human Resource Management Review, 11*, s. 11-29

.

Burke, C. S., Sims, D. E., Lazzara, E. H., & Salas, E. (2007). Trust in leadership: A multi-level review and integration. *The Leadership Quarterly, 18*(6), s. 606-632.

Curtis, P., & Prazeres, N. (2021). *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide* (4.baskı). IT Governance Publishing.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society, 3*, s. 247-251.

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

Çekin, M. S., Berktaş, A. E., & Akıncı, M. F. (2023). *Veri Hukuku.* On İki Levha Yayıncılık.

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review, 35*, Article 105342.

Domingo, A., & Villar, N. (2018). Self-regulation in data protection. Madrid, Spain.

Eryılmaz, B., & Biricikoğlu, H. (2011). Kamu yönetiminde hesap verebilirlik ve etik. *4. İş Ahlakı Dergisi*, s.19-45.

Gunasekara, G. (2013). Paddling in unison or just paddling? International trends in reforming information privacy law. *International Journal of Law and Information Technology*, 21(2), s. 141-177.

Gül, S. K. (2008). Kamu yönetiminde ve güvenlik hizmetlerinde hesap verebilirlik. *Polis Bilimleri Dergisi*, 10, s. 71-94.

Hepburn, G. (2009). OECD Report: Alternatives to Traditional Regulation.

Hirsch, D. D. (2013). In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct. *Ohio State Law Journal*, 74, s. 1527-1556.

Jabbra, J. G., & Dwivedi, O. P. (Eds.). (1989). Public service accountability: A comparative perspective. Connecticut, Kumarian Press; Cendón, A.B. (1999*). Accountability and Public Administration: Concepts, Dimensions, Developments*.

Kamara, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology*, 8(1).

Kamara, I., & Burnik, J. (2017). Recommendations on European data protection certification. *European Union Agency For Network and Information Security.*

Kamara, I. & De Hert, P. (2018). Data protection certification in the EU: Possibilities, Actors And Building Blocks In a Reformed Landscape. *Privacy and Data Protection Seals*, s. 7-34.

Kaya, M. B. (2020). Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. *İstanbul Hukuk Mecmuası*, 78, s. 1859-1897.

Kaya, M. B. (2022). *Avrupa Birliği P2B Tüzüğü: Aracı Hizmet Sağlayıcılar ve Arama Motorları İçin Adil ve Şeffaf Platform Kuralları.* On İki Levha Yayıncılık.

Koščík, M., & Myška, M. (2018). Data protection and codes of conduct in collaborative research. *International Review of Law, Computers & Technology*, 32(1), s. 141-154.

Kuner, C., Bygrave, L. A., & Docksey, C. (2021). *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*. Oxford, UK: Oxford University Press.

Lachaud, E. (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. *Computer Law & Security Review*, 32(6), s. 814-826.

Lachaud, E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review*, 34(2), s. 244-256.

Lachaud, E. (2019). Adhering to GDPR codes of conduct: A possible option for SMEs to GDPR certification. *Journal of Data Protection & Privacy*, 3(1), s. 48-68.

Lachaud, E. (2020). What GDPR tells about certification. *Computer Law & Security Review*, 38.

Lambert, P. (2016). The Data Protection Officer: Profession, Rules, and Role (1st ed.)

Leenes, R. (2020). *Article 42 certification*. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation: A Commentary* (s. 732-743). Oxford, UK: Oxford University Press.

Meuwissen, M. P., Velthuis, A. G., Hogeveen, H., & Huirne, R. B. (2003). Technical and economic considerations about traceability and certification in livestock production chains. In *New approaches to food safety economics*, Wageningen (s. 41-54).

Noain-Sánchez, A. (2016). "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. *Journal of Information, Communication and Ethics in Society*, 14(2), s. 124-138.

Papakonstantinou, V. (2018). Introduction: Privacy and Data Protection Seals. In *Privacy and Data Protection Seals*, s. 1-6.

Quelle, C. (2018). Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation*, 9(3), s. 502-526.

Rodrigues, R., Barnard-Wills, D., De Hert, P., & Papakonstantinou, V. (2016). The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology*, 30(3), s. 248-270.

Romzek, B. S. (2000). Dynamics of Public Sector Accountability in an Era of Reform. *International Review of Administrative Sciences*, 66, s.21–44.

Sümer, B. (2019). *The certification mechanism under the EU General Data Protection Regulation* (Yüksek Lisans Tezi). Marmara Üniversitesi.

Tutar, H., & Altınöz, M. (2017). Hesap verebilirlik bağlamında iç denetim ve sorun alanları: Eleştirel bir analiz. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 8, s. 225-248.

Vander Maelen, C. (2021). First of many? First GDPR transnational code of conduct officially approved after EDPB opinions 16/2021 and 17/2021. *European Data Protection Law Review,* 7(2), s.228-231.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide* (1st ed.). Cham: Springer International Publishing.

Elektronik Kaynaklar

Court of Justice of the European Union (4 Mart 2020). Case C-61/19. Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal. Opinion of Advocate General Szpunar. https://curia.europa.eu/juris/document/document.jsf?text=accountability&docid=224083&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=10154021#ctx1 (Erişim Tarihi: 29.05.2023)

Court of Justice of the European Union (16 Temmuz 2020). Case C-311/18 Facebook Ireland Ltd v Maximillian Schrems. Judgment of The Court (Grand Chamber. https://curia.europa.eu/juris/document/document.jsf;jsessionid=920F8236EAD65FFA7730C23834493B78?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2052319 (Erişim Tarihi: 29.05.2023)

Court of Justice of the European Union (28 Nisan 2022). Case C-129/21. Proximus NV (Public electronic directories) v Gegevensbeschermingsautoriteit. Opinion of Advocate General Collins. https://curia.europa.eu/juris/document/document.jsf?text=accountability&docid=258506&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=10154021#ctx1 (Erişim Tarihi: 29.05.2023)

Court of Justice of the European Union (4 Mayıs 2023). Case C-60/22. UZ v Bundesrepublik Deutschland. Judgment of The Court (Fifth Chamber). https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3395552 (Erişim Tarihi: 29.05.2023)

Dülger, M. V., & Gümüş, G. (17 Haziran 2021). *Scherms II Kararı ve Sonuçları (Scherms II Decision and Results)*. https://ssrn.com/abstract=3869038 (Erişim Tarihi: 29.05.2023)

European Court of Human Rights. (17 Temmuz 2008). *Case of I v. Finland* (Application no. 20511/03) https://hudoc.echr.coe.int/eng?i=001-87510 (Erişim Tarihi: 29.05.2023)

EDPB. (4 Haziran 2019). *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation (Version 3.0).* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf (Erişim Tarihi: 29.05.2023)

EDPB. (4 Haziran 2019). *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (Version 2.0).* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf (Erişim Tarihi: 29.05.2023)

EDPB. (4 Haziran 2019). *Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 of the General Data Protection Regulation (2016/679).* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf (Erişim Tarihi: 29.05.2023)

EDPB. (6 Nisan 2021). *Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment.* https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_certification_criteria_assessment_formatted_en_0.pdf (Erişim Tarihi: 29.05.2023)

EDPB. (22 Şubat 2022). *Guidelines 04/2021 on Codes of Conduct as tools for transfers (Version 2.0).* https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (Erişim Tarihi: 29.05.2023)

EDPB. (14 Şubat 2023). Guidelines 07/2022 on certification as a tool for transfers (Version 2.0). https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (Erişim Tarihi: 29.05.2023)

EDPB. (25 Mayıs 2018 & 6 Nisan 2022). *European Data Protection Board Rules Of Procedure (Version 8).* https://edpb.europa.eu/system/files/2022-04/edpb_rules_of_procedure_version_8_adopted_20220406_en.pdf (Erişim Tarihi: 29.05.2023)

ISO/IEC. (2011). *ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework.* https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en (Erişim Tarihi: 29.05.2023)

ISO. (2012). ISO/IEC 17065:2012(en) *Conformity assessment -- Requirements for bodies certifying products, processes and services.* https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en (Erişim tarihi: 29.05.2023)

ISO. (2017). *ISO 31700-1, Consumer protection - Privacy by design for consumer goods and services - Part 1: High-level requirements.* https://www.iso.org/obp/ui/#iso:std:iso:31700:-1:ed-1:v1:en (Erişim Tarihi: 29.05.2023)

ISO. (2019). *ISO 31700-1, Consumer protection - Privacy by design for consumer goods and services - Part 2: Use cases*

https://www.iso.org/obp/ui/#iso:std:iso:tr:31700:-2:ed-1:v1:en (Erişim Tarihi: 29.05.2023)

ISO/IEC. (2019). *ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en (Erişim Tarihi: 29.05.2023)

Greenleaf, G. (2019, Mayıs). Accountability Without Liability: 'To Whom'and 'With What Consequences'? (Questions for the 2019 OECD Privacy Guidelines Review). *UNSW Law Research Paper No. 19-67*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427 (Erişim Tarihi: 29.05.2023)

Lambert, P. (2017). *Understanding the New European Data Protection Rules* (1st ed.). Auerbach Publications. https://doi.org/10.1201/9781315115269 (Erişim Tarihi: 29.05.2023)

Madde 29 Çalışma Grubu. (1998). Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp7_en.pdf (Erişim Tarihi: 29.05.2023)

Madde 29 Çalışma Grubu (13 Temmuz 2010). *Opinion 3/2010 on the principle of accountability*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (Erişim Tarihi: 29.05.2023)

Madde 29 Çalışma Grubu. (1 Aralık 2009). *The Future of Privacy.* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf (Erişim Tarihi: 29.05.2023)

Privacy Bridges. (2015). EU and US Privacy Experts in Search of Transatlantic Privacy Solutions, 37th International Privacy Conference Amsterdam. https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf (Erişim Tarihi: 29.05.2023)

Quelle, C. (2017). The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too. In R. Leenes, R. van Brakel, S. Gutwirth, & P. De Hert (Eds.), *Data Protection and Privacy: The Age of Intelligent Machines (Forthcoming).* Tilburg Law School Research Paper No. 17. Tilburg University - Tilburg Institute for Law, Technology, and Society (TILT). https://ssrn.com/abstract=3000382 (Erişim Tarihi: 29.05.2023)

Tene, O. (2013). Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. Ohio State Law Journal, 74(6), s. 1217-1262. https://core.ac.uk/download/pdf/159560945.pdf (Erişim Tarihi: 29.05.2023)