

**GDPR IŞIĞINDA
KİŞİSEL VERİLERİN KORUNMASINDA
AKREDİTASYON VE SERTİFİKASYON SİSTEMİ**

ALİ OSMAN ÖZDİLEK

**ÖZYEĞİN ÜNİVERSİTESİ
HAZİRAN, 2024**

GDPR IŞIĞINDA
KİŞİSEL VERİLERİN KORUNMASINDA
AKREDİTASYON VE SERTİFİKASYON SİSTEMİ

Ali Osman Özdilek

Kamu Hukuku

Doktora Tezi

Danışman: Prof. Dr. Mustafa Topaloğlu

Sosyal Bilimler Enstitüsü
Özyeğin Üniversitesi
İstanbul

Haziran, 2024

GDPR IŞIĞINDA KİŞİSEL VERİLERİN KORUNMASINDA AKREDİTASYON VE SERTİFİKASYON SİSTEMİ

Jüri:

Prof. Dr. Mustafa Topaloğlu, Danışman
Özel Hukuk Bölümü
Özyeğin Üniversitesi

Dr. Öğr. Üyesi Zeynep Reva
Kamu Hukuku Bölümü
Özyeğin Üniversitesi

Dr. Öğr. Üyesi Müge Çetin
Özel Hukuk Bölümü
Özyeğin Üniversitesi

Prof. Dr. Ender Ethem Atay
Kamu Hukuku Bölümü
Başkent Üniversitesi

Prof. Dr. Mehmet Emin Akgül
Kamu Hukuku Bölümü
Başkent Üniversitesi

Kabul Tarihi: 06.06.2024

ORİJİNALLİK BEYANI

Bu tez çalışmasının tek yazarı olduğumu ve bu tez metninin düzeltmeler de dahil olmak üzere tez jürisi tarafından kabul edilen ve onaylanan son metin olduğunu beyan ederim. Bu çalışmadaki tüm veri ve bilgiler araştırma etiği kuralları ve akademik dürüstlük ilkelerine uygun olarak elde edilmiş, üretilmiş ve sunulmuştur. Tüm bilgimi, fikir, düşünce ve telif hakkıyla korunan her türlü materyali standart referans kurallarına uygun olarak sunduğumu, bu tezin orijinalliğini ve herhangi bir bölümünün başka bir yükseköğretim kurumundaki bir diploma programına sunulmadığını beyan ederim.

Ali Osman Özdilek

ÖZET

Kişisel verilerin teknolojinin gelişimine paralel olarak hem çeşitlerinin hem de işleme yöntem ve hacimlerinin gelişimi, bu verilerin bir süre sonra sadece kişilik haklarını koruyan hükümler veya cezai hükümlerle değil, kendine özgü bir mekanizma çerçevesinde korunmasını gündeme getirmiştir. Aynı zamanda teknolojik gelişime bağlı bu durum kişisel verilerin daha üst seviyede bir koruma altına alması gerekliliği düşüncesini ortaya çıkarmış ve kişisel veriler anayasalar kapsamında korunan haklar olarak anayasa hukuku kapsamındaki yerini almıştır. Türkiye’de Anayasa’nın 20. maddesinde yapılan değişiklik ile kişisel verilerin korunması hakkı bir anayasal hak olarak düzenlenmiştir. 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ile de AB ve dünya düzenlemeleri ile uyumlu bir kişisel verileri koruma hukuku düzenlemesi benimsenmiştir. AB’de 95/46 sayılı Yönerge döneminde uygulamaları görülen “e-mahremiyet mühürleri” uygulamaları ile veri sorumluları, veri işleme süreçlerinde bir nevi sertifikasyona tabi tutularak, veri işleme süreçlerinin mevcut hukuki düzenlemelere uygun olduğu yönünde karineler meydana getirilmiştir. GDPR’ın yürürlüğe girmesinden sonra ise GDPR’ın akreditasyon ve sertifikasyona dair düzenlemelerinin yanı sıra bu düzenlemelere açıklamalar getirmek üzere, AB çapında kişisel verilerin korunmasında bir akreditasyon ve sertifikasyon sistemini yürürlüğe sokmaya dair rehberler yayınlanmıştır. GDPR’da yapılan düzenlemeler ve çıkarılan rehberlerin ardından, AB’de, kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemi, “EUROPRIVACY” adı ile çok yeni kurulmuştur.

Anahtar Kelimeler: Kişisel veriler, akreditasyon, sertifikasyon, gdpr, europprivacy

ABSTRACT

The evolution of personal data, both in terms of its types and methods and volumes of processing, parallel to the advancement of technology, has brought to the forefront the necessity for its protection not only through provisions safeguarding personality rights or penal provisions but also through a unique mechanism framework. Simultaneously, due to technological advancements, this situation has necessitated a higher level of protection for personal data, prompting the consideration of personal data as rights protected within the scope of constitutional law. In Turkey, the right to the protection of personal data was regulated as a constitutional right through an amendment to Article 20 of the Constitution. With the enactment of Law No. 6698 on the Protection of Personal Data in 2016, a personal data protection law compatible with EU and global regulations was adopted. During the period of Directive 95/46/EC in the EU, the "e-privacy seals" practices were observed, where data controllers were subjected to a sort of certification, indicating compliance of data processing processes with existing legal regulations. Following the enforcement of the GDPR, in addition to the accreditation and certification provisions of the GDPR, guidelines have been published at the EU level to provide explanations and further clarifications to these regulations in the context of personal data protection. Subsequently, in the EU, a system of accreditation and certification for the protection of personal data, under the name "EUROPRIVACY," has been newly established.

Keywords: Personal data, accreditation, certification, gdpr, europri vac

TEŞEKKÜR

Doktora yapmam gerekliliğine herkesten önce beni ikna eden, bizzat doktora derslerime giren, tezin konusunun ve kapsamının belirlenmesinden, ortaya çıkmasına kadar her aşamada; konunun zorluğu, iş hayatının ve aile hayatının yoğunluğu, sağlık sebepleri gibi çeşitli nedenlerle umutsuzluğa düştüğümde her an beni yönlendiren, teşvik eden, bilimsel olduğu kadar manevi olarak da destekleyen, tezin ana mimarı olan, tanımaktan ve öğrencisi olmaktan büyük onur duyduğum Sayın Hocam, büyüğüm Prof. Dr. Mustafa Topaloğlu'na sonsuz teşekkürlerimi sunuyorum.

Yine tezin her aşamasında, özellikle anayasa ve idare hukuku ile ilgili zorlandığım tüm konularda ufuk açıcı bilgeliği ile bana yön veren, bıkmadan, usanmadan ne zaman görüşmek istesem, soru sorsam bana cevap veren, beni yönlendiren çok kıymetli hocam, büyüğüm Sayın Prof. Dr. Ender Ethem Atay'a en içten teşekkürlerimi sunuyorum.

Doktora dersleri boyunca uzun hukuk felsefesi tartışmaları başta olmak üzere akademik yaşantımın en doyurucu sohbetlerini yaptığım, bir hukuk pratiği uygulayıcısı düşünce tarzı ve çalışma yöntemlerinden bir akademi mensubunun düşünce tarzına ve çalışma yöntemlerine dönüşmem yolunda bana büyük katkısı olan çok kıymetli hocam Doç. Dr. Altan Heper'e en içten teşekkürlerimi sunuyorum.

Tezimde danışman olarak yer almayı kabul edip beni onurlandıran, tezin özellikle şekillenmesi aşaması başta olmak üzere tüm aşamalarında beni makamında kabul ederek uzun tartışmalarla, sorduğu sorularla ufkumu açan, bana güven aşılayan, Kurum'un kütüphanesini bana açan, tanıdığım en vizyoner insanlardan biri olan çok kıymetli hocam, büyüğüm Kişisel Verileri Koruma Kurumu Başkan Yardımcısı Dr. Cihan Kanlıgöz'e en içten teşekkürlerimi sunuyorum.

Doktora derslerimde ceza hukuku ile ilgili derslerime giren, ceza hukukunun daha önce hiç inemediğim derinliklerine inmemi sağlayan, bana bu yönde yepyeni bakış açıları kazandıran, tanıdığım en zeki ama aynı zamanda en alçakgönüllü insanlardan biri olan çok kıymetli hocam Dr. Barış Atladı'ya en içten teşekkürlerimi sunuyorum.

Doktora derslerimde, eleştirel aklın idare hukuku kapsamında nasıl kullanılacağını bana gösteren, idare hukukunu Devlet Planlama Teşkilatından gelen devlet birikimi ile bana bambaşka yönleriyle aktaran ve bende yepyeni ufuklar açan çok kıymetli hocam Dr. Hasan Dursun'a en içten teşekkürlerimi sunuyorum.

Tez izleme komitelerinde yer alma inceliğini göstererek, her zaman pozitif enerjisi ile beni TİK toplantılarında tezin sağlıklı ilerleyişi yönünde teşvik eden ve uzun yıllar uygulamanın içinde yer alıp da sonradan akademik hayata geçiş yapılabileceğinin en canlı örneğini gösteren, çok kıymetli hocam Dr. Zeynep Reva'ya en içten teşekkürlerimi sunuyorum.

Tez savunma jürisinde yer alma inceliğini göstererek, desteğini esirgemeyen tezin sağlıklı ilerleyişi yönünde teşvik eden ve uzun yıllar uygulamanın içinde yer alıp da sonradan akademik hayata geçiş yapılabileceğinin en canlı örneğini gösteren, çok kıymetli hocam Dr. Müge Çetin'e en içten teşekkürlerimi sunuyorum.

Prof. Dr. Mustafa Topaloğlu hocamla birlikte doktora başlamam ve bu tezin ortaya çıkmasındaki en önemli kişi olan, beni bazen tatlı dille bazen zorlayarak doktora çalışmalarımı devam ettirmemi sağlayan, beş çocuğumuzun ve evin tüm sorumluluğunu ve aynı zamanda işyerlerimizin sorumluluğunu alan, hayat arkadaşım, adalete olan sarsılmaz inancıyla tam bir hukuk savaşçısı olan, ama aynı zamanda mükemmel bir eş ve anne olan, bütün bu uğraşlarının arasında iki yüksek lisans bitirmiş olan, azimli, kararlı,

sevgisi ile beni ve ailemizi her zaman güven içinde tutan eşim Av. Hafize Özdilek'e sonsuz teşekkürlerimi ve minnettarlığımı sunuyorum. Sen olmasan bu tez olmazdı.

Bütün bu süreç boyunca en çok kendilerinden zaman çaldığım, zaman zaman sevgimi ve şefkatimi tam olarak gösterememe boyutuna geldiğim, buna rağmen sevgilerinde en ufak bir azalma görmediğim, yaşama sebeplerim, çocuklarım, Anatolia, İlaria, Alişia, Devrim ve Kerem'e sonsuz teşekkürlerimi ve çaldığım vakitler için özürlerimi sunuyorum.

Tüm doktora süreci boyunca, hocalarımla, enstitü ile ve diğer tüm paydaşlar ve ilgililer ile olan tüm süreçleri adım adım takip eden, tüm evrak işlerini, randevuları, süreleri takip eden, kılı kırk yaran bir titizlikle tüm sürecin sağlıklı yürütmesinde çok büyük emeği olan, yılgınlık gösterdiğim zamanlar da dahil olmak üzere sürekli peşimde olarak özellikle tez yazım sürecindeki planlamaya adım adım uymamı sağlayan sevgili asistanımız Habibe Aydın'a da özel teşekkürlerimi sunmak istiyorum.

Son olarak, tüm süreç boyunca bana doktora ile ilgili her konuda destek olan çok kıymetli Enstitü çalışanlarına ve tüm Özyeğin Üniversitesi ailesine teşekkürlerimi sunuyorum.

İÇİNDEKİLER

ORJİNALLİK BEYANI.....	iii
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
KISALTMALAR LİSTESİ	xiv
1. GİRİŞ	1
1.1 Konunun Önemi Ve Tezin Amacı	1
1.1.1 Konunun Önemi.....	1
1.1.2 Tezin Amacı.....	3
1.2 Tezin Sınırları, Planı ve Kaynakları	3
1.2.1 Tezin Sınırları	3
1.2.2 Tezin Planı	4
1.2.3 Tezin Kaynakları.....	6
2. KAVRAMSAL AÇIKLAMALAR.....	8
2.1 Genel Olarak	8
2.2 Veri, Bilgi, Kişisel Veri	8
2.2.1 Veri	8
2.2.2 Bilgi	9
2.2.3 Kişisel Veri	10
2.3 Veri Sorumlusu, Müşterek Veri Sorumlusu, Veri İşleyen.....	13
2.3.1 Veri Sorumlusu	14
2.3.2 Müşterek Veri Sorumlusu.....	17
2.3.3 Veri İşleyen.....	20
2.4. Veri Sorumlularının Yükümlülükleri.....	23
2.4.1 Aydınlatma Yükümlülüğü	23
2.4.2 İlgili Kişilere Haklarını Kullandırma Olanağını Sağlama Yükümlülüğü.....	25
2.4.3 Kişisel Veri Güvenliğine İlişkin Yükümlülükler.....	26
2.4.4 Veri İhlal Bildirimi Yükümlülüğü	28
2.4.5 Veri Sorumluları Siciline Kayıt Yükümlülüğü.....	31
2.4.6 İrtibat Kişisi ve Veri Koruma Uzmanı Atama Yükümlülüğü.....	33

2.4.7 Kişisel Veri İşleme Envanteri Hazırlama Yükümlülüğü	36
2.5 Veri Sahiplerinin Kişisel Verilerin Korunması Kapsamındaki Hakları	39
2.5.1 Genel Olarak	39
2.5.2 Bilgi Alma Hakkı.....	41
2.5.3 Erişim Hakkı	43
2.5.4 Veri Taşınabilirliği.....	46
2.5.5 Düzeltme Hakkı	47
2.5.6 İtiraz Hakkı	48
2.5.7 Kişisel Verilerin İmhasını Talep Etme Hakkı.....	49
2.5.8 Unutulma Hakkı.....	52
2.6 Akreditasyon, Sertifikasyon.....	57
2.6.1 Genel Olarak	57
2.6.2 Akreditasyon.....	59
2.6.3 Sertifikasyon	62
3. ANAYASAL BİR TEMEL HAK OLARAK KİŞİSEL VERİLERİN KORUNMASI HAKKI.....	64
3.1 Genel Olarak Anayasa ve Anayasa Hukuku Kavramları.....	64
3.2 Temel Haklar ve Özgürlükler	66
3.3 Temel Hak Olarak Kişisel Verilerin Korunması Hakkı.....	72
3.3.1 Kişisel Verilerin Korunması Hakkının Hukuki Niteliği	72
3.3.2 Kişisel Verilerin Korunması Hakkının Anayasal Bir Hak Olma Niteliği	79
4. KİŞİSEL VERİLERİN KORUNMASINDA AKREDİTASYON VE SERTİFİKASYON	90
4.1 Genel Olarak	90
4.2 GDPR m.42 ve 43. Kapsamında Akreditasyon ve Sertifikasyon	91
4.2.1 GDPR 42. Madde Düzenlemeleri	91
4.2.2 GDPR 43. Madde Düzenlemeleri, Sertifikasyon Kuruluşları ve Akredite Edilmeleri.....	95
4.2.3 GDPR ile Düzenlenen Akreditasyon ve Sertifikasyon Sistemi Hakkında Değerlendirmeler	100
4.2.3.1 Genel Olarak Akreditasyon.....	100
4.2.3.2 GDPR m.43 Kapsamında Akreditasyon	103

4.2.3.3 765/2008 Sayılı Tüzük ile GDPR m.43 Kapsamındaki Düzenleme	
Arasındaki İlişki.....	104
4.2.3.4 GDPR Kapsamında Akreditasyonda Ulusal Akreditasyon Kuruluşunun	
Rolü.....	105
4.2.3.5 GDPR Kapsamında Akreditasyonda Veri Koruma Otoritesinin Rolü..	106
4.2.3.6 Veri Koruma Otoritesinin Sertifikasyon Kuruluşu Olarak Hareket Etmesi	
.....	108
4.2.4 Akreditasyon Gereklilikleri	109
4.2.4.1 Genel Olarak	109
4.2.4.2 Akreditasyon İçin Genel Şartlar.....	111
4.2.4.3 Akreditasyon için Yasal Şartlar	112
4.2.4.3.1 Sertifikasyon Sözleşmesi	112
4.2.4.3.2 Tarafsızlık	113
4.2.4.3.3 Sorumluluk ve Finansman	113
4.2.4.3.4 Kamunun Bilgilendirilmesi.....	113
4.2.4.3.5 Personel Nitelikleri	113
4.2.4.4 Süreç Gereklilikleri	114
4.2.4.5 Yönetim Sistemleri Gereklilikleri	118
4.2.5 Sertifikasyon Gereklilikleri.....	119
4.2.5.1 Genel Olarak	119
4.2.5.2 Akreditasyon ve Sertifikasyon Rehberlerinin Niteliği.....	120
4.2.5.3 Sertifikasyon ile GDPR Uyumluluğu Arasındaki İlişki.....	122
4.2.5.4 GDPR Kapsamında Kişisel Verilerin Korunmasında Sertifikasyon	
Kavramı.....	123
4.2.5.5 GDPR Kapsamındaki Sertifikasyonda İlgili Ülke Veri Koruma	
Otoritelerinin Rolü	124
4.2.5.6 Sertifikasyon Kuruluşu Olarak Veri Koruma Otoritesi	125
4.2.5.7 Sertifikasyon Kuruluşunun Rolü.....	127
4.2.5.8 Sertifikasyon Kriterlerinin Onaylanması	128
4.2.5.9 Avrupa Veri Koruma Mührü Kriterleri.....	130
4.2.6 Sertifikasyon Kriterlerinin Geliştirilmesi	132
4.2.7 Sertifikasyon Kriterlerinin Tanımlanması	139

4.2.8 Sertifikasyon Mekanizmasının Kapsamının Belirlenmesi İçin Kriterler.....	142
4.2.8.1 Genel Olarak	142
4.2.8.2 Veri İşleme Kriterleri	144
4.2.8.3 Veri Koruma İlkeleri ve İşleme Şartları (GDPR m.5, 6)	145
4.2.8.4 Veri Sorumlularının ve Veri İşleyenlerin Genel Yükümlülüklerine Dair Kriterler	145
4.2.8.5 Veri Sahiplerinin Hakları	146
4.2.8.6 Gerçek Kişilerin Hakları ve Özgürlükleri Açısından Risk Kriterleri ...	147
4.2.8.7 Veri Korumayı Garanti Eden Teknik ve İdari Tedbirler.....	147
4.2.8.8 Avrupa Veri Koruma Mührü İçin Ek Gereklilikler	148
4.2.9 Europrivacy Sistemi.....	149
4.2.9.1 Europrivacy Sistemi Nedir?	149
4.2.9.2 Sertifikasyon Kapsamı	151
4.2.9.3 Sertifikasyon Aşamaları	151
4.2.9.3.1 Hazırlık Aşaması.....	151
4.2.9.3.2 Bağımsız Sertifikasyon Aşaması	152
4.2.9.3.3 Geçerlilik	153
4.3 Türk Hukukunda Kişisel Verilerin Korunmasında Akreditasyon ve Sertifikasyon ile İlgili Düzenlemeler	153
4.3.1 Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ	153
4.3.1.1. Personel Belgelendirme Kuruluşu	154
4.3.1.2 Veri Koruma Görevlisi.....	155
4.3.1.3 DPO ve VKG	155
4.3.2 Veri Koruma Görevlisi Belgelendirme Programı	156
4.3.3 VKG'ye İlişkin Düzenlemelerin İptali Hakkında Başvuru.....	157
4.3.4 Akreditasyon ve Sertifikasyon Sistemi Hakkında Türkiye Özelinde Değerlendirme ve Öneriler	157
5. HUKUKİ GÜVENLİK İLKESİ	160
5.1 Genel Olarak Hukuk Devleti Kavramı ve Hukuki Güvenlik İlkesi ile İlişkisi ...	160
5.2 Hukuki Güvenlik İlkesinin Tanımı	162
5.3 Hukuki Güvenlik İlkesinin Alt İlkeleri ve İlkenin Neticeleri	166

6. AKREDİTASYON VE SERTİFİKASYON SİSTEMİNİN HUKUKİ GÜVENLİK İLKESİ KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI HAKKINA ETKİSİ	170
6.1 Genel Olarak	170
6.2 Anayasal Normlar Arasındaki Hiyerarşi	170
6.3 Akreditasyon ve Sertifikasyon Sisteminin Hukuki Güvenlik İlkesi Kapsamında Sayılması Durumunda Anayasal Bir Temel Hak Olarak Kişisel Verilerin Korunması Hakkına Etkisi	175
7. SONUÇ	183
KAYNAKÇA	189
EKLER	201
EK A. ÖZGEÇMİŞ	202

KISALTMALAR LİSTESİ

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

AİHM: Avrupa İnsan Hakları Mahkemesi

AİHS: Avrupa İnsan Hakları Sözleşmesi

BGYS: Bilgi Güvenliği Yönetim Sistemi

CNIL: Commission Nationale Informatique et Libertés (Ulusal Bilişim ve Özgürlükler Komisyonu – Fransız Veri Koruma Otoritesi)

COPPA: Children's Online Privacy Protection Act (Çocukların Online Mahremiyetini Koruma Yasası)

DPC: Data Protection Commision (Veri Koruma Komisyonu – İrlanda Veri Koruma Otoritesi)

DPO: Data Protection Officer (Veri Koruma Uzmanı)

EA: European Co-operation for Accreditation (Avrupa Akreditasyon Kuruluşu)

EDPB: European Data Protection Board (Avrupa Veri Koruma Kurulu)

ECCP: European Centre for Certification and Privacy (Avrupa Mahremiyet ve Sertifikasyon Merkezi)

EIPACC: European Institute for Privacy, Audit, Compliance and Certification (Avrupa Mahremiyet, Denetim, Uyum ve Sertifikasyon Enstitüsü)

GDPR: General Data Protection Regulation (Genel Veri Koruma Tüzüğü)

IAF: International Accreditation Forum (Uluslararası Akreditasyon Forumu)

ILAC: International Laboratory Accreditation Cooperation (uluslararası Laboratuvar Akreditasyon Kuruluşu)

ICO: Information Commissioner's Office (Bilgi Komisyoneri Ofisi – İngiliz Veri Koruma Otoritesi)

ISO: International Organization for Standardization (Uluslararası Standardizasyon Kuruluşu)

KVKK: Kişisel Verilerin Korunması Kanunu

MAC: Media Access Control (Medya Erişim Kontrolü)

NOCAR: National Obligation Compliance Assessment Report (Ulusal Uyum Yükümlülüğü Değerlendirme Raporu)

OECD: Organization for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)

PGD: Piyasa Gözetimi ve Denetimi

SERTABİS: Sertifika Takip ve Doğrulama Bilgi Sistemi

TBB: Türkiye Barolar Birliği

TDK: Türk Dil Kurumu

ToE: Target of Evaluation (Değerlendirme Hedefi)

WP29: Working Party 29 (29. Madde Çalışma Grubu)

VKG: Veri Koruma Görevlisi



1. GİRİŞ

1.1 Konunun Önemi Ve Tezin Amacı

1.1.1 Konunun Önemi

Kişisel verilerin korunması yukarıda da belirtildiği üzere çeşitli uluslararası, bölgesel ve ulusal düzenlemelere konu olan, hukuki yönünün yanı sıra teknoloji ile ilgili de çok önemli yönleri bulunan bir hukuk alanı olarak giderek daha fazla hayatımıza giren ve insanların da giderek bu alandaki haklarının çok daha fazla farkına vardıkları, görece diğer hukuk alanlarına göre yeni bir hukuk alanı olarak karşımıza çıkmaktadır.

Konunun önemi, kişisel verilerin korunmasının, gelişen teknoloji karşısında bireylerin mahremiyet alanlarının çok daralmasından, buna karşın mevcut genel düzenlemelere dayalı hukuki sistemlerin, kişilerin daralan bu mahremiyet alanlarının genişletilmesi ve fütursuzca kişisel verilerin işlenmesinin önüne geçememesi nedeniyle, kişisel verilerin korunmasının öncelikle bir anayasal hak olarak kabul edilmesi ve böylece temel haklar ve özgürlükler alanına dahil edilmesinden gelmektedir.

Temel haklar ve özgürlükler alanına alınmış olmasına rağmen kişisel verilerin korunması çok büyük oranda, “sui generis” şekilde ve teknolojik gerekliliklerle iç içe düzenlenmiş bir dizi hukuki düzenleme içerisinde ele alınmakta ve hukuk pratiği de bu yönde hızla gelişmektedir. Başka bir deyişle teknolojinin gelişimine paralel olarak ortaya çıkan yeni iş modelleri veya diğer sosyal, kültürel, ekonomik, siyasi alanlarda kişisel verinin daha önce hiç düşünülemeyecek bir şekilde işlenmeye başlanması ile kendini gösteren günlük pratiğe ve ihtiyaçlara cevap verme şeklinde cereyan eden hukuki uygulama ve gelişme yönünden çok sayıda bilimsel eser veya uygulamaya yönelik eser

olmasına rağmen, konunun temelini oluşturan temel haklar ve özgürlükler bağlamında konuyu ele alan eserlerin sayısı çok azdır.

Diğer yandan AB haricinde henüz dünyada uygulanmayan kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemini teorik ve pratik olarak inceleyen herhangi bir eser de bulunmamaktadır. Şu ana kadar var olan çalışmalar GDPR m.42 ve 43 çerçevesindeki düzenlemeler ve bu düzenlemelerle ilgili olarak AB'nin yetkili organlarının yayınladığı rehberler ve raporlardan ibarettir. Ayrıca çok az sayıda makale yayınlanmıştır.

Durum böyle iken, akreditasyon ve sertifikasyon sistemlerini anayasal bir çerçevede hukuki güvenlik ilkesi kapsamında ele alıp, hukuki güvenlik ilkesi ile yine bir anayasal hak olarak temel haklar ve özgürlükler alanına dahil edilen kişisel verilerin korunması hakkı arasında meydana gelecek çatışmayı inceleyen herhangi bir çalışma tezin yazıldığı tarihe kadar bulunmamaktadır. Bu nedenle tezde hem şu ana kadar bilimsel bir eserde detaylı bir incelemesine yer verilmemiş olan kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemi GDPR'daki düzenleme çerçevesinde, Türk hukukuna da değinilerek incelenecek, hem de daha spesifik olarak bu tür bir sistem kapsamında akredite edilen, sertifika alan veri sorumlularının ve veri işleyenlerin hukuki güvenlik ilkesinden faydalanıp faydalanamayacağı incelenecektir.

İncelemenin ardından ise iki anayasal düzenlemenin çatışması durumunda veri sorumlularının mı yoksa veri sahiplerinin mi menfaatlerinin üstün tutulacağı ele alınacaktır. Bu teorik bir sorun olarak görülse dahi, özellikle AB'nin yeni yaklaşım yönergeleri adını verdiği yönergelerle kurulan ve Türkiye'de de çeşitli sektörlerde yansımaları olan akreditasyon ve sertifikasyon sisteminde görüldüğü üzere, uygunluk değerlendirme, sertifikasyon kuruluşları, akreditasyon kuruluşları ile gerçek veya tüzel

kişiler arasında yaşanan günlük hayata dair gerçek sorunlar da aynı şekilde kişisel verilerin korunması alanında da ortaya çıkacaktır. Bu nedenle kurulacak böyle bir akreditasyon ve sertifikasyon sisteminin, henüz kuruluş aşamasında en temelde anayasal bir konu olarak incelenmesi ve menfaatler dengesinin doğru kurgulanması gerekmektedir.

1.1.2 Tezin Amacı

Tezin amacı da hem kişisel verilerin korumasında akreditasyon ve sertifikasyon sistemini incelemek hem de bu tür bir sistemin kurulmasından kaynaklanabilecek anayasal sorunlar hakkında hukuk dünyasına bilimsel bir katkı yapabilmektir.

1.2 Tezin Sınırları, Planı ve Kaynakları

1.2.1 Tezin Sınırları

Kişisel verilerin korunması konusunun doğası gereği sadece hukuki bir konu olmaması, yoğun bir teknik içeriğe de sahip olması ve birçok hukuk dalını ve teknoloji dalını yatay düzlemde kesen bir dal olması nedeniyle, konunun sınırlandırılması zorunluluk arz etmektedir. Bu nedenle konunun teknoloji boyutu sadece konunun anlatımı için olmazsa olmaz bir zorunluluk oluşturuyorsa tezde ele alınacaktır. Teknik açıklamaların gerekli olduğu yerlerde teknik derinliğe girilmeyecek, sadece ilgili konunun hukuki açıklamasını destekleyecek miktarda ve hukukçular tarafından anlaşılabilir nitelikte ele alınacaktır.

Tez konusunun hukukun iki farklı alanını bir noktada ele almaya çalışmasından dolayı da ne anayasa hukukunun ne de kişisel verilerin korunması hukukunun tüm kavramlarına girilip, bunlarla ilgili tartışmalar yapılmayacak, sadece kişisel verilerin korunmasında akreditasyon ve sertifikasyon sisteminin Anayasa kapsamında hukuki güvenlik ilkesi karşısındaki durumu, idarenin takdir yetkisi ve gerçek kişilerin kişisel

verilerinin korunmasına dair anayasal hakları ve yasal düzenlemelerle getirilen hakları karşısındaki durumu ele alınacaktır. Ancak bu yapılırken, ilgili olduğu ölçüde anayasa ve kişisel verilerin korunması hukuku kapsamındaki çeşitli kavramlar ele alınacaktır.

Tez, başlığında da yer aldığı üzere gerçek kişilerin kişisel verileri ile ilgilidir. Bu nedenle ticari sırlar, tüzel kişilerin verileri, devlet sırrı gibi gerçek kişilerin verileri dışındaki veriler ile ilgili herhangi bir içermemektedir.

Tezin ana kapsamı veri sorumlusu ve veri işleyen sıfatlarına sahip tüzel kişilerin akreditasyon ve sertifikasyon mekanizmaları ile ilgili olup, bireysel sertifikalandırmalar tezin ana odağına yer almamaktadır. Ancak yeri geldikçe bireysel sertifikalandırmalara da değinilecektir.

Tez ayrıca ISO standartları kapsamında yapılan kalite çalışmalarını da kapsamamaktadır. Bu nedenle de ISO'nun 27000 ailesinde yer alan gerek bilgi güvenliği standardı ISO 27001 gerekse de veri mahremiyeti yönetimi standardı ISO 27701 tez içerisinde ele alınmayacaktır.

1.2.2 Tezin Planı

Tezde üçüncü bölümde bazı kavramsal açıklamalar yapılacaktır. Konunun anlaşılması açısından veri, bilgi, kişisel veri, veri sorumlusu, müşterek veri sorumlusu, veri işleyen, veri sorumlularının yükümlülükleri, kişisel veri sahiplerinin hakları, akreditasyon ve sertifikasyon kavramlarının çok iyi anlaşılması gerekmektedir. Kişisel verilere ilişkin kavramlar görece yeni olduğu için ve özellikle Türkiye'de kişisel verilerin korunmasına dair hukuki düzenlemeler Avrupa'ya göre çok sonra çıkarıldığı için, kendine özgü bir düzenlemeye ve mekanizmaya sahip olan kişisel verilerin korunması alanında terminolojinin yerleşmesi ve yeknesaklaşması zaman alacaktır. Bu nedenle

anlam kaymalarına ve anlam kargaşasına meydan vermemek için kişisel veriler açısından tezin en önemli kavramları detaylı bir şekilde açıklanmıştır.

Buna karşın genel anlamdaki akreditasyon ve sertifikasyon, uygulamada kalite yönetim sistemleri nedeniyle ve sağlık sektörü gibi bazı sektörlerde zorunluluk arz eden hususlar olması hasebiyle çok yaygın olarak kullanılmasına karşın, bu kavramlar üzerinde çokça yazının yazılmadığı, akademik çalışmaların yapılmadığı kavramlardır.

Nitekim kavramsal açıklamaların yapıldığı bölümde açıklanan akreditasyon ve sertifikasyon, tezin ana konusunu oluşturan kişisel verilerin korunmasındaki akreditasyon ve sertifikasyona göre önemli farklılıklar arz etmektedir. Bunda en büyük etken, kişisel verilerin korunması alanının “sui generis” ve aynı zamanda multidisipliner bir alan olmasıdır. Hukuk ile teknolojinin iç içe geçtiği bir alan olan kişisel verilerin korunmasında akreditasyon ve sertifikasyon denildiğinde bir ürünün ya da hizmetin belli standartlara uygun olmasından ziyade, veri sorumlusunun veya veri işleyenin kişisel veri işleme süreçlerinin mevcut hukuki, teknik ve idari düzenlemelere uyumu kastedilmektedir.

Ancak kişisel veriler alanındaki akreditasyon ve sertifikasyon, kişisel verilerin korunması için gerekli olan yazılım ve donanım gibi ürünlerin sertifikasyonunu da içerdiği gibi bütün bir kişisel veri sistemi içerisinde hareket edecek veri koruma uzmanları, veri koruma temsilcileri, irtibat kişileri gibi kişilerin sahip olacakları bireysel sertifikaları da aynı zamanda içermektedir. Ancak tez kapsamında akreditasyon ve sertifikasyon yukarıda belirtildiği gibi veri sorumlularının veya veri işleyenlerin veri işleme süreçlerinin mevcut düzenlemelere uyumu anlamında kullanılacak ve bu yönüyle incelenecektir.

Dördüncü bölümde, Anayasa hukuku kapsamında bir hak olarak kişisel verilerin korunması ele alınacaktır.

Beşinci bölümde, kişisel verilerin korunmasında akreditasyon ve sertifikasyon incelenecektir. Bu incelemenin esasını ise GDPR'ın akreditasyon ve sertifikasyona dair 42 ve 43. maddeleri oluşturacaktır. Bu bağlamda EDPB'nin yayınladığı rehberler, Avrupa Konseyi'nin hazırlattığı rapor, bu sistemin ilk kez hayata geçirildiği EUROPRIVACY sistemi ele alınacak ve aynı zamanda Türkiye'de Kişisel Verileri Koruma Kurumu tarafından yayınlanmış olan personel sertifikasyon mekanizmasına dair düzenlemeler ele alınacaktır.

Altıncı bölümde, kişisel verilerde akreditasyon ve sertifikasyon sisteminin hukuki güvenlik ilkesi kapsamında değerlendirilip değerlendirilemeyeceği incelenecektir.

Yedinci bölümde ise, kişisel verilerde akreditasyon ve sertifikasyon sisteminin hukuki güvenlik ilkesi kapsamında bir Anayasal hak olan kişisel verilerin korunması hakkına etkileri ele alınacaktır.

Sonuç kısmında ise GDPR kapsamındaki akreditasyon ve sertifikasyon sisteminin genel bir değerlendirilmesi yapılacak, anayasal hukuki güvenlik ilkesi ile sert çekirdekli temel haklar arasındaki muhtemel bir çatışmaya ve bu çatışmanın sonuçlarına dair değerlendirmeler yapılacak, son olarak bu sistemin geleceği ve Türkiye'ye olası etkileri ve Türkiye'de yapılabilecek akreditasyon ve sertifikasyon düzenlemesi hakkında görüşümüz açıklanarak tez sonlandırılacaktır.

1.2.3 Tezin Kaynakları

Kişisel verilerin korunması özellikle Avrupa menşeli düzenlemelerle yaklaşık elli yıldır uygulamada ve öğretilerde ele alınmakta ve teknolojik gelişmeler paralelinde de sürekli gelişmektedir. Özellikle 108 nolu Konvansiyon, OECD Rehber İlkeleri, 95/46

sayılı AB Yönergesi ve nihayet GDPR ile kişisel veri koruma hukuku benzer ilkeler ve düzenlemeler ile dünya çapında yayılmış ve yayılmaya devam etmektedir.

Bu nedenle tezde başvurduğumuz kaynaklar Türk hukuk literatüründe yer alan anayasa hukuku ile ilgili çalışmalar ile kişisel verilerin korunmasına dair çalışmaların yanı sıra başta AB olmak üzere, uluslararası, bölgesel veya diğer devletlerdeki düzenlemeleri de kapsamaktadır.

Bu bağlamda kişisel verilerin korunması alanında ve anayasa hukuku alanında yazılmış Türkçe, İngilizce, Fransızca ve İtalyanca kitapların yanı sıra, özellikle akreditasyon ve sertifikasyon konusunda AB'nin çıkardığı rehberler, AB'nin çeşitli kurum ve kuruluşları tarafından hazırlanan raporlar ile İngilizce, Fransızca ve İtalyanca dillerinde yazılmış çeşitli bilimsel makalelerden ve çeşitli internet kaynaklarından da faydalanılmıştır.

Ancak belirtmek gerekir ki gerek tez konusunda gerekse kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemi konusunda çok kısıtlı çalışmalar bulunmaktadır. Bu nedenle toplanan ve yukarıda bahsi geçen tüm kaynaklar tez konusunu doğrudan ele alan kaynaklar olmayıp, tarafımızca özgün bir şekilde fikrin teze dökülmesinde kullanılan dolaylı kaynaklar olarak göz önünde tutulmalıdır.

2. KAVRAMSAL AÇIKLAMALAR

2.1 Genel Olarak

Kişisel verilerin korunması hukuku alanı, teknik yönü yoğun olan bir alan olarak karşımıza çıkmaktadır. Aynı zamanda diğer hukuk alanlarına kıyasla yeni bir hukuk alanı olması ve kendine özgü düzenlemeleri ve terminolojisi olması dolayısıyla bazı kavramların bu kısımda açıklanması gerekmektedir. 2016 yılından beri uygulanan 6698 sayılı Kişisel Verilerin Korunması Kanun'u¹ ve ikincil düzenlemeleri ve Kişisel Verileri Koruma Kurumu'nun kararları ve rehberleri ile Türk hukukunda da bazı kavramlar artık terminolojik olarak oturmuş sayılabilir. Yine de uygulamada kavram kargaşasının devam ettiği tarafımızca gözlemlenmektedir. Bu nedenle tezde anlatım birliğinin sağlanması ve terminolojinin oturtularak doğru anlaşılması için bazı kavramlar bu kısımda ele alınacaktır.

2.2 Veri, Bilgi, Kişisel Veri

Uygulamada en çok karıştırılan kavramlar “veri” ve “bilgi” kavramlarıdır. Bunların yanı sıra “kişisel veri” kavramına uygulamada halen birçok kişinin farklı anlamlar verdiği tarafımızca gözlemlenmektedir. Tezin ana konusunun kişisel veri olması nedeniyle bu kavramların açıklanması ve aralarındaki farkların izah edilmesi gerekmektedir.

2.2.1 Veri

TDK Sözlüğü'nde “veri” *“bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done”* olarak tanımlanmaktadır². Yine “veri” kavramı

¹ RG. T. 7.4.2016, S. 29677.

² Veri kavramının tanımı için: <https://sozluk.gov.tr/>, (e.t. 26.09.2022).

anlamlarından biri olarak “bilgi, data” kavramları kullanılmaktadır³. Bir başka tanıma göre veri, bilginin bilgisayarlar tarafından kullanılabilir ve işlenebilir sayısal birimler ile gösterilen formudur⁴.

2.2.2 Bilgi

TDK Sözlüğü’nde “bilgi” *İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat; öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, vukuf; insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü*” olarak tanımlanmaktadır⁵.

Başka bir tanıma göre “bilgi”, *“anamlı bir biçime sokularak, kullanıcısına güncel ve olası kararların alınmasında yardımcı olan veri”*dir⁶. Başka bir tanıma göre ise “bilgi”, *“verinin işlenmek suretiyle alıcısının anlamasının sağlandığı haline diğer bir ifadeyle veri ile anlamın birleşmesi halidir”*⁷. ISO 27001 Bilgi Güvenliği Yönetimi Standardında ise bilgi, bir gerçek kişi veya tüzel kişi için bir değeri olan veriler bütünü olarak tanımlanmaktadır⁸.

Dolayısıyla bu tanımlardan yola çıktığımızda bilginin veriden daha ileri bir aşamayı, daha geniş bir kavramı ifade ettiğini tespit etmekteyiz⁹. Ancak günümüzde, TDK Sözlüğünde de görüldüğü üzere genel olarak veri ile bilgi eş anlamlı olarak

³ COŞKUN, Cemrenur: Milletlerarası Özel Hukukta Haksız Fiil Bağlamında Kişisel Verilerin Korunması, Yetkin Yayınevi, Ankara 2023, s.23.

⁴ KAMA IŞIK, Sezen: Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, Oniki Levha Yayınları, İstanbul 2020, s.62.

⁵ Bilgi kavramının tanımı için: <https://sozluk.gov.tr/>, (e.t. 26.09.2022), GÜRSES, Bekir: AB ve Türk Hukukunda Kişisel Verilerin Korunması: Mevzuat Uyumuna Yönelik Bir Değerlendirme, Platon Hukuk Yayınları, İstanbul 2022, s.48.

⁶ KÜZECİ, Elif: Kişisel Verilerin Korunması, Oniki Levha Yayınevi, İstanbul 2021, s.12.

⁷ YILMAZ, Berrak: Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Yetkin Yayınevi, Ankara 2022, s.25.

⁸ CASTROREALE, Renato/PONTI, Chiara: Il Sistema Integrato Per La Sicurezza Delle Informazioni Ed Il GDPR, EPC Editore, Rome 2021, s.16.

⁹ KÜZECİ, s.12, YILMAZ, s.25, BAŞAR, Cemal: Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, Yayınlanmış Doktora Tezi, İzmir 2019, s.12, Ulusal Tez Merkezi | Anasayfa (yok.gov.tr), (e.t. 26.09.2022).

kullanılmaktadır. Ancak belirtmek gerekir ki bütün veriler bilgi olduğu halde bütün bilgiler veri değildir¹⁰.

2.2.3 Kişisel Veri

Avrupa’da ilk kez Almanya’nın Hesse Eyaleti’nde 1970 yılında kişisel verilerin korunması hakkında düzenleme yapılmıştır¹¹. Kişisel veri, 6698 sayılı Kanun’da “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)’nin hazırladığı ve kişisel verilere dair ilk milletlerarası belge olan, “Mahremiyetin ve Kişisel Verilerin Sınırötesi Transferinin Korunmasına Dair OECD Rehber Prensipleri”nin “Genel Tanımlar” başlığında 1. maddede kişisel veriler, “*kimliği belirli veya belirlenebilir bir gerçek kişiye dair her türlü veri*” şeklinde tanımlanmıştır¹².

Kişisel Verilerin Otomatik İşlenmesine Dair Bireylerin Korunması Hakkında 108 Sayılı Avrupa Konseyi Sözleşmesi’nin “Tanımlar” başlığı altındaki 2. maddesinde kişisel veriler, “*kimliği belirli ya da belirlenebilir kişilere (veri öznesine) dair her türlü veri*” şeklinde aynen OECD rehberindeki gibi tanımlanmıştır¹³.

Avrupa Parlamentosu ve Konseyi’nin 24.10.1995 tarih ve 95/46/EC sayılı “Kişisel Verilerin İşlenmesine Dair Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımına Dair Yönerge”nin 2. maddesinde ise kişisel veri yine OECD Rehberi ve 108 Sayılı Konvansiyon ile aynı şekilde, “*kimliği belirli veya belirlenebilir bir gerçek kişiye*

¹⁰ AKGÜL, Aydın: Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Yayınlanmış Doktora Tezi, Kocaeli 2013, s.6., Ulusal Tez Merkezi | Anasayfa (yok.gov.tr), (e.t. 26.09.2022).

¹¹ TOPALOĞLU, Mustafa: Bilişim Hukuku, Karahan Kitabevi, Adana 2005, s.166.

¹² OECD tarafından yapılan tanım için: <https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1664218853&id=id&accname=guest&checksum=64B27A30C461A9063F681CB8FCDD0B85>, (e.t. 26.09.2022).

¹³ 108 sayılı Avrupa Konseyi Sözleşmesi için: <https://rm.coe.int/1680078b37>, (e.t. 26.09.2022), TANSUĞ, Çağla: İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması, Oniki Levha Yayınları, İstanbul 2023, s.11, COŞKUN, s.24.

ilişkin her türlü” veri olarak tanımlanmış ancak “kimliği belirlenebilir” kavramı için de aynı maddede bir açıklama yapılmıştır. Maddeye göre kimliği belirlenebilir gerçek kişi, “bilhassa kimlik numarası veya kişiye münhasır olan fiziki, fizyolojik, zihni, ekonomik, kültürel yahut içtimai kimliğine dair bir yahut daha fazla etmene atfen, doğrudan veya dolaylı biçimde belirlenebilen kişidir”¹⁴.

Nihayet Avrupa Parlamentosu ve Konseyi’nin 27.04.2016 tarih ve 2016/679 sayılı “Kişisel Verilerin İşlenmesine Dair Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımına ve 95/46/EC Yönerge’nin Yürürlükten Kaldırılmasına Dair Tüzük”ün (GDPR) “Tanımlar” başlıklı 4. maddesinde kişisel veri yine, *“kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü”* veri olarak tanımlanmış ancak *“kimliği belirlenebilir”* kavramı için de 95/46/EC sayılı Yönerge’de olduğu gibi aynı maddede bir açıklama yapılmıştır. Maddeye göre kimliği belirlenebilir gerçek kişi, *“bilhassa isim, kimlik numarası, coğrafi yer verisi, çevrimiçi bir tanımlayıcı gibi tanımlayıcılar veya kişiye münhasır olan fiziki, fizyolojik, genetik, zihni, ekonomik, kültürel yahut içtimai kimliğine dair bir yahut daha fazla etmene atfen, doğrudan veya dolaylı biçimde belirlenebilen kişidir”¹⁵.*

Bütün bu tanımlardan yola çıkacak olursak kişisel veri ile ilgili şu sonuçlara varabiliriz: Kişisel veri, kimliği belirli veya belirlenebilir olan bir gerçek kişiye dair her türlü veridir¹⁶.

¹⁴ 95/46/EC sayılı Yönergenin metni için: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN> , (e.t. 26.09.2022), BALABAN, Mahmut Furka.; Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2023, s.77.

¹⁵ GDPR’daki kişisel veri tanımı için: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1489-1-1> , (e.t. 26.09.2022).

¹⁶ TOPALOĞLU, s.163., HİZARCİ, Emine: 6698 Sayılı KVKK’nun AB Veri Koruma Hukuku Işığında Değerlendirilmesi, Yetkin Yayınları, Ankara 2020, s.19., AŞIKOĞLU, Şehriban İpek: AB ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Oniki Levha Yayınları, İstanbul 2018, s.5., ÇEKİN, Mesut Serdar: AB Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, Oniki Levha Yayınları, İstanbul 2020, s. 44., ÇAVUŞOĞLU,

Dolayısıyla kişisel veri mefhumundan, 95/46 sayılı Yönerge ve GDPR’da yapılan açıklamalar da göz önüne alınmak suretiyle, kişi ile ilgili olabilecek, bir şekilde o veriden hareketle bir gerçek kişiyi tanımlayabilecek, bizi o kişiye bir şekilde götürebilecek tüm veriler anlaşılmalıdır. Bir kişinin kimlik numarası, bedeni nitelikleri, sağlığına dair bilgiler, etnik kökeni, inancı, politik görüşü, genetik verileri, mali durumu, eğitim durumu, adresi, banka verileri, içtimai hayatı, çevrimiçi hareketleri, mobil cihazlar üzerinden yaptığı haberleşmeler, internete bıraktığı çeşitli doğrudan veya dolaylı izler

Gökçe Filiz/YILMAZ, Süleyman: Kişisel Verileri Koruma Hukuku, Yetkin Yayınları, Ankara 2020, s.35., CİVELEK, Dilek Yüksel: Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, T.C. Başbakanlık DPT Müsteşarlığı Bilgi Toplumu Daire Başkanlığı, Uzmanlık Tezi, Ankara 2011, s.59., KANGAL, Zeynel T.: Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, Oniki Levha Yayınları, İstanbul 2019, s.20., AKGÜL, Aydın: Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınevi, İstanbul 2014, s. 7., TURAN, Metin: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2019, s.52., AYÖZGER, A. Çiğdem: Kişisel Verilerin Korunması, Beta Yayınevi, İstanbul 2016, s.5., ÖZKAN, Oğulcan: Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara 2020, s.5., BÜK, Alaattin: Bilişim Alanında Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2018, s.33., DEVELİOĞLU, Hüseyin Murat: AB Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması, Oniki Levha Yayınları, İstanbul 2017, s.5., YILDIZ, Elif: Kişisel Verilerin Korunması Hukuku, Bilge Yayınevi, Ankara 2021, s.16., ALTINDERE, Murat: Kişisel Verilerin Korunması Hukuku ve Uygulaması, Adalet Yayınevi, Ankara 2020, s.30., KAMA IŞIK, s.62., TEPE, Esra: Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2021, s.22., YILMAZ, s.19., DÜLGER Murat Volkan: Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul 2020, s.62., DENİZ, İlknur: Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve KVKK Kapsamında Korunması, Seçkin Yayınevi, Ankara 2021, s.69., ÇAVUŞOĞLU, Gökçe Filiz: Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları, Yetkin Yayınevi, Ankara 2021, s.17., BASKIN, Onur: Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2021, s.21., UYARER GÖÇMEN, Sinem: Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2020, s.106., GÜREL, Begüm/BULGURCU, Berfin Helin: Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı, Platon Hukuk, İstanbul 2020, s.13., YİĞİT, Esra: İş İlişkisinde Kişisel Verilerin Korunması, Güncellenmiş 2. Bası, Oniki Levha Yayınları, İstanbul 2023, s.1., BERBER KESER, Leyla/BİLGİLİ, Ali Cem (Editörler): “Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku”, Marmara Hukuk Bilimsel Toplantılar Serisi I, 17 Nisan 2019, Haydarpaşa, Oniki Levha Yayınları, İstanbul 2020., YILMAZ, Ozan Barış: Türkiye ve Avrupa Birliği’nde Kişisel Verilerin Korunması ve Uygulanacak Hukuk, Adalet Yayınevi, Ankara 2022, s.25., KOTİL ÖĞRETMEN, Zeynep: Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka, Oniki Levha Yayınları, İstanbul 2022, s.80., TANSUĞ, s.26., GÜRSER, s.45., CASSANO, Giuseppe/COLAROCCO, Vincenzo/GALLUS Giovanni Battista/MICOZZI, Francesco Paolo: Il Processo Di Adeguamento al GDPR, GIUFFRÉ Edizioni, Milano 2022, s.11., TEPE, s.22., LANDY, Gene K.: The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law, Syngress Publishing, 2008 United States of America, s.454., OKUR, Zeki: İş Hukukunda Elektronik Gözetleme, Legal Yayınevi, İstanbul 2013, s.73., SEVİMLİ, Ahmet K.: İşçinin Özel Yaşamına Müdahalenin Sınırları, Legal Yayınevi, İstanbul 2006, s.119., KORKMAZ, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Seçkin Yayınevi, Ankara 2017, s.22.

gibi bilgilerin tümü, bir gerçek kişiyi tanımlamaya, diğerlerinden ayırd etmeye yarayabileceği için kişisel veri olarak kabul edilmektedir¹⁷.

Teknolojinin gelişimi ile daha önce kişisel veri olarak düşünülemeyecek yepyeni veriler de kişisel veri olarak ortaya çıkmaktadır. Örneğin bir pilotun radyasyon maruziyet oranı, bir hastaya verilecek yemek içeriğine dair barkod, internete bağlantısı olan bir mobil cihazın ethernet donanımının MAC adresi gibi sayılamayacak kadar çeşitli durumlarda ortaya çıkabilen veriler hep kişisel veriler olarak nitelendirilecektir. Bu veriler ilk bakışta kişisel veri olarak değerlendirilmeyebilir veya anlaşılmayabilir ama kişisel verilerin işlendikleri süreçlerin analiz edilmesi neticesinde bu süreçlerdeki veri setlerinin içerisinde yukarıdaki tanıma uyan çeşitli veriler bulunup çıkarılabilir.

2.3 Veri Sorumlusu, Müşterek Veri Sorumlusu, Veri İşleyen

Kişisel verileri koruma hukukunun kişisel veri tanımından sonra en önemli kavramları veri sorumlusu ve veri işleyen kavramlarıdır. Bu kavramlar verisi alınan ve işlenen gerçek kişilerin verileri üzerinde çeşitli tasarruflarda bulunan iki farklı ama birbirleri içinde hukuki bağımlılıkları olan hukuk sükelerini tanımlamaktadır. Bu nedenle bu kavramların da doğru anlaşılması büyük önem arz etmektedir.

¹⁷ BAŞALP, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara 2004, s.33., ÜÇÜNCÜ, Sümeyye Hilal: Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, Yayınlanmış Doktora Tezi, Ankara 2018, s.4., AYDIN, Sedat Erdem: AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, 12 Levha Yayınevi, İstanbul 2015, s.5., KABADAYI, Elif Sinem: Unutulma Hakkı, Yetkin Yayınları, Ankara 2021, s.38., DOĞAN, Bayram: Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, Adalet Yayınevi, Ankara 2022, s.48., BOZKURT, Habip: Kişisel Verilerin İşlenmesinin Hukuki Boyutu, Yetkin Yayınları, Ankara 2021, s.3., BAŞAR, s.7, AKGÜL, s.4, YILMAZ, s.25, KÜZECİ, s.10, GÜREL/BULGURCU, s.13, UYARER GÖÇMEN, s.107., DENİZ, s.71., DÜLGER, s.155., ÇAVUŞOĞLU/YILMAZ, s.35., ÖZKAN, s.9., KANGAL, s.22., KAMA IŞIK, s.63., BÜK, s.21., TURAN, s.58., TEPE, s.22.

2.3.1 Veri Sorumlusu

İlgili kişi yani verileri işlenen gerçek kişi dışında kişisel veri işlemeye dair hukuki düzenlemelerde en önemli hukuk s  jelerinden biri veri sorumlusudur. Veri sorumlusu verilerin işlenmesinin amaç ve araçlarına karar veren kişi ya da örg  t   ifade eder¹⁸.

6698 sayılı Kanun’un 3/1-ı maddesi uyarınca veri sorumlusu, *“kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya t  zel kişi”* olarak tanımlanmıştır. 95/46 sayılı Y  nergesi’nin 2/d maddesinde veri sorumlusu *“yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve y  ntemleri belirleyen gerçek veya t  zel kişi, kamu kuruluşu, kurumu veya diğ  r herhangi bir organ”* olarak tanımlanmış¹⁹, keza GDPR m.4/7 ile de bu tanım aynen alınmıştır²⁰.

Veri sorumlusu, veriyi işleyen kişiyi ya da veriye sahip olan kişiyi belirtmemektedir²¹. Veri sorumlusunu belirlerken temel kriter kişisel veriyi işleme veya kişisel verinin sahipliğı diğ  l, işlemler   zerindeki denetimin kime ait olduğudur²². Bu denetimi belirleme aynı zamanda veri işleme y  ntemini belirlemeyi de i  ermektedir²³.

Veri sorumlusu ger  ek kişiler olabileceğı gibi kamu kuruluşları, şirketler, dernekler, vakıflar ve sair t  zel kişilikler de olabilir²⁴. Ancak t  zel kişilik organizasyon

¹⁸ K  ZEC  , s.17., DEN  Z, s.93.,   AVUŐ GLU, s.53., BASKIN, s.64., G   MEN UYARER, s.118., DOĐAN, s.54., DEM  RBAŐ , Ali: Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Y  k  ml  l  kleri, Oniki Levha Yayınları, İstanbul 2023, s.17.

¹⁹ 95/46 sayılı Direktifteki veri sorumlusu tanımı i  in: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN>, (e.t. 16.02.2024).

²⁰ GDPR’daki veri sorumlusu tanımı i  in: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1>, (e.t.16.02.2024, DEM  RBAŐ , s.18.

²¹   AVUŐ GLU/YILMAZ, s.51.

²² K  ZEC  , s.17.,   AVUŐ GLU/YILMAZ, s.51., G   MEN UYARER, s.118., DOĐAN, s.55.

²³   AVUŐ GLU/YILMAZ, s.52.

²⁴   ZKAN, s.78.,   AVUŐ GLU/YILMAZ, s.51., D  LGER, s.188., ALTINDERE, s.34., G   MEN UYARER, s.118., Kişisel Verilerin Korunması Kanunu Tasarısı ve Adalet Komisyonu Raporu i  in: <https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf> ,(e.t. 27.09.2022).

yapısına bağı olarak çalışan gerçek kişiler veya tüzel kişiliği bulunmayan şubeler ve birimler, veri sorumlusu sıfatını haiz olmayacaktır²⁵. Veri sorumlusu olmaya dair hukuki statü bakımından veri sorumlusunun özel hukuk tüzel kişisi veya kamu hukuku tüzel kişisi olmasının bir önemi yoktur²⁶.

Belirli bir mesleği, bazı meslek kuralları ve yasal düzenlemeler kapsamında yürüten avukat, mali müşavir, noter gibi meslek mensupları, faaliyetlerini icra ederken işledikleri kişisel veriler yönünden veri sorumlusu olacaklardır. Bu gibi meslekleri icra edenlere kendi kanunlarınca veya meslek kurallarınca kişisel verileri işleme kapsamı, sınırları, zorunlulukları ve bu işlemeye dair yetkileri ve sorumlulukları konusunda düzenleme getirilmektedir²⁷. Bu düzenlemeler kapsamında da bu tür meslek mensupları işledikleri kişisel veriler üzerinde denetim yetkisine sahip oldukları için veri sorumlusu olarak sayılacaklarında bir tereddüt bulunmamalıdır.

Şirketin resmi kararı olmamasına karşın şirket yönetim kurulu üyesinin, kamera kayıtları vasıtasıyla gizlice çalışanları takip etmesi halinde dahi sadece şirket, veri sorumlusu olacak; veri güvenliğini sağlamakla yükümlü şirket, yönetim kurulu üyesinin eylemleri sonucu ortaya çıkabilecek hukuka aykırı veri işleme faaliyetinden dolayı veri sorumlusu sıfatıyla sorumlu olacaktır²⁸.

Veri sorumlusunun, veri işleme faaliyetinin yanı sıra verilerin hukuka uygun bir biçimde işlenmesi ve aktarımı, verilerin muhafazası için gerekli idari ve teknik tedbirlerin alınması gibi veri yaşam döngüsünde hukuka uygun kişisel veri almayı ve işlemeyi

²⁵ ÖZKAN, s.78., 100 Soruda Kişisel Verilerin Korunması Kanunu, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf>, (e.t. 27.09.2022).

²⁶ BASKIN, s.64.

²⁷ DÜLGER, s.191.

²⁸ 29. Madde Çalışma Grubu, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, (e.t. 27.09.2022).

sağlamak konusunda geniş yükümlülöklere sahip olması sebebiyle, hangi gerçek veya tüzel kişilerin veri sorumlusu olacaklarının tespiti önem arz etmektedir²⁹.

6698 sayılı Kanun’da veri sorumlusu net bir biçimde tanımlanmış olsa da uygulamada veri sorumlusunun belirlenmesi sırasında bazı somut kriterlerin göz önünde tutulması gerekmektedir. Bu bağlamda Kişisel Verileri Koruma Kurumu’nun yayınladığı rehberde yer verdiği aşağıda sayılmış olan ölçütlerin belirlenmesinde söz sahibi olan gerçek veya tüzel kişi, veri sorumlusu olarak değerlendirebilecektir³⁰.

- Kişisel verilerin işlenmesi ve işleme yöntemi,
- İşlenecek kişisel veri ve kişisel veri grupları,
- Kişisel verisi işlenecek ilgili kişi grupları,
- İşlenecek kişisel verilerin hukuki işleme dayanakları,
- İşlenen kişisel verilerin hangi amaçlarla kullanılacağı,
- İşlenen kişisel verilerin üçüncü taraflarla paylaşılıp paylaşılmayacağı,
- Kişisel verilerin aktarılacağı üçüncü taraflar,
- Üçüncü taraflara aktarılacak kişisel veriler, aktarım amacı ve hukuki dayanağı,
- İlgili kişilerin haklarının nasıl sağlanacağı,
- İşlenen kişisel verilerin saklama yöntemi ve saklama süresi,
- Saklama süresinin sona ermesini takiben kişisel verilerin imha yöntemi.

²⁹ ÇEKİN, s.53.

³⁰ Kişisel Verileri Koruma Kurumu’nun Veri Sorumlusu ve Veri İşleyen Rehberi: <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>, (e.t. 27.09.2022)., Avrupa Veri Koruma Otoritesi Veri Sorumlusu ve Veri İşleyen Rehberi: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf, (e.t. 27.09.2022), İngiliz Veri Koruma Otoritesi’nin Veri Sorumlusu Veri İşleyen Rehberi: <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> (e.t., 27.09.2022)., ÇEKİN s.54., DÜLGER s.211., KÜZECİ s. 366.

2.3.2 Müşterek Veri Sorumlusu

Müşterek veri sorumlusu kavramı, bir veri kayıt sistemi kapsamındaki veri işleme süreçlerinde, bu süreçlerin amaçlarının ve yöntemlerinin birden fazla veri sorumlusunca müşterek bir şekilde belirlenmesi için kullanılmaktadır³¹.

Müşterek veri sorumlusu kavramı, GDPR’ın 26. maddesi ile düzenlenmiş olup, 6698 sayılı Kanun’da müşterek veri sorumlusu kavramına dair açık bir düzenleme bulunmamaktadır. Bununla birlikte 6698 sayılı Kanun’un mehzaz düzenlemesi olan 95/46 sayılı AB Yönergesinde yer alan “*tek başına veya başkalarıyla birlikte*” ibaresinin 6698 sayılı Kanun’a alınmamış olmasının müşterek veri sorumlusu kavramının Türk hukukunda tümüyle dışlanmadığını, çünkü “*tek başına*” şeklinde bir ibareye 6698 sayılı Kanun’da yer verilmemiş olmasının bir kısıtlama getirmediği olarak yorumlanması gerektiğini ileri süren bir görüş bulunmaktadır³². Bu görüşe, hukuk tekniği açısından katılmamakla beraber, uygulamada teknolojinin de gelişimi nedeniyle müşterek sorumluluk teşkil eden birçok müşahhas olayın meydana geldiğini gözlemlediğimiz için, bu hususta açık bir yasal düzenleme yapılincaya kadar, gerçek hayattaki bu durumun, pratik nedenlerden dolayı, yukarıda belirtilen görüşe itibar edilerek çözülmesi gerektiği kanaatindeyiz.

Nitekim belirttiğimiz teknolojideki gelişmeler ve kişisel veri işleme faaliyetlerindeki yakınsama nedeniyle uygulamada çıkan durumları çözmede doğrudan bir düzenleme yapmanın yeterli olacağı görüldüğü için GDPR ile müşterek veri sorumlusu konusu açık bir düzenlemeye kavuşturulmuştur.

Müşterek veri sorumlusu kavramında taraflar arasında akdedilecek sözleşmede, GDPR yükümlülüklerinin ifası ve ilgili kişi haklarının karşılanması hususlarında

³¹ DÜLGER, s.196., DEMİRBAŞ, s.53.

³² DÜLGER, s.196.

tarafların rollerinin ve sorumluluklarının ele alınması gereklidir. Fakat bu tespit icra edilirken sözleşmede yazılmış olan hususlar ile yetinilmeyerek, faaliyetlerin icrasındaki hakiki ve cari kişisel veri işleme yaşam döngüsünün incelenmesi gerekir³³.

GDPR, yukarıda bahsi geçen müşterek veri sorumluları arasında akdedilecek bu sözleşmeye özel bir önem atfetmektedir³⁴. Gerçekten de gerçek kişilerin haklarının korunabilmesi açısından bir veri işleme faaliyetindeki hukuk sùjelerinin hukuki statülerinin net olarak belirlenmesi aynı zamanda Anayasal bir hak olan hukuk güvenliğı ilkesi ile de doğrudan bağlantılıdır. Bu nedenle bu yapılacak sözleşmenin tarafların yükümlölüklerini ve haklarını tereddüde yer vermeyecek şekilde açık ve şeffaf bir biçimde yansıtması gerekmektedir.

Müşterek veri sorumluları arasındaki ilişkinin yoğun veya zayıf olmasının herhangi bir önemi yoktur. Buna ek olarak veri sorumlularından birinin bütün kişisel veriye erişim sağlayamaması müşterek veri sorumluluğunu ortadan kaldırmayacaktır³⁵. Göz önüne alınması gereken kriter, toplu bir şekilde müşterek veri sorumlularınca kişisel verileri işleme amaçlarının ve yöntemlerinin tespit edilmesidir. Başka bir söyleyişle, müşterek veri sorumlusu hususunda, veri işleme amaçlarının ve yöntemlerinin bir tek veri sorumlusunca belirlenmiyor oluşu kafi gelecektir³⁶.

6698 sayılı Kanun’da müşterek veri sorumlusuna ilişkin belirsizliğe karşın, 20 Ocak 2022 tarihli ve 31725 sayılı Resmi Gazete’de yayımlanan “Araç Kiralama Sektöründe Kara Liste Uygulamaları Hakkında İlke Karar” ile müşterek veri sorumlusuna

³³ DÜLGER, s.196.

³⁴ DÜLGER, s.197.

³⁵ Avrupa Adalet Divanı Başsavcısı Mengozzi’nin görüşü: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=198949&pageIndex=0&doclang=en&mode>, (e.t. 29.09.2022)

³⁶ KÜZECİ s.365.

dair açık bir hukuki atıf yapılmıştır³⁷. İlke Karar’da Kurum, araç kiralama sektöründe kullanılan uygulamalarda veri girişi gerçekleştiren firma dışındaki sair araç kiralama firmalarının da söz konusu kişisel verilere aynı veri tabanı üzerinden erişimini ve hakimiyetini göz önünde tutarak yazılımı kullanan ve yazılımdan menfaat sağlayan araç kiralama firmalarını ve yazılım firmasını müşterek veri sorumlusu olarak değerlendirmektedir.

Bu kararında Kurum, müşterek veri sorumlularının kusur sorumluluklarını değerlendirirken, işlenen verinin ilk ve son kullanıcısının kim olduğu, verinin kim tarafından işlendiği, veri işleme amacı, verinin silinmesine, değiştirilmesine veya aktarılmasına kim tarafından karar verildiği ve veriyi toplayan veri sorumlusu dışındaki veri sorumlularının veri işleme faaliyetleri gibi ölçütlerin göz önünde tutulması gerektiğini vurgulamaktadır.

Kanunla ele alınması gerekli bir düzenlemenin normlar hiyerarşisine aykırılık teşkil edecek bir biçimde ikincil düzenleme vasıtasıyla, müşterek veri sorumlusu müessesesinin kabul edilmesi, müşterek veri sorumlusuna dair net bir tanımlama yapılmaması ve müşterek veri sorumlusunun belirlenmesi sırasında esas alınacak kıstasların ifade edilmemesi sebepleriyle İlke Karar’ın isabetli olmadığı, ancak 6698 sayılı Kanun’da yapılacak düzenleme sonrası müşterek veri sorumluluğunun uygulama alanı bulması gerektiği kanaatindeyiz.

Yapılacak kanun değişikliğinde müşterek veri sorumlusu ele alınırken GDPR’da olduğu gibi veri sorumlusu dışında ayrı bir hüküm altında düzenleme yapılması ve düzenlenecek hükümde, müşterek veri sorumlularının kendi aralarındaki ilişkilere dair düzenlemelere de yer verilmesi gerekmektedir. Ayrıca değişiklik sonrası Kanun’da

³⁷ RG. T. 20.01.2022, s.31725

müşterek veri sorumlusu hükümlerinin düzenlenmesini müteakiben, iyi uygulama örnekleri oluşturması adına Kurum rehberleri ve Kurul kararları gibi ikincil düzenlemeler ile kavramın desteklenmesi de büyük önem arz etmektedir.

2.3.3 Veri İşleyen

Veri işleyen, veri sorumlusunun tanıdığı yetkiye istinaden, onun namına kişisel verileri işleyen gerçek ve/veya tüzel kişilerdir³⁸. Veri sorumlusu ile veri işleyen arasındaki ilişki bir veri işleme sözleşmesi ile düzenlenmektedir. Bu sözleşmede, kişisel verilerin veri sorumlusundan veri işleyene aktarılması, bu aktarımın yöntemleri³⁹, aktarımda alınacak teknik tedbirler, sınır aşan bir veri aktarımı varsa kişisel verilerin uluslararası aktarımına dair yerel ve uluslararası mevzuata göre yapılması gerekenler, veriyi aldıktan sonra veri işleyenin veriyi işleme metodları, kullandığı araçlar, bu işleme faaliyeti ile ilgili aldığı hukuki, idari ve teknik tedbirler, verilerin saklanması ve işleme amacı ortadan kalktıktan sonra verileri iadesi ya da imhası gibi birçok konu düzenlenmektedir.

Ancak bu yapılan sözleşme tarafların hukuki statüsünün tespitinde dikkate alınacak olmakla birlikte veri koruma otoriteleri, mahkemeler ve veri sahipleri gibi üçüncü kişiler açısından bağlayıcı değildir⁴⁰. Veri sorumlusu ya da veri işleyen olmaya dair hukuki statü; taraflar arasındaki ilişkiye, teknik düzenlemelere, kimin kişisel veri üzerinde ne gibi yetkileri olduğuna ve bu yetkileri nasıl kullandığına bakılarak ve ilgili kişisel veri işleme faaliyetinin yer aldığı süreçler incelenerek belirlenecektir.

³⁸ KÜZECİ, s.18., ALTINDERE, s.35., DOĞAN, s.55., GÜREL/BULGURCU, s.17., GÖÇMEN UYARER, s.69., ÇAVUŞOĞLU, s.52., DENİZ, s.95.

³⁹ BOZKURT, s.19., GÖÇMEN UYARER, s.70.

⁴⁰ GÖÇMEN UYARER, s.70.

6698 sayılı Kanun'un 3/1-ğ maddesi uyarınca veri işleyen “*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak tanımlanmıştır. GDPR m.4/8’e göre ise veri işleyen, “*veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*”dır Veri işleyen kavramından söz edilebilmek için veri işleyen, veri sorumlusunun talimatlarına bağlı gerçek veya tüzel kişi olmalı ve veri sorumlusu adına veri işleme faaliyeti gerçekleştirmelidir. Yani veri işleyen kişisel verileri kendi namına işlememekte, veri sorumlusunun talimatları doğrultusunda işlemektedir⁴¹.

Belirli bir kişisel veri işleme faaliyetine dair bir iş sürecinde kimin veri sorumlusu yahut veri işleyen olduğunu belirleyebilmek için, hangi kişisel verilerin, hangi metodlarla işleneceğini, ne kadar ve nasıl tutulacağını belirleyen kim olduğuna bakmak gerekmektedir. Bu soruların cevaplarını veren taraf veri sorumlusu olacaktır⁴².

Veri işleyen hukuki statüsünün tespiti bakımından uygulanması gereken ölçütlerden biri de bir veri sorumlusunun namına faaliyet icra ediyor olmaktır. Eğer veri işleyen, veri sorumlusu adına icra ettiği faaliyetten veri işleme sözleşmesindeki veri işleme karşılığı elde edeceği menfaatin dışında bir menfaat elde ediyorsa, o takdirde artık veri sorumlusunun adına hareket etmemekte, bu nedenle de bu elde ettiği menfaat nedeniyle bu işleme faaliyeti açısından veri sorumlusu haline gelmektedir⁴³.

Veri sorumlusu, yapacağı kişisel veri işleme sözleşmesi ile, aşağıda örnek olarak belirtilen hususlarda karar verme yetkisini veri işleyene bırakabilir⁴⁴:

⁴¹ ÖZKAN, s.79.

⁴² ÖZKAN, s.80., BASKIN, s.65.

⁴³ DÜLGER, s.209.

⁴⁴ Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu Veri İşleyen Rehberi”, s.3., <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf>, (e.t. 28.09.2022).

- Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı,
- Kişisel verilerin hangi yöntemle saklanacağı,
- Kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları,
- Kişisel verilerin aktarımının hangi yöntemle yapılacağı,
- Kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için hangi metotun kullanılacağı,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemlerinin neler olacağı.

Hem GDPR’da hem 6698 sayılı Kanun’da veri sorumlusu ile veri işleyen müşterek olarak sorumlu tutulmuşlardır. 6698 sayılı Kanun’un 12 (2) maddesinde bu durum, *“veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.”* şeklinde belirtilmiştir.

6698 sayılı Kanun ile GDPR’deki veri işleyen tanımlarının büyük bir ölçüde örtüşmesine karşın veri işleyene atfedilen yükümlülüklerde 6698 sayılı Kanun’un GDPR’ın gerisinde kaldığı görülmektedir⁴⁵. 6698 sayılı Kanun’da veri işleyenin, kişisel veri güvenliğinin sağlanması, kişisel verilerin hukuka aykırı aktarılmayacağı ve işleme amaçları dışında kullanılmayacağı yükümlülükleri bulunurken, GDPR kapsamında veri işleyenlerin kayıt alma, veri koruma görevlisi (*data protection officer*) atama, sınır ötesine veri aktarımı gibi yükümlülükleri gündeme gelebilecektir⁴⁶.

⁴⁵ ÇEKİN s.63., BAKIREL, Nur Buğçe: Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımının Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi, Yüksek Lisans Tezi, Ankara 2020, s.42.

⁴⁶ DÜLGER, s.213.

2.4. Veri Sorumlularının Yükümlülükleri

Kişisel verileri koruma düzenlemeleri ile belirlenen veri sorumlusu ve veri işleyenlere düzenlemeler tarafından çeşitli yükümlülükler yüklenmiştir. Bu yükümlülükler açısından en fazla sorumluluk taşıyan hukuk süjesi veri sorumlusudur⁴⁷.

Bu yükümlülükler genel olarak aydınlatma yükümlülüğü, veri sahiplerine tanınan hakların kullandırılmasına dair yükümlülük, veri güvenliğine dair yükümlülükler, Türkiye ve İngiltere gibi bazı ülkeler bakımından veri sorumluları sicilinde kayıt yükümlülüğü, irtibat kişisi ve veri koruma uzmanı atama yükümlülükleri olarak başlıklandırılabilir. Devam eden kısımda bu yükümlülüklerle ilişkin temel bilgiler verilmiştir.

2.4.1 Aydınlatma Yükümlülüğü

Türkiye Cumhuriyeti Anayasası kapsamında, herkes, kişisel verilerinin işlenmesi hakkında bilgilendirilme, kişisel verilerine ulaşma ve kişisel verilerinde değişiklik (düzeltmeler) yapılmasını veya kişisel verilerinin imha edilmesini isteme gibi bazı haklara sahiptir. İşte bu hakların neler olduğu, nasıl kullanılacağı gibi konularla ilgili olarak gerçek kişilerin aydınlatılması yükümlülüğü veri sorumlusuna aittir⁴⁸. Aydınlatma yükümlülüğü, ilgili kişinin işlenen kişisel verileri ile ilgili bilgilendirilmesine dair var olan ve Anayasa ile güvence altına alınmış olan hakkının ve ilgili kişinin kendi kişisel verilerinin geleceğini tayin etme hakkının karşılığını teşkil etmektedir⁴⁹. Bu bakımdan da aydınlatma yükümlülüğü, haklar penceresinden bakıldığında aynı zamanda ilerleyen kısımlarda ele aldığımız ilgili kişinin bilgi edinme hakkı olarak karşımıza çıkmaktadır.

⁴⁷ DEMİRBAŞ, s.11.

⁴⁸ ÇAVUŞOĞLU/YILMAZ, s.99., DEMİRBAŞ, s. 59., ÖZKAN, s.135., DOĞAN, s.66., KAMA IŞIK, s.275., DÜLGER, s.524.

⁴⁹ ÖZKAN, s.135.

Aydınlatma yükümlülüğü GDPR’ın 13-14. maddelerinde, ilgili kişinin hakları başlıklı üçüncü bölümünün “bilgilendirme ve kişisel verilere erişim” başlıklı ikinci kısmında düzenlenmiştir. Türkiye’de ise 6698 sayılı Kanun’un 10. maddesi ile düzenlenmiştir. Bu düzenlemeler AB’nin 95/46/EC sayılı yürürlükten kaldırılan Yönergesi ile de çok benzerdir⁵⁰.

Aydınlatma yükümlülüğü, ana olarak, ilgili kişinin kişisel verilerinin işlenmesi esnasında, kişi, sebep, amaç, işleme yöntemleri, hukuki sebepler, işleme dayanakları, verinin paylaşıldığı yerler, saklama süreleri ve yasal hakların kullanılma yöntemi unsurları çerçevesinde aydınlatılmasını içerir⁵¹. Aydınlatma yükümlülüğünün kapsamı 6698 sayılı Kanun’un 10. maddesi ile ve daha detaylı olarak da Kişisel Verileri Koruma Kurumu’nun 10.03.2018 tarihli ve 30356 sayılı Resmi Gazete’de yayınlanan “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ ile belirlenmiştir⁵².

Aydınlatma yükümlülüğü veri sorumlusunun mutlak bir yükümlülüğü olarak karşımıza çıkmaktadır. Başka bir deyişle, veri sorumlusu hangi kişisel veri işleme şartına dayanırsa dayansın, bu dayanaklar veri sorumlusunu aydınlatma yapma yükümlülüğünden kurtarmaz. Kişisel verinin işlendiği her durumda aydınlatma yapılmalıdır⁵³. Bu yükümlülük idare için de yaptığı tüm veri işleme faaliyetleri için geçerlidir⁵⁴. Böylece idarenin şeffaflığı da sağlanmaktadır⁵⁵. Bu açıdan, veri sorumlusunun bir özel hukuk tüzel kişisi veya bir kamu tüzel kişisi olup olmaması aydınlatma yükümlülüğü bakımından bir fark yaratmaz. Fakat 6698 sayılı Kanun’un

⁵⁰ DEMİRBAŞ, s.11., DOĞAN, s.66., TEPE, s.75.

⁵¹ TEPE, s.75.

⁵² ALTINDERE, s.70., DÜLGER, s.524.

⁵³ ÖZKAN, s.136.

⁵⁴ TANSUĞ, s.95.

⁵⁵ BOZKURT, s.209.

28'inci maddesi ile getirilen istisnaların aydınlatma yükümlülüğü bakımından da istisna teşkil edeceği gözden uzak tutulmamalıdır⁵⁶.

2.4.2 İlgili Kişilere Haklarını Kullandırma Olanaklarını Sağlama Yükümlülüğü

İlgili kişiler GDPR m.15 – 22, KVKK m.11’de düzenlenen ve bir sonraki bölümde ele alacağımız verilerin işleme amaçlarını öğrenme, paylaşıldığı yerleri öğrenme, imha talebinde bulunma gibi çeşitli haklara sahiptirler. Gerek GDPR’da gerek KVKK’da gerekse de dünyanın çeşitli ülkelerindeki düzenlemelerde bu hakların ilgili kişilere kullandırılması ile ilgili veri sorumlularına yükümlülükler yüklenmiştir. Bu yükümlülüğün yerine getirilmesine ilişkin yürütülen süreç mahremiyet terminolojisinde “DSAR – Data Subject Access Request/İlgili Kişi Başvuru Talebi” süreci denilmektedir. GDPR’da 15. madde, KVKK’da ise 13. madde ile düzenlenmiştir. Türk Kişisel Verileri Koruma Kurumu ilgili kişilerin haklarını nasıl kullanacakları ile ilgili detaylı düzenlemeyi 10.03.2018 tarihli ve 30356 sayılı Resmi Gazete’de yayınlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ile yapmıştır.

İlgili kişi, veri sorumlusuna yapacağı başvuru ile bir yandan KVKK 11. madde kapsamındaki haklarına dair taleplerini veri sorumlusuna iletirken diğer yandan Türk Kişisel Verileri Koruma Kurumu’na başvurabilmesi için zorunlu bulunan veri sorumlusuna başvuruya dair yolu tüketmektedir⁵⁷.

KVKK m.13/2 hükmü gereğince, veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmak zorundadır. Veri sorumlusunun bu başvuruları ne şekilde ele alacağı, başvurunun usulü ve veri sorumlusunun başvuruya cevabında yer alması gereken unsurlar

⁵⁶ BOZKURT, s.211, İdarenin aydınlatma yükümlülüğünün istisnaları hakkında ayrıntılı bir inceleme için bkz. TANSUĞ, s.131 vd.

⁵⁷ DEMİRBAŞ, s.141., ÖZKAN, s.158.

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ile ayrıntılı bir şekilde düzenlenmiştir.

KVKK m.14 kapsamında, ilgili kişinin yaptığı başvurunun veri sorumlusu tarafından reddedilmesi, verilen cevabın yetersiz olması veya süresinde başvuruya yanıt verilmemesi durumunda ise, ilgili kişi veri sorumlusunun cevabını tebellüğ ettiği veya otuz günlük sürenin bittiği tarihten itibaren otuz gün ve her halükârda başvurudan itibaren altmış gün içinde ilgili kişi Kişisel Verileri Koruma Kurulu'na şikâyetle bulunabilir.

2.4.3 Kişisel Veri Güvenliğine İlişkin Yükümlülükler

Bilişim teknolojileri alanındaki hızlı gelişmeler, veri sorumlularının uğrayabilecekleri zararları, riskleri ve tehditleri arttırmaktadır. Bu tehditler karşısında ise sadece teknik tedbirlerin alınması yeterli olmamakta, özellikle sosyal mühendislik gibi durumlara karşı insanların farkındalığının artırılması ve böylece insan faktörüne dayalı veri ihlallerinin önlenmesi gerekmektedir⁵⁸.

Bu hızlı ilerleme nedeniyle de dünya üzerinde kanun koyucular veri sorumluları ve veri işleyenlere çeşitli teknik ve idari tedbirler alma yükümlülükleri getirmişlerdir. Veri sorumluları ve veri işleyenler kişisel verilerin ilk kez alınmasından başlamak üzere işlenmesi, aktarılması, saklanması gibi tüm aşamalarda tedbirler almak ve kişisel verilerin yeterli güvenlik düzeyini sağlamakla yükümlüdürler. Bu yükümlülük devamlılık arz eden bir yükümlülük olup, herhangi bir anda bu yükümlülüklerin yerine getirilmiş olması sonraki bir zamanda ve sonraki aşamalarda bu yeterli güvenliğin aranmayacağı anlamına gelmez⁵⁹. Teknolojinin sürekli gelişen doğası, özellikle de veri işleme kapasitesinin ve

⁵⁸ ALTINDERE, s.79.

⁵⁹ DÜLGER, s.537.

yöntemlerinin olağanüstü artması, doğal olarak bu yükümlülüğü sürekli bir yükümlülük olarak karşımıza çıkarmaktadır.

Kişisel verilerin güvenliği ile ilgili tedbirler GDPR'ın 32. maddesi ile düzenlenmiş iken KVKK'da ise 12. madde ile düzenlenmiş ve her iki düzenleme de veri sorumlusunun uygun güvenlik düzeyini temin etmek için her türlü teknik ve idari tedbiri alması gerektiğini belirtmiştir⁶⁰. Bu da alınacak tedbirlerin teknik ve idari tedbirler şeklinde iki başlığa ayrıldığını bize göstermektedir. Kanaatimce bu tedbirlere üçüncü bir başlık olarak hukuki tedbirler de eklenmelidir.

Kişisel verilerin güvenliğinin sağlanması için sadece verilerin hukuka uygun olarak işlenmesi yeterli değildir⁶¹. Kaldı ki aslında kişisel verilerin genel ilkelere ve işleme şartlarına uygun olarak işlenmesi, kişisel veri mahremiyeti kavramı içinde ve “sui generis” olarak ele alınmalıdır. Bu bakımdan da kişisel verinin mahremiyet düzenlemelerine uygun olarak işlenmesi, kişisel veri güvenliğinden farklı bir konudur. Kişisel veri güvenliği verilerin hukuka aykırı bir şekilde elde edilmesi ve işlenmesinin önüne geçmeyi amaçlayan bir teknik ve idari kontroller bütünüdür. Bu nedenle de kişisel verilerin mahremiyet düzenlemelerine uygun olarak işlenmesine rağmen yetkisi olmayan üçüncü kişilerin eline geçmesi bir kişisel veri güvenliği konusudur.

Teknik ve idari tedbirler; çalışanlara eğitim verilmesi, güvenlik uyarılarının yapılması, güçlü parola kurallarının uygulanması, yetki matrislerinin ve erişim kontrollerini yapılması, veri kaybı önleme yazılımlarının kullanılması, penetrasyon testleri yaptırılması, fiziki erişim kontrollerinin yapılması gibi tedbirlerdir. Bu tedbirler

⁶⁰ DÜLGER, s.537.

⁶¹ ÖZKAN, s.139.

süreklilik arz eden bir şekilde denetlenmeli ve gelişen teknolojiye ve ihtiyaçlara göre de sürekli güncellenmelidir⁶².

Kişisel veri güvenliğine ilişkin önemli bir diğer yükümlülük ise veri sorumlusunun denetim yapma veya yaptırtma yükümlülüğüdür. Veri sorumluları bu denetimi kendileri yapabilecekleri gibi bağımsız üçüncü taraflara da yaptırtabilirler⁶³.

Bu konuda son olarak belirtilmesi gereken önemli bir husus ise, 6698 sayılı Kanun'un 12. maddesinin 2. fıkrasında belirtilen durumdur. Kişisel verilerin, veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda, birinci fıkra da belirtilen tedbirlerin alınması hususunda veri sorumlusu, bu kişilerle birlikte müştereken sorumlu olacaktır. Dolayısıyla veri işleyenler de veri güvenliğinin sağlanması için tedbir alma yükümlülüğü altındadır.

2.4.4 Veri İhlal Bildirimi Yükümlülüğü

Kişisel veri ihlali, uygun bir biçimde ve zamanında müdahale edilmediği takdirde, gerçek kişilere bedeni veya maddi zararlar verebilecek olan, kişisel verilere hukuka aykırı erişilmesi veya işlenmesi vakasıdır. Her halükârda, veri sorumlusu herhangi bir kişisel veri ihlalinin etkisini hafifletmek için çaba harcamalı ve özellikle ilgili kişiler üzerindeki etkileri ortadan kaldırmaya veya azaltmaya çalışmalıdır.

Bu nedenle kişisel verilerle ilgili hukuki düzenlemeler veri sorumlularının veri ihlali durumunda bu veri ihlalinin kişisel verileri koruma otoritelerine bildirim yükümlülüğü getirmiştir. KVKK'da bu husus 12. maddenin 5. bendi ile düzenlenmiştir. Buna göre veri sorumlularınca işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve

⁶² KAMA IŞIK, s.276.

⁶³ TEPE, s.76.

Kurula bildirmekle yükümlüdür. En kısa sürenin ne olduğu konusunda tereddütler yaşanması nedeniyle Kişisel Verileri Koruma Kurumu bu süreyi ihlalin öğrenilmesinden itibaren 72 saat olarak belirlemiştir. Bu belirlemeyi yaparken de GDPR düzenlemesine atıf yapmıştır.

Bir kişisel veri ihlali, gerçek kişiler üzerinde çeşitli önemli olumsuz etkilere sahip olabilir. Bu ihlal bedeni veya maddi zararlara yol açabilir. GDPR’da bunun kişisel verilerin kontrolünü kaybetme veya hakların sınırlanması, ayrımcılık, kimlik hırsızlığı veya sahtekarlık, mali kayıp, itibarın zarar görmesi, mesleki sır ile korunan kişisel verilerin gizliliğinin kaybı veya bireylere karşı başka önemli ekonomik veya sosyal dezavantajlar gibi faktörler içerebileceği düzenlenmiştir. Türk hukukunda ise bu konuda açık bir düzenleme bulunmamakla birlikte, Kişisel Verileri Koruma Kurumu’nun yayınladığı, veri ihlallerinde Kurum’a iletilmesi gereken veri ihlali bildirim formunda bu hususlar yer almaktadır.

GDPR m.33 ve 34 kapsamında veri sorumluları, aynen Türk hukukundaki düzenleme gibi kişisel verileri koruma otoritelerine ve ilgili kişilere bildirim yapmak zorundadırlar.

GDPR’ın Resital kısmının 88 numaralı bendinde de belirtildiği üzere; aynı zamanda, kişisel verilerin uygun teknik koruma önlemleriyle korunup korunmadığı ve bu ihlalin koşullarına göre, kimlik hırsızlığı veya diğer yanlış kullanımların olasılığını etkili bir şekilde sınırlayıp sınırlamadığı gibi, bu ihlalin koşullarına da dikkat edilmelidir.

GDPR ile yürürlükten kaldırılan 95/46/EC sayılı AB Yönergesi bu konuya değinmemiş olsa da veri ihlali bildirim kavramı AB mevzuatında yeni değildir. Örneğin, e-Gizlilik Yönergesi olarak adlandırılan AB’nin 2002/58/EC sayılı Mahremiyet ve Elektronik İletişim Yönergesi’nin 4. maddesinde, halka açık olarak sunulan elektronik

iletiřim hizmeti saęlayıcılarının, kiřisel veri ihlallerini ilgili ulusal otoritelere bildirme ve ihlal kapsamındaki vakıaları, etkileri ve alınan dzeltici nlemleri ieren bir veri ihlali envanteri tutma zorunluluęu dzenlenmiřtir.

Ulusal dzeyde, GDPR'ın yrrlęe girmesinden nce bile, bazı ye devletler veri ihlallerini ynetmek iin dzenlemeler yapmıřlardır. rneęin Alman Federal Veri Koruma Kanunu, 2009'da veri ihlallerini bildirme ykmllę getirmiřtir. 2011'de İrlanda, Bir Kiřisel Veri Gvenlik İhlali Uygulama Kılavuzu yayınlamıřtır. 2014 ve 2015 arasında İtalya, ilgili veri trne baęlı olarak veri ihlallerini bildirmek iin, Trk Kiřisel Verileri Koruma Kurulu'nun yayınladıęına benzer řablonlar yayınlamıřtır.

Kiřisel veri ihlalinin bildirilmesi ve iletiřimi; ilgili kiřilerin haklarını glendirmek, veri sorumlularının ve veri iřleyenlerin sorumluluęunu artırmak ve Avrupa'da veri gvenlięini teřvik etmek aısından veri sorumlularına bir ykmllk getirmektedir.

Kiřisel veri ihlali GDPR'ın 4. maddesinin 12. bendinde kazara veya yasa dıřı olarak kiřisel verilerin imha edilmesine, kaybolmasına, deęiřtirilmesine, izinsiz iřşasına veya eriřilmesine yol aan gvenlik ihlali olarak tanımlanmaktadır.

Her bilgi gvenlięi olayı bir kiřisel veri ihlali olmayabilir, ancak her kiřisel veri ihlali bir bilgi gvenlięi olayıdır.

AB 29. Madde alıřma Grubu (WP29) tarafından  tr kiřisel veri ihlali tanımlanmaktadır:

- Gizlilik ihlali: Yetkisiz veya kazara kiřisel verilerin iřşası veya eriřimi, bu bilgiye sahip olma hakkına sahip olmayan biri tarafından kiřisel verilerin bilgisine ulařılması durumudur.

- Erişilebilirlik ihlali: Yetkisiz veya kazara verilere erişimin kaybedilmesi veya kişisel verilerin yok edilmesi durumu, kişisel verilere erişim kontrolünün kaybedilmesi veya kişisel verilerin yanlışlıkla silinmesi ile ilgilidir.
- Bütünlük ihlali: Yetkisiz veya kazara kişisel verilerin değiştirilmesi veya bozulması ile ilgilidir.

Veri ihlali bir dizi nedenle meydana gelebilir, örneğin:

- İhmal nedeniyle,
- Bir kazanın sonucu olarak veya
- İçeriden veya dışarıdan kişiler tarafından kasıtlı olarak yapılan bir eylem sonucu.

Özetle, her kişisel veri ihlali bir güvenlik olayıdır ve duruma bağlı olarak kişisel verilerin gizliliğini, bütünlüğünü veya erişilebilirliğini ihlal edebilir veya bunların herhangi bir kombinasyonunu içerebilir. Veri ihlallerinin sebepleri arasında ihmal, kazalar veya teknik arızaların yanı sıra iç veya dış aktörlerin kasıtlı eylemleri bulunmaktadır. Bu veri ihlalleri gerçek kişiler üzerinde çeşitli etkiler yaratabilir. Bu etkilerin ortadan kaldırılması veya azaltılması için ilgili kişilere ve ilgili otoriteye bildirim yapılması veri sorumlularının en önemli yükümlülüklerinden biridir.

2.4.5 Veri Sorumluları Siciline Kayıt Yükümlülüğü

Kişisel Verilerin Korunması Kanunu'nun 16. maddesiyle, veri sorumlularının kayıt olmaları gereken Veri Sorumluları Sicili (VERBİS) düzenlenmiştir. Maddeyle, veri sorumlularının kayıt yaptırması için Kişisel Verileri Koruma Kurumu nezdinde kamuya açık olarak VERBİS sistemi oluşturulmuştur. Veri sorumluları veri işlemeye başlamadan önce Kişisel Verileri Koruma Kurumu'na başvuracak ve Kurum'dan kendilerine verilen kullanıcı adı ve şifre ile VERBİS'i doldurarak kayıtlarını yapacaklardır. Kişisel Verileri Koruma Kurulu tarafından belirlenecek objektif kriterlere göre, Kurul tarafından,

VERBİS'e kayıt zorunluluğuna istisnalar getirilebilecektir. Nitekim Kurul bazı meslek grupları için ve bazı kriterler dahilinde istisnaları belirlemiştir.

Maddenin 3. fıkrasında VERBİS'e yapılacak kayıta bulunacak unsurlar düzenlenmiştir. Bu kapsamda, veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin aktarılabilceği alıcı veya alıcı grupları, veri güvenliğine ilişkin alınan tedbirler, kişisel verilerin işlendikleri amaç için gerekli olan azami süre gibi hususlar VERBİS'e girilmelidir. Meydana gelen değişiklikler ise derhal Kurum'a bildirilecektir. Böylece VERBİS sistemindeki kayıtların güncel tutulması ve bu suretle de kamuoyunun şeffaf ve doğru bilgiye ulaşması amaçlanmıştır. VERBİS'e ilişkin sair konular ve detaylar bir yönetmelikle düzenlenmiştir.

Kurul tarafından 30.12.2017 tarihli Resmi Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik ile bu konudaki detaylı düzenleme yapılmıştır.

Veri Sorumluları Sicili'ne kayıt olmak için başvuru, aşağıdaki bilgileri içeren bir bildirim ile yapılmalıdır. Bunlar:

- Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri,
- Kişisel verilerin hangi amaçla işleneceği,
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- Kişisel verilerin aktarılabilceği alıcı veya alıcı grupları,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- Kişisel veri güvenliğine ilişkin alınan tedbirler,
- Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

2.4.6 İrtibat Kişisi ve Veri Koruma Uzmanı Atama Yükümlülüğü

6698 sayılı Kanun'a göre veri sorumlusu eğer Türkiye'de yerleşik olan bir tüzel kişi ise, bir irtibat kişisi atamak ve VERBİS'e kayıt sırasında atadığı bu irtibat kişisine ait bilgileri VERBİS'e işlemek zorundadır.

VERBİS'e kaydı yapılan irtibat kişisi, veri sorumlusu, ilgili kişi veya Kişisel Verileri Koruma Kurumu arasındaki iletişimin sağlanmasından sorumludur. 6698 sayılı Kanun kapsamındaki yükümlülük ve yaptırımlar açısından sorumluluk irtibat kişisinde değil bu tüzel kişiyi temsil ve ilzama yetkili organdadır. İrtibat kişisi olarak VERBİS'e yapılan bildirim, veri sorumlularının 6698 sayılı Kanun kapsamındaki sorumluluklarını ortadan kaldırmamaktadır.

Veri sorumlusu eğer bir kamu kurumu ise, 6698 sayılı Kanunun Geçici 1 inci maddesinin 5 inci fıkrasına istinaden Kanun'un uygulanmasıyla ilgili olarak kamu kurumunda koordinasyonu sağlamak üzere belirlenerek Başkanlığa bildirilen üst düzey yöneticinin, VERBİS'in hizmete açılması ve kayıt yükümlülüğünün başlamasının akabinde Yönetmeliğin 11 inci maddesinin 5 inci fıkrasına göre VERBİS sistemine irtibat kişisi olarak kaydının yapılması gerekmektedir.

Yönetmeliğin 11 inci maddesine göre; veri sorumlusu eğer yurtdışında yerleşik olan bir tüzel kişi ise, bir veri sorumlusu temsilcisi atamak zorundadır. Atanacak bu veri sorumlusu temsilcisi, Türkiye'de yerleşik olan bir tüzel kişi ya da Türk vatandaşı bir gerçek kişi olmak zorundadır.

Yurtdışında yerleşik tüzel kişi veri sorumluları, veri sorumlusu temsilcisi atadığına ilişkin bir karar almalı ve kararın tasdikli örneğini bildirilen bu veri sorumlusu temsilcisi marifetiyle Kuruma sunmalıdır. Bu karar, veri sorumlusu temsilcisinin yurtdışında yerleşik veri sorumlusu adına VERBİS'e ilişkin iş ve işlemleri yapmak görevinin

yanısıra, ilgili kişiler tarafından yapılacak başvurular veya Başkanlığa yapılacak tebligat ve yazışmalar konusunda iletişimi kurma görev ve yetkisinin bulunduğuna ilişkin bilgileri de içermelidir.

6698 sayılı Kanun kapsamındaki yükümlülük ve yaptırımlar açısından sorumluluk, veri sorumlusu temsilcisinde değil, bu veri sorumlusu tüzel kişiyi temsil ve ilzama yetkili olan organ üzerindedir. Veri sorumlusu atamasının yapılmış olması, Kanun hükümleri uyarınca yurtdışında yerleşik veri sorumlusunun sorumluluğunu ortadan kaldırmaz.

GDPR kapsamında ise, belli şartları sağlayan veri sorumlularının ve veri işleyenlerin bir Veri Koruma Uzmanı (DPO) ataması zorunludur. Bu durum işledikleri veri türünden bağımsız olarak tüm kamu otoriteleri ve kurumları için geçerli olduğu gibi gerçek kişileri sistemli ve büyük ölçekte izleyen veya özel nitelikli kişisel veri kategorilerini büyük ölçekte işleyen diğer kuruluşlar için de geçerlidir.

GDPR kapsamında bir DPO atanması zorunlu olmasa dahi, kuruluşlar bazen gönüllü olarak bir DPO atayabilirler.

DPO kavramı yeni değildir. 95/46/EC sayılı Yönerge hiçbir kuruluşa DPO atama zorunluluğu getirmese de yıllar içinde birkaç üye ülkede DPO atama uygulaması gelişmiştir.

GDPR'ın kabulünden önce, WP29, DPO'nun hesap verebilirliğin temel taşı olduğunu ve bir DPO atamanın uyum sağlamayı kolaylaştırabileceğini ve ayrıca işletmeler için rekabet avantajı haline gelebileceğini verdiği görüşlerde belirtmiştir.

Hesap verebilirlik araçlarının uygulanması yoluyla uyumu kolaylaştırmanın yanı sıra (örneğin, veri koruma etki değerlendirmelerini ve denetimleri kolaylaştırma veya gerçekleştirme), DPO'lar ilgili taraflar arasında arabuluculuk yapmaktadırlar, örneğin, kişisel veri koruma otoriteleri, ilgili kişiler ve bir kuruluşun içindeki iş birimleri gibi.

GDPR'a uyumsuzluk durumunda DPO'lar bireysel olarak sorumlu değildir. GDPR, işlenen verilerin GDPR m.24(1) hükümlerine uygun olarak işlendiğini sağlama ve bunu kanıtlama yükümlülüğünün veri sorumlusu veya veri işleyen tarafından yerine getirilmesi gerektiğini açıkça belirtmektedir.

Veri sorumlusu ve veri işleyen ayrıca DPO'nun görevlerini etkin bir şekilde yerine getirmesine olanak sağlamak zorundadır. Bir DPO atamak birinci adım olmakla birlikte, DPO'lara görevlerini etkili bir şekilde yerine getirebilmeleri için yeterli özerklik ve kaynak da sağlanmalıdır.

GDPR m.37(1), aşağıdaki üç durumda bir DPO atanmasını zorunlu kılmaktadır:

- İşlem, bir kamu otoritesi veya kurumu tarafından gerçekleştiriliyorsa;
- Veri sorumlusu veya veri işleyenin temel faaliyetleri, büyük ölçekte düzenli ve sistemli olarak ilgili kişileri izlemeyi gerektiren işlemlerden oluşuyorsa;
- veya
- Veri sorumlusu veya veri işleyenin temel faaliyetleri, büyük ölçekte özel veri kategorilerinin veya suç ve suçlamalara ilişkin kişisel verilerin işlenmesinden oluşuyorsa.

Bir kuruluş gönüllü olarak bir DPO atadığında, GDPR'ın 37 ila 39. maddelerindeki gereklilikler, atamanın zorunlu olduğu durumda olduğu gibi atama, pozisyon ve görevleri için geçerlidir. Bu, gönüllü olarak bir DPO atamak istemeyen ve yasal olarak bir DPO atama zorunluluğu olmayan bir kuruluşun, yine de kişisel verilerin korunmasıyla ilgili görevleri olan personel veya dış danışmanlar istihdam etmesine engel teşkil etmemektedir.

2.4.7 Kişisel Veri İşleme Envanteri Hazırlama Yükümlülüğü

GDPR'ın 30. maddesi, veri sorumlularının ve veri işleyenlerin, kuruluşları içinde kişisel veri işlenen süreçlerdeki veri işleme faaliyetlerini doğru bir şekilde gösteren detaylı bir kişisel veri işleme envanteri hazırlama yükümlülüğü getirmektedir. Bu yükümlülüğe kişisel veri mahremiyeti terminolojisinde ROPA (Register of Processing Activities – İşleme Faaliyetleri Kaydı) adı verilmektedir. İlgili iş süreçlerindeki kişisel veri işleme faaliyetlerinin doğru olarak kişisel veri işleme envanterlerinde gösterilmesi hesap verebilirlik ve şeffaflık kriterleri açısından olduğu kadar veri sorumlusunun içinde veri yönetiminden ve kişisel verilerin yönetilmesinden sorumlu olan birimlere de bir harita sağlaması bakımından çok önemlidir. Envanterdeki hatalar veya güncel olmayan bilgiler veri işleme faaliyetinin hukuka aykırı hale gelmesine neden olabilir.

GDPR'ın 30(1) maddesi, kişisel verileri işleyen tüm kuruluşların, veri sorumlusu ya da veri işleyen olarak, sorumlulukları altındaki işleme faaliyetlerini kayıt altında tutmaları gerektiğini düzenlemektedir. 30(1) Maddesi, bu kayıta aşağıdaki bilgilerin bulunmasını zorunlu kılmaktadır:

- Veri sorumlusunun adı ve iletişim bilgileri, varsa, müşterek veri sorumlusu, veri sorumlusunun temsilcisi ve Veri Koruma Uzmanı (DPO) bilgileri,
- İşleme amaçları,
- Veri konularının kategorileri ve kişisel verilerin kategorilerinin açıklaması,
- Kişisel verilerin aktarıldığı veya aktarılacağı alıcıların kategorileri,
- Kişisel veriler üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılıyorsa, bu üçüncü ülkenin veya uluslararası kuruluşun bilgileri,
- Alınan teknik ve idari tedbirler
- Saklama süreleri

Bu kayıtlar, bir organizasyonun hangi kişisel verileri işlediğini, bu verileri neden kullandığını, kimlere aktardığını ve gerektiğinde hangi üçüncü ülkelere veya uluslararası kuruluşlara aktardığını anlamak için kritik öneme sahiptir. Ayrıca, kişisel verilerin korunması için alınan önlemlerin etkinliğini de değerlendirmek için önemlidir. Bu kayıtların eksik veya yanlış olması, GDPR uyumlu olmayan bir veri işleme sürecine yol açabilir ve organizasyon için ciddi uyumluluk sorunlarına neden olabilir.

Türk hukukunda ise kişisel veri işleme envanteri, 30.12.2017 tarihli Resmi Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 4. maddesinin 1. fıkrası (h) bendinde tanımlanmıştır. 28.04.2019 tarihli Resmi Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 1. maddesi ile bentte bir değişiklik yapılmıştır.

Veri Sorumluları Sicili Hakkında Yönetmelik’in 4. maddesine göre kişisel veri işleme envanteri veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri ifade eder.

Buna göre envanter, iş süreçlerindeki veri işleme faaliyetleri çerçevesinde kişisel veri işleyen veri sorumluları tarafından bütün iş süreçlerinin ele alınması, bu süreçler çerçevesindeki bütün veri işleme faaliyetlerinin incelenmesi, tüm faaliyetlerle alakalı olarak işlenen kişisel verilerin tespit edilmesi, bu tespit edilen kişisel verilerin hangi amaçlarla ve hukuki sebeplere dayalı olarak işlendiğinin tespiti, üçüncü taraflara transfer edilip edilmediği, ediliyorsa kimlere transfer edildiği, işlenmekte olunan kişisel verilerin

ilgili kişilerinin kimler olduğu, tespit edilen kişisel veriler ile alakalı olarak belirlenen saklama müddetleri, sınırötesi veri transferi olup olmadığı, kişisel verilerin güvenliğinin sağlanması amacıyla ne gibi teknik veya idari tedbirlerin hayata geçirildiği bilgilerinin yer aldığı önemli bir dökümandır.

Kişisel veri envanteri oluşturulmasına dair bir düzenleme getirilmesindeki amaç; veri sorumlularının kişisel veri işledikleri faaliyetlerinin ilişkili olduğu bütün iş süreçlerinde Kanun’a uyumun tesis edilmesi, diğer bir deyişle Kanuna aykırı bir kişisel veri işleme faaliyetinin yapılıp yapılmadığının tespit edilmesi, veri yönetişimi, veri mimarisi gibi birimler ile bilgi güvenliği önlemlerini almakla yükümlü olan birimlere ve kişisel verilerin korunması mevzuatını yöneten kişilere bir harita verilmesini sağlamaktır. Örneğin bir dinamik veritabanı maskeleyme ihtiyacı var ise bu maskeleymenin hangi süreçlerde hangi veriler için yapılacağına belirlenmesi, bir veri kaybı önleme yazılımının politikalarının hangi iş süreçlerinde hangi veriler için uygulanacağını tespit edilmesi, bir veri sınıflandırma çalışmasında veri kategorilerinin, verilerin işlendiği süreçlerin tespiti gibi çeşitli konularda kişisel veri işleme envanteri anahtar bir rol oynayacaktır.

Veri Sorumluları Sicili Hakkında Yönetmeliğin 5. maddesinin 1. fıkrası (ç) bendine göre, “Sicile kayıtlı yükümlü olan veri sorumluları, Kişisel Veri İşleme Envanteri hazırlamakla yükümlüdür. Sicil başvurularında Sicile açıklanacak bilgiler Kişisel Veri İşleme Envanterine dayalı olarak hazırlanır.” hükmü, (d) bendinde de, Kanunun 10. maddesinde veri sorumluları için belirtilen aydınlatma yükümlülüğünde, Kanunun 13. maddesinde belirtilen ilgili kişi başvurularının yanıtlanmasında ve ilgili kişiler tarafından açıklanacak açık rızanın kapsamının belirlenmesinde kişisel veri işleme envanterine dayalı olarak Sicile sunulan ve Sicilde yayınlanan bilgiler esas alınır hükmü yer almaktadır.

Ayrıca Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 5. maddesinin 1. fıkrasında, Kanunun 16. maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür hükmü yer almaktadır.

Bu hukuki düzenlemeler kapsamında Veri Sorumluları Siciline kayıt yükümlülüğü bulunan bütün veri sorumlularının kişisel veri işleme envanteri oluşturması zorunludur. Bu envanter üzerinden de sicile kayıt ve aydınlatma yükümlülüğü yerine getirilirken veya ilgili kişi başvuruları yanıtlanırken ve açık rızanın kapsamı belirlenirken veri sorumluları tarafından bu kişisel veri işleme envanterine müracaat edilecektir.

2.5 Veri Sahiplerinin Kişisel Verilerin Korunması Kapsamındaki Hakları

2.5.1 Genel Olarak

Kişisel verilerin korunmasına ilişkin olarak gerek Türk hukukunda gerek AB hukukunda yapılan düzenlemeler ile ilgili kişiye, kişisel verilerinin korunmasını sağlamaya yönelik olarak sürece aktif bir şekilde katılmasına ve kendi kişisel verilerinin üzerinde hakimiyet kurabilmesine yönelik haklar tesis edilmiştir⁶⁴. İşlenen kişisel verilerine ulaşma hakkı, kişisel verilerinin düzeltilmesini isteme hakkı ve bazı şartların gerçekleşmesi durumunda veri işlemeye itiraz etme hakkı bu haklar kapsamında sayılabilir.

İşlenen kişisel verilere ulaşma hakkı, bilgi edinme hakkı ile yakın ilişkilidir. Veri sorumlusunun, kişisel verilerinin işlendiği konusunda ilgili kişiyi bilgilendirmemesi durumunda, ilgili kişinin bu işlemeden bilgisi olmayacağından, kişisel verilerine ulaşma,

⁶⁴ KÜZECİ, s.247., CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.73., YILDIZ, Sevil: Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, Nobel Yayınevi, Ankara 2007, s.188.

düzeltilme, sildirme, yok etme, üçüncü kişilere aktarılmasını engelleme gibi haklarını da kullanabilmesi mümkün olmayacaktır. İlgili kişinin kişisel verilerine ulaşma hakkı, çeşitli hukuki metinler ile düzenleme altına alınmıştır. GDPR ile bugün kapsamlı bir haklar manzumesi ilgili kişilere tanınmıştır.

GDPR haricinde 108 nolu Konvansiyon, OECD Rehber İlkeleri ve BM Rehber İlkeleri'nde kişilere tanınan haklar bakımından düzenlemeler bulunmaktadır. AİHM de kararlarında ilgili kişinin verilerine erişim hakkının AİHS'nin 8. maddesi kapsamında korunduğunu belirtmiştir. Çeşitli ülkelerde özellikle GDPR model alınarak yapılan düzenlemelerde de birbirine çok benzer haklar ilgili kişilere tanınmış bulunmaktadır.

GDPR kapsamında tanınan haklar da Türk hukukundaki haklar ile büyük benzerlik göstermekte ancak bazı haklar yönünden Türk hukukundan ayrılmaktadır. GDPR ile, ilgili kişilere bilgi alma hakkı, kişisel verilere erişme hakkı, düzeltme hakkı, kişisel veri işlemeye son verme hakkı, kişisel veri işlemeyi sınırlama hakkı, kişisel veriyi bir veri sorumlusundan diğerine taşıyabilme hakkı, kişisel verilerin işlenmesine itiraz etme hakkı ve otomatik işleme tabi tutulan kişisel verilere dayanılarak verilen karara itiraz etme hakkı ve unutulma hakkı tanınmıştır⁶⁵.

Türk hukuku bakımından Türkiye Cumhuriyeti Anayasası m.20/3'de kişisel verilerin korunmasını isteme hakkının, kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi kapsadığı düzenlenmektedir. Bu sebeple, KVKK m.11'de sayılan ilgili kişi hakları anayasal güvence altındadır⁶⁶.

⁶⁵ CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.74

⁶⁶ ÖZKAN, s.154.

Kişisel Verilerin Korunması Kanunu'nun 11. maddesinde kişisel verileri işlenen ilgili kişinin hakları düzenlenmektedir. Bu düzenlemeye göre, kişisel verileri işlenen ilgili kişi, kişisel verilerinin işlenip işlenmediğini öğrenme, işleniyorsa buna ilişkin bilgileri talep etme, kişisel verilerin işlenme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurtiçinde veya yurtdışında verilerin aktarıldığı üçüncü kişileri bilme, 7. maddede öngörülen koşullar çerçevesinde kişisel verilerin silinmesini, yok edilmesini yahut kişisel verinin içeriğinin eksik ya da gerçeğe aykırı olması hallerinde bunların düzeltilmesini isteme haklarına sahiptir. Bu maddeye dayalı olarak ilgili kişi, talebi doğrultusunda yapılan düzeltme, silme ve yok etme işlemlerinin, verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, verilerinin kanuna aykırı olarak işlenmesi nedeniyle zarara uğraması halinde, veri sorumlusundan zararın giderilmesini talep etme haklarına da sahiptir.

Madde ile ilgili kişinin, kişisel verilerinin otomatik sistemler kullanılarak analiz edilmesi suretiyle kendisi hakkında çıkan aleyhe neticelere de itiraz hakkının bulunduğu düzenlenmiştir.

Genel olarak hem Türk hukukunda hem de GDPR ve diğer ülke hukukları ile uluslararası düzenlemelerde ilgili kişilere tanınan hakları aşağıdaki şekilde özetlemek mümkündür.

2.5.2 Bilgi Alma Hakkı

Bilgi alma hakkı, GDPR'da 12. ve devamı maddelerde, KVKK'da ise 11. maddede düzenlenmiştir. Her iki düzenlemede de kişisel verilerin alınmasından itibaren veri sorumlusunun ve bulunuyorsa veri koruma uzmanının kimlik ve iletişim bilgileri ile

işleme amacı ve işleme faaliyetlerinin neler olduğu konusunda ilgili kişinin bilgi alma hakkı olduğu düzenlenmiştir⁶⁷.

Kişisel verilerin korunması alanında ilgili kişinin en temel hakkının bilgi alma hakkı olduğu söylenebilir. İlgili kişi kendisi hakkında işlenen kişisel verilerle ilgili her türlü bilgiye erişebilmeli ve bilgi alabilmelidir. Bu hakkın temel bir hak olarak ifade edilmesinin nedeni, çoğu durumda, bu hak kullanılmadan diğer hakların kullanılmasının mümkün olmamasından kaynaklanmaktadır⁶⁸.

KVKK m.11 kapsamında ilgili kişi, kişisel verilerinin işlenip işlenmediğini öğrenme, eğer kişisel verileri işlenmiş ise işlenen kişisel veriler hakkında bilgi alma, kişisel verilerin hangi amaçla işlendiğini ve bu verilerin işlendikleri amaçlara uygun kullanılıp kullanılmadığını öğrenme hakkına sahiptir⁶⁹.

Veri sorumluları, kişisel verilerin işlenmesi ile ilgili tüm bilgileri ilgili kişiye açık, anlaşılır ve gereğinden uzun veya kısa olmayacak şekilde sağlamalıdır⁷⁰. Yapılan bilgilendirme açık ve sade bir dille sahip olmalı, ortalama bir zekaya sahip herkesin anlayabileceği şekilde hukuki ve teknik dilden arı olmalıdır.

Bu noktada fiziksel veya zihinsel engelliler ile çocukların da bilgi alma hakkının bulunduğunu, bu nedenle bu gruplara yönelik özel bilgilendirme yöntemlerinin kullanılması gerektiğini belirtmek isterim. Nitekim sadece çocuklara yönelik özel düzenlemelerin de yapıldığı görülmektedir. Örneğin GDPR 8.maddesi ile çocukların verilerinin işlenmesine yönelik özel bir düzenleme getirmiştir. Benzer şekilde ABD’de COPPA (Children’s Online Privacy Protection Act – Çocukların Çevrimiçi

⁶⁷ GÜRSER, s.85., DÜLGER, s.472., ÖZKAN, s.154., DOĞAN, s.68., ÇAVUŞOĞLU/YILMAZ, s.97., KAMA IŞIK, s.269., YİĞİT, s.187., KÜZECİ, s.248.

⁶⁸ ÖZKAN, s.154., DÜLGER, s.472., BOZKURT, s.217.

⁶⁹ UYARER GÖÇMEN, s.143.

⁷⁰ DÜLGER, s.473.

Mahremiyetinin Korunması Yasası) ile doğrudan çocuklara yönelik mahremiyet düzenlemeleri yapılmıştır⁷¹. Bu yaklaşım kapsamında videolar, animasyonlar, infografikler, görme engelli yazısı, büyük fontların kullanılması, gece görünümü gibi görsel işitsel duylara hitap eden çok çeşitli bilgi verme metotları ve teknolojileri kullanılmalıdır. Yine ayrıca dezavantajlı bu grupların dışında diğer kişilere de artık yazılı bir şekilde bilgi vermekten ziyade daha kolay anlaşılabilir, yukarıda belirtilenler veya uygun olabilecek diğer yöntemlerle bilgi verme yönünde bir eğilim olduğu da gözlemlenmektedir. Bu durumun bilgi alma hakkının özüne daha uygun olduğu kanaatindeyim.

2.5.3 Erişim Hakkı

Kişisel verilerin korunması ile ilgili yasal düzenlemelerin tanıdığı hakların kullanılabilmesi için yukarıda da belirttiğimiz üzere kişinin kendi verileri üzerinde bir hakimiyetinin olması ve kişisel verilerinin geleceğini belirleyebilecek durumda olması gerekir. Bunun için ise ön koşul kişinin bu işlenen kişisel verilerine ulaşabilmesidir. Şeffaf bir şekilde veri sorumluları ilgili kişilerin kendi kişisel verilerine ulaşabilmelerine ve yasal düzenlemeler ile güvence altına alınan haklarını kullanabilmelerine imkân tanımak zorundadırlar. Başka bir deyişle, bu veriler veri sorumluları nezdinde tamamen genel ilkelere ve işleme şartlarına uygun işleniyor ve tutuluyor olsa dahi, ilgili kişi açısından bu kişisel veriler her daim erişilebilir, denetlenebilir ve gerektiği takdirde de müdahale edilebilir halde olmalıdır⁷².

Uluslararası ve ulusal birçok düzenlemede ilgili kişinin veri sorumlularının veya veri işleyenlerin elinde bulunan kişisel verilerine erişme hakkı bulunduğu düzenlenmiştir.

⁷¹ TOPALOĞLU, s.173., LANDY, s.476.

⁷² DÜLGER, s.476.

GDPR, 108 Numaralı Konvansiyon, OECD Rehber İlkeleri, BM Rehber İlkeleri gibi düzenlemeler bunlara örnek verilebilir. AİHM de ilgili kişinin kişisel verilerine erişim hakkını AİHS'nin 8. maddesi kapsamında değerlendirmektedir⁷³.

Erişim hakkı GDPR'da 15. madde ile düzenlenmiştir. GDPR'da ilgili kişiye erişim hakkı tanınmasının amacı, kişisel veriyi işlemenin hukuka uygun şekilde yapıldığından emin olmak ve bu uygun işlemeyi teyit etmek olarak belirtilmiştir⁷⁴. Buna göre, ilgili kişi kişisel verilerinin işlenip işlenmediğini öğrenmenin yanı sıra, işlemenin amaçları, işlenen kişisel veriler ve kişisel veri kategorileri, aktarım yapılması durumunda aktarılan kişisel veriler ve kişisel veri kategorileri, kişisel verilerin saklanma süresi, düzeltme, işlemenin sınırlandırılmasını talep etme ve işlenen kişisel verilerinin bir kopyasının kendisine verilmesini isteyebilir. İlgili kişi talebini elektronik yoldan yapmış ise ve aksi ilgili kişi tarafından belirtilmemişse veri sorumlusu işlenen kişisel verilerin bir kopyasını elektronik ortamda ilgili kişiye verecektir⁷⁵.

Ancak bu erişim hakkının sınırının ne olduğu GDPR'da veya KVKK'da belirtilmemiştir. Yani ilgili kişinin, işlenen kişisel verilerinin bizzat işlenmiş hallerini veri sorumlusunun kayıt sisteminde tutulduğu haliyle talep edip edemeyeceği belli değildir. Türk Kişisel Verileri Koruma Kurulu bu konuda verdiği bir kararda konuyu Türk hukuku açısından açıklamıştır. Kurul 14.01.2020 tarih ve 2020/13 sayılı kararında ve bu karara da atıf yaparak verdiği 30.06.2020 tarih ve 2020/504 sayılı kararında şu şekilde bir karar vermiştir:

“6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinin birinci fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler

⁷³ KÜZECİ, s.251., DOĞAN, s.69., BOZKURT, s.218., GÖÇMEN/UYARER, s.145., GÜRSER, s.86.

⁷⁴ DÜLGER, s.477.

⁷⁵ CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.86.

işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığına ve erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağladığına,

Ancak bu hakkın, kişisel verilerin işlendiği veri kayıt sisteminin/kayıt ortamının doğrudan kendisine erişimi, bu kayıt ortamının kendisinin ilgili kişiye teslimini veya doğrudan verinin kendisinin “elde edilmesini” değil; veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri de dikkate alınarak, işlenen kişisel verilerin, teknik/fiziki imkânların el verdiği ölçüde ve verinin muhtevasına/içeriğine ilgili kişi tarafından makul bir şekilde ulaşılabilmesine imkân tanınmasını kapsadığına,

Şikâyetçi ilgili kişinin, veri sorumlusu tarafından işlenen kişisel verilerinin içeriğine, içeriğin tam olarak anlaşılmasına imkan tanıyacak şekilde erişim hakkı ile veri sorumlusunun, teknolojik olarak müdahale ve tahrif edilerek aleyhe kullanılabilecek olan ve şikâyetçi dışındaki kişilerin de hassas nitelikli verisini içeren konuşma kayıtlarının kaydedildiği kayıt ortamının kendisinin, ancak yasal makamlar tarafından talep edildiği takdirde teslim edilebileceği yönündeki, makul kabul edilebilecek açıklaması arasındaki dengenin, şikâyetçi ilgili kişi tarafından veri sorumlusundan talep edilen ses kayıtlarına ilişkin kayıt ortamlarının doğrudan ilgili kişiye teslimi suretiyle değil; ancak, talep edilen ses kayıtlarının dökümlerine, verilerin içeriğinin ilgili kişi tarafından tam olarak anlaşılmasına imkan tanıyacak şekilde, erişim hakkı sağlanarak gerçekleştirilebileceğine...”

Bu kararda ilgili kişinin; telefon kayıtlarının bizzat kendisine, veri sorumlusunun veri kayıt sisteminde erişmek istediği, ancak burada yapılan bir denge testi uyarınca telefon görüşmelerinin transkriptlerinin verilmesinin yeterli olacağı yönünde bir kanaate

varılarak, kişisel verilere erişim hakkının bizzat kişisel verilerin işlendiği kayıt ortamına erişilerek veya o kayıt ortamı alınarak kullanılamayacağına dair Kurul tarafından karar verilmiş ve böylece bu husus aydınlatılmıştır⁷⁶.

2.5.4 Veri Taşınabilirliği

Veri taşınabilirliği hakkı, 95/46/EC sayılı Yönergede yer almayan, teknolojinin gelişimine bağlı olarak ortaya çıkmış olan ve ilk kez GDPR m.20 ile tanınan yeni bir haktır. Bu hak 6698 sayılı Kanun'da yer almamaktadır.

Veri taşınabilirliği hakkı özetle, ilgili kişinin bir hizmet sağlayıcıda yer alan tüm kişisel verilerini bu hizmet sağlayıcıdan alarak diğer bir hizmet sağlayıcıya aktarabilme hakkıdır⁷⁷. Bu hak kapsamında, ilgili kişinin, işlenen kişisel verilerini yapılandırılmış, yaygın olarak kullanılan ve bir makine tarafından okunabilecek formatta alma hakkı bulunmaktadır⁷⁸. Ayrıca, ilgili kişi kişisel verilerini aldığı veri sorumlusunun herhangi bir engellemesi olmadan başka bir veri sorumlusuna bu hak kapsamında verebilmelidir⁷⁹.

Veri taşınabilirliği 6698 sayılı Kanun'da bir hak olarak tanınmamış olmasına karşın elektronik haberleşme sektöründe bu hakkın bir uygulaması olarak karşımıza numara taşınabilirliği çıkmaktadır⁸⁰. Bu kapsamda, bir abone bir operatörden diğer bir operatöre telefon numarasını taşıyarak o operatörün hizmetlerinden faydalanabilmektedir⁸¹. Ancak elektronik haberleşme sektörüne ve mevzuatına ait bu

⁷⁶ Kişisel Verileri Koruma Kurumu'nun 2020/13 sayılı kararı için: <https://kvkk.gov.tr/Icerik/6698/2020-13>, (e.t.15.12.2023)., Kişisel Verileri Koruma Kurumu'nun 2020/504 sayılı kararı için: <https://kvkk.gov.tr/Icerik/6932/2020-504>, (e.t. 15.12.2023).

⁷⁷ BALABAN, s.243., CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.98., THIENE, Arianna/CORSO, Stefano: La Protezione dei Dati Sanitari: Privacy e Innovazione Tecnologica tra Salute Pubblica e Diritto alla Riservatezza, Jovene Editore, Napoli, 2023, s.59., DÜLGER, s.483., GÜRSSES, s.93.

⁷⁸ CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.99., DÜLGER, s.483.

⁷⁹ KAMA IŞIK, s.270.

⁸⁰ Numara Taşınabilirliği Yönetmeliği için: <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=13180&MevzuatTur=7&MevzuatTertip=5>, (e.t. 15.12.2023).

⁸¹ BALABAN, s.245.

uygulamanın genel bir hak kategorisi olarak kişisel verilerin korunması alanına teşmil edilmesinin mümkün olmadığı kanaatindeyiz. Bu nedenle numara taşınabilirlik hakkına rağmen Türk hukukunda GDPR'ın 20. maddesini karşılayacak bir düzenlemenin bulunmadığını söylemek yanlış olmayacaktır.

2.5.5 Düzeltme Hakkı

İlgili kişinin, bir veri sorumlusu tarafından işlenen kişisel verilerinin noksan, hatalı veya güncel olmaması durumunda yine bilgi alma hakkı, erişim hakkı gibi haklarını kullanmasına engel teşkil edecek veya hakkını gereği gibi kullanamamasına neden olacak durumlar ortaya çıkacaktır. Bu sebeple ilgili kişiye tanınan bir diğer hak, ilgili kişinin veri sorumlusu tarafından işlenen veya saklanan kişisel verilerinde düzeltme talep edebilmesi hakkıdır⁸². Bu hak GDPR m.16 ile, Türk hukukunda ise 6698 sayılı Kanun'un 11/d maddesinde düzenlenmiştir. Düzeltme hakkı ayrıca tamam olmayan, eksik olan bilginin tamamlanması hakkını da kapsamaktadır. Ayrıca bu hak hem GDPR'da hem 6698 sayılı Kanun'da sayılan genel ilkelerden olan kişisel verilerin doğru ve gerektiğinde güncel olması ilkesi ile de doğrudan bağlantılıdır⁸³.

İlgili kişinin, kişisel verilerinin düzeltilmesi için veri sorumlusuna başvurması durumunda, veri sorumlusu kendi kayıt ortamındaki kişisel verileri düzeltmenin yanı sıra, bu kişisel verilerin paylaşıldığı üçüncü kişiler varsa onlar nezdinde de kişisel verileri düzeltmekle yükümlüdür⁸⁴. Ancak bazı durumlarda bu talebi karşılamak veri sorumlusu açısından imkânsız veya aşırı çaba gerektiren bir durum teşkil edebilir. GDPR m.19'da bu konuyla ilgili bir düzenleme yapmış ve düzeltme talebinin, bu talebin imkânsız

⁸² CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.91., DÜLGER, s.486., GÖÇMEN UYARER, s.146., GÜRSES, s.87., BOZKURT, s.219., ÇAVUŞOĞLU/YILMAZ, s.98., DOĞAN, s.69., KÜZECİ, s.254.

⁸³ KAMA IŞIK, s.271., ÖZKAN, s.155.

⁸⁴ DÜLGER, s.486.

olmaması veya aşırı bir çabayı gerektirmemesi kaydıyla veri sorumlusu tarafından yerine getirilebileceği belirtilmiştir⁸⁵. Türk hukukunda ise bu yönde bir düzenleme bulunmamaktadır.

2.5.6 İtiraz Hakkı

İlgili kişi, kişisel verilerinin işlenmesine, kendisi ile ilgili özel durumlara ve gerekçelere dayanarak herhangi bir zamanda itiraz etme hakkına sahiptir⁸⁶. İtiraz hakkı GDPR m.21 ile ayrı bir hak olarak düzenlenmişken, 6698 sayılı Kanun'da sadece m.11/g ile işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı tanınmıştır⁸⁷. Yani Türk hukukunda GDPR'daki gibi ayrı ve geniş bir hak olarak değil sadece otomatik sistemler vasıtasıyla analiz edilen sonuçlara itiraz hakkı tanınmıştır. Örneğin bir bankaya ilgili kişinin yaptığı kredi başvurusu tamamen otomatik sistemler vasıtasıyla analiz edilerek bir red cevabı verilirse, ilgili kişi bu red cevabına 6698 sayılı Kanun m.11/g kapsamında itiraz edebilecektir.

Türk hukukunda itiraz hakkını tam olarak karşılamasa da, Kişisel Verileri Koruma Kurulu'nun kararları ve rehberleri ile de açıkça vurgulandığı üzere ilgili kişilerin kişisel verilerinin bir işleme şartı olarak Kanun'un 5. maddesindeki işleme şartlarından açık rızaya dayanılarak işlenmesi durumunda, ilgili kişilerin bu açık rızalarını her zaman ve herhangi bir koşula tabi olmadan geri almalarının mümkün olması aslında kanaatimizce işlemenin durdurulması ve bütünüyle işlemeye itiraz etme anlamını da taşımaktadır. Ancak açık rıza dışındaki işleme şartları için bunu söylemek mümkün değildir.

⁸⁵ DÜLGER, s.487.

⁸⁶ CASSANO/COLAROCCHO/GALLUS/MICOZZI, s.102., DÜLGER, s.487., BOZKURT, s.228., DOĞAN, s.69.

⁸⁷ KAMA IŞIK, s.273., ÇAVUŞOĞLU – YILMAZ, s.99., ÖZKAN, s.157.,

Türk hukukunda bu konu çok az eserde ele alınmış ancak bu ele almalarda da konu sadece doğrudan pazarlamaya yönelik izinler kapsamında değerlendirilmiştir. Buna göre bu itiraz hakkı, kişisel verilerin doğrudan pazarlama için işlendiği durumlarda mutlak⁸⁸. Fakat bu görüş zaten kısıtlı olan itiraz hakkını daha da kısıtlayan ve sadece doğrudan pazarlama ile ilgili olarak verilen açık rızaların geri alınmasına hasreden bir görüştür. Hatta görüşün bu şekilde ileri sürülmesi bu hakkı kişisel verilerin korunması alanından çıkarıp, elektronik ticari ileti alanına sokmaktadır. Bu görüşün bu şekilde kabul edilmesi, bu hakkı pazarlama amacıyla verilen iletişim bilgilerine pazarlama yapılmasına dair açık rızanın geri çekilmesi ile sınırlı olan bir alana hapseder. Kişisel verilerin korunması ile ilgili yasal düzenlemelerin ve ilgili kişilere tanınan hakların doğasını ve bu düzenlemelerin ruhunu dikkate aldığımızda böyle kısıtlayıcı bir yoruma gitmenin ilgili kişinin Anayasal hakkının kısıtlanması anlamına geleceği kanaatindeyiz.

2.5.7 Kişisel Verilerin İmhasını Talep Etme Hakkı

Yukarıda da belirttiğimiz üzere Türk hukukunda ilgili kişiler 6698 sayılı Kanun'un 11/e maddesi kapsamında kişisel verilerinin silinmesini, yok edilmesini veya anonim hale getirilmesini isteyebilirler. Bu yöntemlerden hangisinin seçileceğini belirlemek ise veri sorumlularına bırakılmıştır. Bu husus Yönetmelik m.7/5'te "*veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer*" şeklinde düzenlenmiştir. Bu düzenleme ve tercihin veri sorumlusuna bırakılması çok önemlidir. Çünkü uygulamada veri sorumlusunun faaliyet alanı, stratejik hedefleri, iş gerekleri gibi çeşitli hususlar

⁸⁸ DÜLGER, s.487.

yönünden ilgili kişinin imha talebinin yerine getirilmesinin veri sorumlusu tarafından değerlendirilebilmesi gerekmektedir.

GDPR m.17’de silme hakkı ve parantez içinde kullanımla unutulma hakkı olarak düzenlenen, ancak bizim aşağıda unutulma hakkını ayrı bir hak olarak inceleyeceğimiz hak, kastettiğimiz kişisel verilerin imhası hakkını teşkil etmemektedir. Literatüre bakıldığında da konunun hem AB hukukunda hem de Türk hukukunda genellikle silme hakkı/unutulma hakkı şeklinde ele alındığı görülmektedir. AB hukuku için mevcut düzenleme nedeniyle konunun silme/unutulma hakkı gibi bir konu içinde ele alınması bir ölçüde makul görünse de Türk hukukunda da konunun hemen hemen bu kapsamda ele alınmış olması şaşırtıcıdır. Çünkü 6698 sayılı Kanun açık bir şekilde 7. maddesinde silme, yok etme ve anonim hale getirme şeklinde üç imha yöntemini düzenlemiş, bunun detaylarını ise 28.10.2017 tarih ve 30224 sayılı Resmi Gazete’de yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile düzenlemiştir⁸⁹. Ayrıca yol gösterici olması açısından da bu üç imha yönteminin ne şekilde uygulanacağına dair detaylı bir rehber yayınlamıştır. Şaşırtıcı olan bir diğer nokta ise, uygulamada uyum çalışmalarında imha konusunun en çok cevap aranan konulardan biri olması ve Kişisel Verileri Koruma Kurumu’nun da imha ile ilgili olarak verdiği birçok ceza kararının bulunmasına karşın doktrinin konuyu bu kapsamda ele almamasıdır. Tezin amacı kapsamında biz de geniş kapsamlı olarak konuyu ele almayacak olmakla beraber konunun can alıcı noktalarını bu başlık altında ele alacağız. Bu belirttiğimiz gerekçelerden dolayı bu hakkı, kişisel verilerin imhasını talep etme hakkı olarak belirledik.

⁸⁹ GÖÇMEN UYARER, s.147.

İmhayı talep etme hakkı kapsamında imha yöntemlerinin ne anlama geldiği yine Yönetmelik'te açıklanmıştır. Kişisel verilerin silinmesi Yönetmeliğin 8, yok edilmesi 9, anonim hale getirilmesi ise 10. madde ile açıklanmıştır. Bu düzenlemeye göre silme aslında kelimenin kendisinin çağrıştırdığı gibi bir silmeden ziyade kişisel verinin bu veriyi işleyenler tarafından erişilemez hale getirilmesidir. Bu bakımdan da “silme” tabiri terminolojik olarak aslında yapılmak istenen eylemi ifade edememektedir. Yok etme ise aslında silme derken insanların günlük hayatta kastettikleri eylemi ifade eder. Yani yok etme kişisel verinin yok edilmesi bu kişisel verinin herhangi bir yöntem kullanılarak dahi geri getirilememesi ve hiçbir şekilde ulaşılamamasını ifade eder. Anonim hale getirme ise çok daha teknik bir konu olup zaman zaman maskeleyme, şifreleme gibi diğer teknik konularla karıştırılmaktadır. Oysa anonimleştirme apayrı teknikler kullanılmasını gerektiren ve günümüz veri işleme kapasitesi nedeniyle anonimlik derecesinin kırılmasının daha kolay olduğu bu nedenle de dikkatle başvurulması gereken bir teknik yöntemdir. Bu yöntemde kısaca kişisel veri, barındırdığı çeşitli unsurlardan çeşitli tekniklerle arındırılarak kişisel veri olma niteliği kaybettirilmektedir. Yani bu verinin yanına artık başka herhangi bir veriyi koysanız dahi bir gerçek kişiye ulaşılabilecek bir veri elde edilemiyorsa o veri anonimleştirilmiş sayılacaktır.

Yönetmelikte bu husus, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak tanımlanmıştır. Bunun yöntemi ise m.10/2'de kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi olarak belirtilmiştir.

İşte ilgili kişi, veri sorumlusuna başvurarak kişisel verilerinin imhasını istediğinde veri sorumlusu, yukarıda kısaca açıkladığımız bu yöntemlerden biri ile, imha için yasal koşullar gerçekleşmiş ise başka bir deyişle işleme amacı artık ortadan kalkmış ve kişisel verinin imha edilmemesi için aksine bir yasal düzenleme yoksa veriyi imha edecektir. Örneğin bir varlık yönetim şirketine başvurarak kişisel verilerinin imhasını isteyen bir borçlu, borcunu ödemiş olmasına rağmen devam eden bir itirazın iptali ya da istirdat davası gibi bir dava varsa ve bu davalar kapsamında bu kişisel verilerin işlenmesi zorunlu ise o takdirde imha için sebepler ortadan kalkmamış olduğu için veri sorumlusu, ilgili kişinin imha talebini reddedebilir. Yasal olarak belli bir saklama süresi zorunluluğu var ise veri sorumlusu her halükârda ilgili kişinin yapmış olduğu imha talebini reddedecektir.

Kişisel verilerin imhası uygulamada en çok zorluk yaratan noktalardan biridir. Bu noktalardan ilki imha edilecek kişisel verinin hangi veriler olduğunun belirlenmesidir. Bu belirleme fizik ortamlarda ve arşivlerde bir kâğıt kayıt ortamında olan kişisel verilerin imhası ile ilgili ise, verilerin ayıklanarak kişisel verilerin çıkarılması, bu kişisel verilerin sınıflandırmasının yapılması, bunların saklama sürelerinin belirlenmesi ve saklama süreleri dolanların uygun bir yöntemle, örneğin sanayi tipi kağıt kıyma makineleri ile imha edilmesi gibi zorlu süreçler söz konusu olacaktır. Dijital ortamdaki kişisel verilerin imhası söz konusu ise durum daha da karmaşık bir hal almakta ve veri keşif yazılımları, etiketleme yazılımları gibi çeşitli yazılımların devreye alınmasını gerektirmektedir. Bu yazılımların da birbirleri ile konuşacak şekilde yapılandırılması gerekecektir ki böyle bir çaba hem ciddi miktarda para hem de kapsamlı yazılım projeleri anlamına gelmektedir.

2.5.8 Unutulma Hakkı

İnsanlık tarihinin görmediği bir hızla gelişen veri işleme kapasitesi ve TCP/IP protokolüne dayalı olarak geliştirilen internetin ve ilişkili teknolojilerin örneğin bulut

bilişim teknolojisinin gelişmesi ile çeşitli veri işleme sistemleri ve ortamlarında ve internette bir kez kayıt altına alınan bir verinin, sonsuza dek var olabileceği bir döneme girilmiş bulunmaktadır. Özellikle arama motorlarında ve sosyal ağlarda, bu arama motorlarının ve sosyal ağların robotları ve algoritmaları tarafından tespit edilip indekslenen bu veriler hem sonsuza kadar orada olmakta hem de arama sonuçlarında milyarlarca insana gösterilmektedir⁹⁰. Bu durumun ise kişisel veri mahremiyetinin özü ile ne büyük bir çatışma halinde olduğu izahtan uzaktır.

Kişisel verilerin bu denli yaygın ve sonsuz bir şekilde kullanımı ilgili kişilerin kişisel verileri üzerindeki hakimiyetlerini kaybetmelerine yol açmaktadır⁹¹. Bilgileri üzerinde hakimiyeti bulunmayan biri, uzun zaman önce yaşamış olduğu ve dijital hafızaya kaydedilmiş olan bir vakanın yükünü bugün geçmişe kıyasla çok daha ağır bir biçimde yüklenebilir⁹². Örneğin yıllar önce işlemediği bir suç yüzünden yargılanıp beraat eden birinin yıllar sonra milletvekili seçimi için aday olduğunda, seçmenlerin vekil adayları için yaptıkları internet araştırmalarında aslında beraat ettiği ama yüz kızartıcı bir suçlamanın konusu olan bir olay hakkında bilgi ediniyor olmaları, seçmende vekil adayı hakkında olumsuz görüşlerin oluşmasına sebebiyet verebilir. Mahkemelerin bir kişi hakkında beraat kararı verip o kişinin yaşamında beyaz bir sayfa açmış olmasına rağmen bu olaya ilişkin bilgilerin dijital hafızada kalması nedeniyle o kişinin hayatında fiiliyatta bir beyaz sayfa açılmıyor olabilir. İşte bu hak tam da bu noktada ilgili kişi ile veri sorumlusu arasındaki bozulan dengenin tekrar tesis edilmesini ve ilgili kişinin kendi kişisel verileri üzerindeki kontrolünü ve hakimiyetini arttırmasını amaçlamaktadır⁹³.

⁹⁰ KABADAYI, s.15.

⁹¹ TEPE, s.95.

⁹² KÜZECİ, s.256.

⁹³ KOTİL, s.144.

Unutulma hakkı, ilk kez AB tarafından gündeme getirilmiş ve daha sonra Adalet Divanı'nın verdiği 13.5.2014 tarihli Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzales v. Google Spain SL, Google Inc. davası⁹⁴ ile uygulamaya konulmuş olan bir haktır. Söz konusu dava, Google arama motorunda “Costeja Gonzales” ismindeki bir avukatın isminin aranması durumunda “La Vanguardia” isimli bir gazetenin internet sayfalarında avukatın ismine kamuya açık bir şekilde yer verilmesi ve sosyal güvenlik primlerinden dolayı meydana gelen borcuna ilişkin olarak yapılan haciz ile ilgili haberlerin kaldırılması ile ilgili olarak açılmış bir davadır. Bu davada Gonzalez isminin geçtiği sayfaların kaldırılmasını veya bu sayfalarda yapılacak değişiklik neticesinde kendisi ile alakalı verilerin kamuya ifşa edilmesinin önlenmesini talep etmiştir⁹⁵. Avrupa Komisyonu unutulma hakkını ele alırken, bu hakkın bireylere kendi kişisel verileri üzerinde kontrol hakkı ve yetkisi vermenin bir başka önemli yolu olduğunu, internetin sınırsız arama ve hafıza kapasitesine sahip olması nedeniyle, küçük bir kısmı dahi kamu ile paylaşılan kişisel verilerin uzun zaman geçmiş olsa da etkilerinin azalmadığını, unutulma hakkının AB vatandaşlarının çevrimiçi olarak kendi verilerini kontrol etmelerini sağlayacağını belirtmiştir⁹⁶.

AB Komisyonu tarafından bu hakka yer verilmesi istenirken, Avrupa Parlamentosu silme hakkı teriminin kullanılmasını istemiştir. Görüşmeler neticesinde AB Konseyi'nin de unutulma hakkı ifadesinin GDPR'da yer almasına onay vermesi üzerine GDPR'ın 17. maddesinin başlığı silme hakkı ve parantez içinde yazımla unutulma hakkı olarak yürürlüğe sokulmuştur⁹⁷.

⁹⁴ Gonzales v. Google Spain Kararının tam metni için bkz. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0131>, (e.t. 22.09.2023).

⁹⁵ KABADAYI, s.105.

⁹⁶ KABADAYI, s.52, KOTİL, s.143.

⁹⁷ DÜLGER, s.490., TEPE, s.97.

Türk hukukunda ise unutulma hakkı ayrı bir hak olarak düzenlenmemiştir. Bu tür farklılıkların oluşmasında elbette 6698 sayılı Kanun'un hazırlanmasında AB'nin 2018 yılında GDPR ile yürürlükten kaldırdığı 95/46/EC sayılı Yönerge'nin esas alınmış olmasının rolü büyüktür. 95/46 sayılı Yönerge'de böyle bir hak tanımlanmadığı için Türk hukukuna da şu ana kadar bu hak bir yasal düzenleme olarak girmemiştir⁹⁸.

Bu hak her ne kadar ağırlıklı olarak arama motorları ve sosyal medya ile ilgili olarak ele alınmışsa da çok kısa bir zamanda büyük ilerleme kaydeden yapay zekâ teknolojisi çerçevesinde de konunun mutlaka ve acil bir şekilde ele alınması gerekmektedir⁹⁹. Yapay zeka makine öğrenimi ve derin öğrenme gibi kavramları da içine alan şemsiye bir kavramdır¹⁰⁰. Gerçekten de kısa süre öncesine kadar mahremiyet açısından kimsenin düşünmediği bir boyut olan yapay zekâ, gösterdiği çok hızlı gelişme ile adeta ürkütücü bir boyuta gelmiş, bunun üzerine hem bu teknolojiyi geliştirenler tarafından teknolojinin geliştirilmesine bir fren konulmak istenmiş hem de yasa koyucular harekete geçmiştir. AB, "EU Artificial Intelligence Act – Avrupa Birliği Yapay Zeka Yasası" isminde bir yapay zekâ düzenlemesi yaparak tezin savunma tarihinden kısa bir süre önce yürürlüğe sokmuştur¹⁰¹. Bu düzenlemenin en çok önem verdiği konuların

⁹⁸ TEPE, s.98.

⁹⁹ KOTİL, s.146.

¹⁰⁰ Yapay zeka, makinelerin insanlar gibi algılama, öğrenme, problem çözme ve karar verme yeteneklerini taklit etmelerini sağlayan bir bilgisayar bilimi dalıdır. Makine öğrenmesi ve derin öğrenme, yapay zekanın alt dallarıdır ve bu alanlarda geliştirilmiş yöntemler ve algoritmalar, yapay zekanın işleyişini sağlar".Wikipedia. (2024), Yapay Zeka: https://tr.wikipedia.org/wiki/Yapay_zeka , (e.t. 27.05.2024)., Yapay zeka, bilgisayar sistemlerinin insan zekasını taklit ederek görevleri yerine getirmesi için tasarlanmış bir alandır. Makine öğrenmesi, yapay zekanın bir alt kümesidir ve sistemlerin veri ile öğrenmesini sağlar. Derin öğrenme ise, makine öğrenmesinin daha spesifik bir alt kümesidir ve büyük veri setleriyle çalışarak öğrenme sürecini derinleştirir", MIT Technology Review.(2024), Understanding AI, [https://www.technologyreview.com/\]\(https://www.technologyreview.com/](https://www.technologyreview.com/](https://www.technologyreview.com/) , (e.t. 27.05.2024)., Yapay zeka, bilgisayarların insan benzeri görevleri yerine getirebilmesi için gerekli olan teorileri ve geliştirmeleri kapsar. Makine öğrenmesi, bu sürecin bir parçasıdır ve verilerle öğrenme yeteneği sağlar. Derin öğrenme ise, makine öğrenmesinin bir uzantısı olarak daha karmaşık ve derin sinir ağlarını içerir, Stanford University.(2024), Artificial Intelligence, [https://ai.stanford.edu/\]\(https://ai.stanford.edu/](https://ai.stanford.edu/](https://ai.stanford.edu/) , (e.t. 27.05.2024)

¹⁰¹ AB Yapay Zeka Yasası'nın metnine <https://artificialintelligenceact.eu/the-act/> adresinden ulaşılabilir. (e.t. 27.05.2024)

başında da mahremiyet gelmektedir. Yapay zekanın eğitilmesinde kişisel verilerin kullanıldığı ve bu kullanımın arama motorları veya sosyal medyada olduğu gibi yapay zekanın da sonsuz hafızasına kazındığı bir gerçektir. Bu nedenle yapay zekâ alanında da unutulma hakkının çok hızlı bir şekilde hem yasa koyucular hem de yargı organları tarafından ele alınması gerektiği kanaatindeyiz.

Unutulma hakkının neyi kapsadığını belirlemek için bir tanımdan hareket edilmek istenirse bu hakkı, ilgili kişilerin dijital hafızada kayıt altına alınmış olunan fotoğrafları, kimlik bilgileri, görüntüleri, sesleri, adresleri gibi çok çeşitli kişisel verilerinin, talep edildiği zaman bir daha herhangi bir yöntem ve teknik kullanılarak geri getirilemeyecek şekilde ortadan kaldırılması olarak tanımlayabiliriz¹⁰². Böylece kişilere kendi kişisel verileri üzerindeki kontrolü yeniden tesis etme imkânı tanınmış olacaktır.

Ancak unutulma hakkı, yarışan haklar bakımından bazı ciddi soruları da beraberinde getirmektedir. Örneğin düşünceyi açıklama hürriyeti, kamunun bilgi edinme hakkı gibi temel haklar ile unutulma hakkının yarıştığı durumlarda nasıl hareket edileceği, buradaki yarışan haklar bakımından dengeleme gereksinimi, orantılılık ilkesinin ne şekilde uygulanacağı gibi bir çok konu gündeme gelecek ve yeni tartışma alanları açılacaktır¹⁰³. Diğer yandan yukarıda da belirttiğimiz gibi yapay zekâ gibi yepyeni, çılgır açan ama aynı zamanda yıkıcı bir niteliği olan teknolojiler karşısında bu hakkın ne şekilde konumlandırılacağı ve nasıl uygulanacağı da ayrı bir soru ve sorun olarak karşımıza çıkmaktadır.

¹⁰² YILMAZ, s.218., GÜREL/BULGURCU, s.36., NALDI, Maurizio/ITALIANO Giuseppe F. /RANNENBER, Kai/MEDINA, Manel /BOURKA, Athena (Eds.): “Privacy Technologies and Policy”, 7th Annual Privacy Forum (APF 2019), Rome/Italy June 13-14, s.15.

¹⁰³ KÜZECİ, s.260.

2.6 Akreditasyon, Sertifikasyon

2.6.1 Genel Olarak

TDK Sözlüğü'nde “akreditasyon” kavramı karşılığı “denklik” olarak, “sertifikasyon” kavramı karşılığı ise “onaylama” olarak belirtilmektedir. Ancak TDK Sözlüğündeki bu karşılıklar tez konumuz açısından pek bir açıklama veya ipucu vermemektedir. Bu nedenle akreditasyon ve sertifikasyonun günümüz ürün ve hizmetler dünyasındaki karşılığının araştırılması gerekmektedir.

Teknolojinin gelişimine paralel olarak ürünlerde ve hizmetlerde büyük bir çeşitlilik yaşanmıştır. Bu çeşitlilik ise ürünlerde ve hizmetlerde kalite, temel sağlık ve güvenlik gereklerine uyum, amaca uygunluk, çeşitli koşullar altında dayanım, hukuki düzenlemelere uyum gibi temel bazı beklentilerin karşılanması ve bu gereklerin karşılandığının güvence ve kayıt altına alınması ihtiyacını meydana getirmiştir.

Bu ihtiyacı karşılamak için, ürünlere, üretim süreçlerine, hizmetlere ve hizmet süreçlerine dair; muayene, denetim, test, analiz ve sertifikasyondan oluşan sertifikasyon sistemleri meydana getirilmiştir. Örneğin bir kuruluşun bilgi güvenliği standartlarını yerine getirip getirmediği ISO 27001 Bilgi Güvenliği Yönetim Standardına göre belirlenmektedir. Bilgi sistemlerini standard ile uyumlu hale getirdiğini ileri süren kuruluş bir sertifikasyon kuruluşunu çağırarak standart kapsamında kendisini denettirir, bu denetim neticesinde standartları karşıladığı tespit edilen kuruluşa ISO 27001 BGYS Sertifikasyonu verilir¹⁰⁴.

Ancak sertifikasyon kuruluşlarının bu yaptıkları sertifikasyon uygunluk değerlendirmesi faaliyetlerinin güvencesi nasıl sağlanacaktır? Başka bir deyişle bu

¹⁰⁴ ISO 27001 Bilgi Güvenliği Yönetim Sistemi için:
<https://www.tse.org.tr/IcerikDetay?ID=2311&ParentID=6890> , (e.t. 27.09.2022)

kuruluşların güvenilirliğinin güvencesi ne olacaktır? Ürünlerin, sistemlerin, hizmetlerin sertifikasyonunu yapan sertifikasyon kuruluşları, deney, analiz ve kalibrasyon laboratuvarları, asansör sektöründeki A Tipi muayene Kuruluşları gibi muayene kuruluşları, bu güvenilirlik sorusunu cevaplayabilmek ve yaptıkları sertifikasyonun geçerliliğini sağlayabilmek için yetkinliklerini ispat etmek zorundadırlar.

Sertifikasyon kuruluşlarının, ilgili oldukları alanlarda yetkin olduklarını denetlemek ve bunu tasdik ve tescil etmek için üst kuruluşlara gereksinim bulunmaktadır. Bu gerekliliği karşılamak için, bu kontrol görevini yapacak tarafsız ve bağımsız akreditasyon kuruluşlarına ihtiyaç duyulmaktadır. Akreditasyon kuruluşları sertifikasyon kuruluşlarını yetkinlikleri kapsamında akredite eder ve belirli aralıklarla da denetimini ve gözetimini icra ederler. Akreditasyon sisteminin temelinde, uluslararası kabul görmüş ölçütleri içeren standartlar yer almaktadır.

Sertifikasyon kuruluşları bu ölçütleri uygulamak ve karşılamak, akreditasyon kuruluşları ise sertifikasyon kuruluşlarının sertifikalandırma süreçlerinde standartlara, hukuki düzenlemelere ve akreditasyon şartlarına uyduklarını düzenli olarak denetlemekle yükümlüdür. Bu bakımdan da genel olarak akreditasyon kuruluşlarının faaliyetleri kamu faaliyeti olarak ortaya çıkmakta ve akreditasyon yetkilendirmeleri kamu yönetimi tarafından yapılmaktadır¹⁰⁵.

Bu açıklamalardan sonra sırasıyla akreditasyon ve sertifikasyon kavramlarının anlamlarına biraz daha yakından bakmak gerekmektedir.

¹⁰⁵ CEYLAN, Mehmet: Türkiye’de Kalite Akreditasyonu ve Türkak, Yüksek Lisans Tezi, Muğla Üniversitesi Sosyal Bilimler Enstitüsü, Muğla 2009, s.1.

2.6.2 Akreditasyon

Akreditasyon kavramı farklı alanlarda farklı anlamlarda kullanılabilmektedir. Akreditasyon, Latince “ad” ile “credere” kelimelerinden oluşmakta olup “birisine güvenmek” anlamına gelmektedir¹⁰⁶. Akreditasyon kelime anlamı olarak bir organizasyonun, önceden belirlenmiş standartlar yahut gereklilikler karşısındaki uyum durumunun bir akreditasyon kurumunca ele alınması ve inceleme yapıldıktan sonra şartları karşılıyorsa uyumunun tasdik edilmesi, kayıt altına alınmasını içeren süreçtir¹⁰⁷.

Diğer bir tanımla akreditasyon, kuruluşların ürün, kalite sistemleri veya personel belgelendirilmesi amacıyla, var olduğunu belirttikleri gerekli teknik kapasiteye haiz bulunup bulunmadıklarının sertifikasyon kuruluşları tarafından incelenmesi ve inceleme neticesinde uygun ise sertifikalandırılmasına dair olan faaliyeti yapacak sertifika kuruluşlarının yetkinliğinin tasdik edilmesidir¹⁰⁸.

Bu tanımlardan hareketle akreditasyon ihtiyacını ortaya çıkaran nedenleri şu şekilde tespit edebiliriz¹⁰⁹:

- Piyasaya arz edilen ürünlerin ve hizmetlerin bütün olarak standartlara ve hukuki düzenlemelere uygunluğunun tespiti,
- Ürünlerin ve hizmetlerin teknik bakımdan güvenliğinin ve kalitesinin standartlara uygunluğunun tespiti,
- Ürünlerde ve hizmetlerde standartlara ve hukuki düzenlemelere uygunluk noktasında akreditasyon yoluyla bir yeknesaklığın sağlanması,

¹⁰⁶ ARTUGAL, Seda Meltem: Mühendislik Eğitiminde Toplam Kalite Yönetimi ve Metalürji ve Malzeme Mühendisliği Bölümündeki ABET Uygulamaları, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul 2010, s.73.

¹⁰⁷ CEYLAN, s.11.

¹⁰⁸ ERKUŞ, Leyla: Eğitim Fakültelerinin Akreditasyon Sürecine Hazır Olma Durumuna İlişkin Öğretim Elemanlarının Görüşlerinin Değerlendirilmesi, Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale 2009, s.26.

¹⁰⁹ CEYLAN, s.19.

- Ticarete teknik engellerin kaldırılmasına dair Dünya Ticaret Örgütü düzenlemelerinin gereklerinin yerine getirilmesi.

Sertifikasyon kuruluşları, sertifikasyon yaparken, önceden tespit ettikleri sertifikasyon ölçütlerini uluslararası genel kabul görmüş standartlara göre belirlemektedirler. Böylece, sertifikasyonu almış olan ürünlerin yahut hizmetlerin, uluslararası genel kabul görmüş olan kalite standartlarını yakaladığı tescil ve ilan edilerek, bu ürünlerin ve hizmetlerin alıcısı konumundaki müşteriler bakımından güven telakki edilmektedir. Bu sertifikasyonu yapan kuruluşların ise bu yetkinliğe sahip oldukları genelde kamu yönetimi tarafında oluşturulan akreditasyon kuruluşlarınca tasdik edilerek tam bir güvence yaratılmaya çalışılır.

Bunun yanı sıra, akreditasyon, bu sahip olduğu uluslararası güven ve kabul edilebilirlik fonksiyonu sayesinde ticarete teknik engellerin kaldırılması yönünde de önemli katkıda bulunmaktadır¹¹⁰.

Başka bir deyişle akreditasyon, deney, test ve analiz laboratuvarları, muayene kuruluşları, yönetim sistemi sertifikasyon kuruluşları gibi uygunluk değerlendirme kuruluşlarının, icra ettikleri sertifikasyon faaliyetlerini yerine getirebilmek için gerekli yetkinliğe sahip olduklarını resmi biçimde ifade ederek gösteren, üçüncü taraf doğruluk beyanı sistemidir¹¹¹.

Akreditasyonun temelinde, uluslararası kabul gören kriterlerin tanımlandığı standartlar bulunmaktadır. Sertifikasyon kuruluşları bu kriterleri uygulamakla, akreditasyon kuruluşları ise uygulandığını düzenli olarak kontrol etmekle yükümlüdür.

¹¹⁰ SARP, Nilgün: Toplam Kalite Yönetimi Uygulamaları, Siyasal Kitabevi, Ankara 2014, s.88.

¹¹¹ CEYLAN, s.1.

Akreditasyonun temel fonksiyonu, kamu adına kabul edilebilecek kalite ve performans standartlarını saptaması açısından, kalite güvencesi olmasıdır¹¹².

Akreditasyon kuruluşları, sertifikasyon kuruluşlarını denetlemekte ve denetim neticesinde gereklilikleri karşılayanları akredite etmektedir. Sertifikasyon kuruluşlarının akreditasyonu, kuruluşun faaliyet alanı kapsamındaki yeterlilik ölçütlerini düzenleyen uluslararası standartlar, ilgili faaliyet alanına özgü gereklilikler, dünyada genel olarak kabul edilmiş ve bölgesel yahut uluslararası sair akreditasyon kuruluşlarınca çıkarılmış rehberlerde düzenlenen gereklilikler temelinde icra edilmektedir. Akreditasyon kuruluşlarının yetkinliği ve akreditasyon alt yapısının güvenilirliği ise Uluslararası Akreditasyon Forumu (IAF), Uluslararası Laboratuvar Akreditasyonu Birliği (ILAC) gibi uluslararası ve Avrupa Akreditasyon Birliği (EA) gibi bölgesel organizasyonlar ile gerçekleştirilen tanımayla dair çok taraflı anlaşmalar yoluyla sağlanmaktadır¹¹³.

Türkiye’de uygunluk değerlendirmesi faaliyetlerini akredite etmek için 4 Kasım 1999 tarihinde yayımlanan 4457 sayılı Kanunla Türk Akreditasyon Kurumu (TÜRKAK) kurulmuştur. TÜRKAK büyük önem taşıyan EA, ILAC ve IAF üyeliklerini tamamlamıştır¹¹⁴.

Kurumsal akreditasyon ve uzmanlık akreditasyonu olarak iki temel akreditasyon bulunmaktadır. Kurumsal akreditasyonda, akreditasyon kuruluşu, akreditasyonu yapılacak kuruluşu bir bütün olarak, misyonu ve akreditasyon kuruluşunun standartları ve ölçütleri bakımından ele alır. Bu değerlendirme yapılırken, kuruluşun ana hedeflerinin

¹¹² CEYLAN, s.11.

¹¹³ YÜKSEL, Birsen: Akreditasyon Süreçlerinde İş Zekası Uygulaması: Bir Kamu Kurumu Örneği, Yayınlanmış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara 2019, s.9.

¹¹⁴ CEYLAN, Özet.

yanısıra idari yapılanması ve idari yönetim tarzı, finansal durumu, kurumsal kaynakları, diğer kurum ve kuruluşlarla mevcut ilişkileri gibi tüm ölçütler birlikte değerlendirilir¹¹⁵.

Uzmanlık akreditasyonu ise belli bir bölüm, bir kurumdaki okul veya programlar için yapılır. Akredite edilen birim, bir üniversitenin bünyesindeki bir fakülte veya enstitü kadar büyük olabileceği gibi, belirli bir disiplinin içindeki bir eğitim programı kadar küçük de olabilir. Ancak, daha ziyade meslek programlarının incelenmesine dayanmaktadır. Bu sebeple daha çok öğrencilerin mesleki olarak hazırlanmalarını odak noktasına alır. Eğitim programının, lisans ve belgeleme de dahil, mesleğe girişteki ve mesleğin gereklerinin yerine getirilmesindeki profesyonel beklentileri ve gereklilikleri karşılayıp karşılamadığı uzmanlık akreditasyonunun odak noktasıdır¹¹⁶.

2.6.3 Sertifikasyon

Ürünün piyasaya arz edilmesinden önce ilgili teknik düzenlemesinde belirtilen ölçütleri karşılayıp karşılamadığının, başka bir söyleyiş ile teknik düzenlemelere uygun olarak üretilip üretilmediğinin deneylerinin, analizlerinin ve muayenesinin yapılması ve bu yapılanların neticesinin belgelenmesi faaliyeti uygunluk değerlendirmesi veya sertifikasyon olarak tanımlanmaktadır¹¹⁷.

Başka bir tanımla sertifikasyon; bir ürünün, sürecin, hizmetin, yönetim sisteminin, personelin ya da organizasyonun uluslararası standartlar, düzenlemeler, vb. ile belirlenen gereksinimleri yerine getirdiğini doğrulamak maksadıyla icra edilen faaliyetlerdir. Sertifikasyon sürecinde, belirlenmiş olan ölçütlere uygunluğu doğrulamak

¹¹⁵ ERKUŞ, s.37.

¹¹⁶ ERKUŞ, s.37.

¹¹⁷ CEYLAN, s.6.

maksadıyla, denetim, kalibrasyon, test, muayene gibi çeşitli faaliyetler icra edilmektedir¹¹⁸.

ISO ise sertifikasyonu bir ürünün, hizmetin veya kişinin belirli ve tanımlanmış bir gereklilikler setine uygun olduğunu gösteren bir beyan olarak tanımlamaktadır. Ancak bu tanım eleştirilmektedir. Buna göre ISO’nun bu tanıma uygunluğu göstermekte kullanılan süreç hakkında birşey söylememektedir. Tanımdaki bu eksikliğin giderilmesi için ise tanıma “uygunluk değerlendirmesi” ibaresinin eklenmesi gerektiği belirtilmektedir¹¹⁹.

Sertifikasyonu yapan kuruluşun, bu faaliyetine ilişkin ürün, hizmet veya süreçlerine ve sistemlerine göre üç çeşit sertifikasyon veya uygunluk değerlendirmesi yapılmaktadır¹²⁰. Bunlardan birinci taraf uygunluk değerlendirmesi, bir ürün ile ilgili olarak o ürünü üreten veya tedarik eden kişi veya kuruluşun yaptığı faaliyettir. İkincisi, ikinci taraf uygunluk değerlendirmesidir. Bir ürün ile ilgili olarak o ürünün kullanıcısının yaptığı faaliyettir. Üçüncü olarak ise üçüncü taraf sertifikasyonu gerçek anlamdaki sertifikasyondur, ürünle alakalı birinci ve ikinci tarafların dışında, bağımsız ve tarafsız olan kuruluşlarca icra edilen sertifikasyondur¹²¹.

¹¹⁸ ISO - ISO/IEC 17000:2004 - Conformity assessment — Vocabulary and general principles, <https://www.iso.org/standard/29316.html>, (e.t. 12.1.2024)

¹¹⁹ LACHAUD, Eric: “What GDPR Tells About Certification”, Computer Law&Security Review 38 (2020) 105457, s.3. , <https://www.sciencedirect.com/science/article/pii/S0267364920300625>, (e.t. 12.1.2024)

¹²⁰ YÜKSEL, s.7.

¹²¹ YÜKSEL, s.7., LACHAUD, s.3.

3. ANAYASAL BİR TEMEL HAK OLARAK KİŞİSEL VERİLERİN

KORUNMASI HAKKI

3.1 Genel Olarak Anayasa ve Anayasa Hukuku Kavramları

Anayasa bir devletin temel yapısını, kuruluşunu, iktidarın devrini ve devlet iktidarı karşısında bireylerin özgürlüklerini düzenleyen bir belgedir. Anayasanın, iç hukuk düzeninde ilk biçimsel kaynak olmasının bir özelliği de normlar hiyerarşisinde en üst sırada yer almasıdır¹²².

Hukuk düzeninin biçimsel kaynaklarının oluşumu, bağlayıcılığı ve kademelenmesi Hans Kelsen tarafından ortaya konulmuştur. Buna normativist teori denmektedir. Kelsen kurmuş olduğu “saf hukuk” teorisi ile pozitivistizmin bir temsilcisidir¹²³. Saf hukuk başlı başına pozitif hukukun kuramıdır. Belirli ulusal veya uluslar üstü hukuk normlarının yorumu değildir ve yalnızca inceleme konusunu, yani nesnesini bilmeyi amaçlar¹²⁴. Kelsen, hukuku norm haricindeki öğelerinden ayırtmış ve sınırlarını “norm” kavramı ile belirginleştirerek saf hukuk teorisini ortaya koymuştur. Norm ise parçası bulunduğu hiyerarşide sadece bir üzerinde bulunan norma aykırılık teşkil etmediği müddetçe geçerli olacaktır. Farklı seviyelerde kademelere yayılmış olan normlar, nihai durumda anayasallık denetimine tabi olmakla beraber, yasama ve yürütme güçlerinin meydana getirdiği yasa ve yasanın altı normlar olarak ortaya çıkarlar¹²⁵.

¹²² TEZİÇ, Erdoğan: Anayasa Hukuku, Tıpkı 25. Bası, Beta Yayınevi, İstanbul, 2021, s.10., GÖZLER, Kemal: Anayasa Hukukunun Genel Esasları, Ekin Yayınevi, Bursa, 2016, s.22., ATAY, Ender Ethem: Anayasa Hukuku, Turhan Kitabevi, Ankara, 2022, s.1., ÖZBUDUN, Ergun: Türk Anayasa Hukuku, Gözden Geçirilmiş 21. Baskı, Yetkin Yayınları, Ankara, 2021, s.37., KABOĞLU, İbrahim Ö.: Anayasa Hukuku Dersleri – Genel Esaslar, Güncellenmiş ve Sadeleştirilmiş 16. Baskı, Legal Yayınevi, İstanbul 2021, s.49.

¹²³ TEZİÇ, s.94.

¹²⁴ KAYA, Semih Batur: Avrupa İnsan Hakları Sözleşmesiyle Karşılaştırmalı Olarak Anayasal Hakların Hukuki Rejimi ve Yorumu, Seçkin Yayınevi, Ankara 2021, s.77.

¹²⁵ ŞİMŞEK AKTAŞ, Duygu: Bilişim Teknolojilerindeki Gelişmelerin Anayasal Fonksiyonlar Üzerindeki Dönüştürücü Etkisi, Oniki Levha Yayınları, İstanbul 2020, s.27.

Bu nedenle temel haklar ve özgürlüklerin güvence altına alındığı en üst hukuk normları Anayasa normlarıdır. Devletlerin, hiyerarşik normlar sistemini içeren hukuk düzenleri bulunmaktadır. Bu sistemde, hiyerarşinin en alt kısmında hukuku uygulayan yürütme organlarının oluşturduğu normlar bulunmaktadır. Bu normlar, kanun koyucu tarafından çıkarılan kanunlara dayanmaktadır. Pozitif normlar olarak değerlendirilen bu sıralama alt düzeydeki normun geçerliliğini bir üst sıradaki normdan alan, kademeli bir sistemi göstermektedir.

Dolayısıyla, anayasanın bu kademeli sistemde pozitif normlar arasında en üst düzeyde olduğu varsayılmaktadır. Normlar hiyerarşisinde en genel, en soyut normdan en özel, en bireysel ve en somut norma doğru bir sıralama izleyen bir geçiş bulunmaktadır¹²⁶. Bu anlamda anayasa kavramı devleti oluşturan yasayı ifade eder ve hukuk sisteminde başta kanunlar olmak üzere diğer bütün hukuki düzenlemelere dayanak teşkil eder¹²⁷. Bu bakımdan bir tanım yapılacak olursa anayasa, bir ülkede geçerli olan tüm siyasal kurumları kuran, hukuksal çerçevelerini oluşturan, onların tümüne temel ve dayanak oluşturan ve tüm bu kurum ve kuralların üzerinde yer alan belgeyi ya da kurallar bütünü ifade etmektedir¹²⁸.

Anayasa kavramını maddi anlamda anayasa ve şekli anlamda anayasa olarak ikiye ayırmak mümkündür. Maddi anlamda anayasa, belli bir devletin siyasi yapısı, iktidarın kullanılışı, yetkileri ve kişi özgürlükleri ile alakalı kuralların bütünüdür. Yine denilebilir ki, devletin yapısı, onun hükümet şekli, devlet organlarının yetkileri, kişi hakları ve özgürlükleri ile alakalı kurallar, maddi anlamda anayasanın içeriğini

¹²⁶ MANGIR, Demet Şefika: Uluslararası Toplumun Anayasası Jus Cogens, Nobel Yayınevi, Ankara 2015, s.11.

¹²⁷ ATAY, s.1.

¹²⁸ BATUM, Süheyl/YILMAZ, Didem/KÖYBAŞI, Serkan: Anayasa Hukuku Temel Kavramlar ve Genel Esaslar, Oniki Levha Yayınları, İstanbul 2021, s.21.

oluştururlar. Kısacası devlet iktidarı ve kişi haklarına dair olan kurallar, maddi anlamda anayasayı oluşturur. Anayasa diğer kanunlardan farklı usullere göre yapılır veya değiştirilir. Bu durumda ise anayasa içeriği ile değil şekli ile nitelendirilmektedir. Buna da şekli anlamda anayasa denilmektedir¹²⁹. İster yazılı isterse yazılı olmayan bir anayasanın her ülkede varlığı, zorunlu biçimde her ülkede maddi anlamda bir anayasanın mevcudiyetinin kabulü neticesini meydana getirir¹³⁰.

Anayasa hukuku ise yasama, yürütme ve yargı gibi devletin temel organlarının kuruluşunu, işleyişini ve bu organlar arasındaki karşılıklı ilişkileri ve devlet karşısındaki vatandaşların temel hak ve özgürlüklerini düzenleyen hukuk kurallarını inceleyen, hukuk biliminin içinde kamu hukuku dalı olarak tanımlanabilir¹³¹.

3.2 Temel Haklar ve Özgürlükler

Anayasalarda yer verilen en önemli konulardan biri de temel haklar ve özgürlüklerdir. Her anayasa bireylerin sahip olduğu temel hakları ve özgürlükleri anayasada sayıp tanımakta ve çoğunlukla da bunların korunması ve sınırlanması konusunda güvence veren bir sistem kurmaya çalışmaktadır¹³². Başka bir deyişle anayasalar, kişilerin temel hakları ve özgürlükleri ile devletin elinde bulundurduğu otoritesi arasındaki hassas dengeyi sağlayacak mekanizmaları, bu mekanizmaların tabi olacağı ilkeleri tespit eden belgelerdir¹³³. Temel haklar ve özgürlükler ise, anayasal güvenceye bağlanmış insan haklarıdır¹³⁴. Anayasanın güvenceye bağladığı bu temel haklar, içerdikleri sosyal bağlılıklar göz önüne alınarak değerlendirmeye tabi

¹²⁹ TEZİÇ, s.171., GÖZLER, s.49., KABOĞLU, s.10.

¹³⁰ ATAY, s.9.

¹³¹ GÖZLER, s.22., ATAY, s.4.

¹³² GÖZLER, s.66.

¹³³ ATAY, s.6.

¹³⁴ TANÖR, Bülent/YÜZBAŞIOĞLU, Necmi: 1982 Anayasasına Göre Türk Anayasa Hukuku, Güncelleştirilmiş 20. Bası, Beta Yayınevi, İstanbul 2020, s.143.

tutulmalıdır. Hukuk devleti ilkesinden gelen hürriyet kavramının toplumsal bağılılığı ve devletin sınırsız ve kamu yararını gözetmeyi ona karşı olan hürriyet kullanımını engellemesi yükümlülüğü ise bu mülâhazalar yapılırken gözlerden ırak tutulmamalıdır¹³⁵.

Genel olarak, temel haklar kavramı belirli bir hukuki düzenin özel bir statü verdiği hakları anlatmaktadır. Bu anlatımda belirtilen hukuki düzen ile anlatılmak istenen husus daha çok ulusal hukuki düzen olsa da mutlaka ulusal bir hukuki düzenin kastediliyor olması da şart değildir. Bu haklar, statüleri gereği genel olarak bir anayasal norm olarak tezahür etmektedirler. Anayasal normlar, bu hakları, kanun koyucuların kolay bir şekilde değiştirebilmesine yahut müdahalede bulunabilmesine imkân vermeyecek şekilde düzenleyerek koruma altına almaktadır¹³⁶.

Negatif yetki normları olarak temel haklar, devletin eylemlerini ve karar alma yetkisini sınırlandırmaktadır. Devletin görevi, temel hakları korumak olsa da devlet, her şeyden önce bu temel hakları somut hale getirmekle yükümlüdür ve aynı zamanda bu yükümlülüğünün yanı sıra temel hakları sınırlandırmakla da yetkilendirilebilir. Ancak, temel haklar ile garanti altına alınmış olunan kişisel hürriyet ve eşitlik statüsü bu sınırlandırma yetkisinin haricinde tutularak devlete karşı garanti altına alınmıştır¹³⁷.

Uluslararası hukuki metinlere bakıldığında ise temel haklar ifadesi daha az görülmektedir. BM Genel Kurulu'nca 1948'de kabul edilen İnsan Hakları Evrensel Beyannamesi temel hakları açık bir şekilde anmakla birlikte, listelenen ve insan hakları şeklinde nitelendirilen hakların yer aldığı hükümlere atıf yapılmamaktadır. Böyle bir atıf yapmak yerine, temel haklar kavramı, her bireyin anayasa ve yasalar tarafından

¹³⁵ GÖREN, Zafer: Temel Hak Genel Teorisi, Geliştirilmiş ve Gözden Geçirilmiş 5. Bası, Yetkin Yayınları, Ankara 2022, s.55.

¹³⁶ DOĞAN, s.132.

¹³⁷ GÖREN, s.64.

kendilerine tanınan haklar ihlal edildiği takdirde, ulusal iç hukuk yollarına müracaat etmek için bir hakka sahip olmasına atıf yapılarak kullanılmıştır¹³⁸.

AB’de ise Adalet Divanı, temel hakların teminat altına alınmasının zorunlu olduğunu ve AB hukukunun genel hukuk ilkelerinin bir parçası olduğu yönünde kararlar vermiştir. Bu kararlar 1969 tarihli Stauder kararı¹³⁹, 1970 tarihli Handelsgesellschaft kararı¹⁴⁰ ve 1974 tarihli Nold II¹⁴¹ kararlarıdır¹⁴².

Temel haklar ve özgürlüklerin neler olduğu ve bunların sınıflandırılması anayasa hukukunun en çok ilgilendiği konulardan biri olmuştur. Bu sınıflandırmalar içinde en bilineni ve kullanılanı Georg Jellinek’in¹⁴³ yaptığı sınıflandırmadır¹⁴⁴. Jellinek’in klasik ayırımına göre temel haklar ve özgürlükler, negatif statü hakları, pozitif statü hakları ve aktif statü hakları olmak üzere üç gruba ayrılırlar. Jellinek bu ayırımı, bireylerin devletten beklentileri ve devlet karşısındaki konumuna göre yapmıştır. Pozitif ve negatif statü hakları, devletin temel haklara ve özgürlüklere müdahil olup olmama durumuna göre tespit edilmekte iken, aktif statü hakları bunlardan farklı bir özellik göstermektedir¹⁴⁵. 1961 ve 1982 Anayasaları da Jellinek’in sınıflandırmasına benzer bir ayırımla temel hakları ve özgürlükleri düzenlemiştir¹⁴⁶.

¹³⁸ DOĞAN, s.133.

¹³⁹ Stauder kararının ingilizce tam metni için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61969CJ0029&from=EN> , (e.t. 16.10.2022).

¹⁴⁰ Handelsgesellschaft kararının ingilizce tam metni için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61970CJ0011&from=EN> , (e.t. 16.10.2022).

¹⁴¹ Nold II kararının ingilizce tam metni için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61973CJ0004&from=EN> , (e.t. 16.10.2022).

¹⁴² DOĞAN, s.136.

¹⁴³ Jellinek Avusturyalı kamu avukatıdır. Avusturya kamu hukukunun en önemli temsilcisi olarak görülmektedir. https://en.wikipedia.org/wiki/Georg_Jellinek, (e.t.14.10.2022).

¹⁴⁴ GÖZLER, s.411.

¹⁴⁵ KABOĞLU, s.265., KAMA IŞIK, s.25., GÖREN, s.49.

¹⁴⁶ KABOĞLU, s.265., DOĞAN, s.27.

Vatandaşların devletten bazı edimleri yerine getirmesini bekledikleri haklar, pozitif statü hakları olarak nitelendirilmektedir. Vatandaşların faydalanırken devletin müdahale edemeyeceği hak grubu da negatif statü hakları olarak adlandırılmaktadır¹⁴⁷.

Negatif statü hakları, kişilerin devletin dokunamayacağı¹⁴⁸ ve aşamayacağı özel alanının sınırlarını çizen¹⁴⁹ düşünce hürriyeti, din ve vicdan özgürlüğü, konut dokunulmazlığı gibi haklardır. Negatif statü hakları, devletin yaptığı müdahalelere karşı bireylere yargısal korunma hakkı veren haklardır¹⁵⁰. Negatif statü hakları, kişilerin devletin müdahalesi olmadan kişisel problemlerini halledebilmeleri, devlet müdahalesi olmadan içtimai yaşamlarını idame ettirebilmeleri için devlet müdahalesinden bağımsızlaşabildikleri haklar grubunu tanımlar¹⁵¹. Başka bir açıdan ele alınacak olursa negatif statü hakları, devletin pasif kaldığı haklardır. Bu haklar açısından önemli olan, devletin kişileri bu haklarını kullanabilmeleri için özgür kılması ve aynı zamanda bu hakların kullanılmasını kolaylaştırması ve garanti altına almasıdır¹⁵².

Pozitif statü haklarındaysa, eğitim, iyi bir çevrede yaşama, çalışma hürriyetinin garanti altına alınması gibi devletin pozitif bir hareketi ile yapmak zorunda olduğu haklar anlaşılmaktadır. Başka bir deyişle pozitif statü hakları, kişilerin devlet müdahalesi olmadan kullanımına erişemedikleri, bu manada hürriyetlerini sağlayamadıkları, bunlara kavuşulması için devletin alacağı tedbirlere ve tedariklere ihtiyaç duydukları hakları tanımlamaktadır. Vatandaşların devlet idaresine iştirak edebilmelerine imkân veren haklara ise aktif statü hakları denilmektedir. Bu hak türüne yurttaşlık

¹⁴⁷ KABOĞLU, s.265.

¹⁴⁸ DOĞAN, s.27.

¹⁴⁹ GÖZLER, s.411.

¹⁵⁰ KAMA IŞIK, s.25.

¹⁵¹ GÖREN, s.50.

¹⁵² DOĞAN, s.27.

hakları¹⁵³, vatandaşlık hakları ya da isteme hakları¹⁵⁴ da denilmektedir¹⁵⁵. Bu haklar, isteme hakkı, ortaklık ve dava hakları şeklinde temel haklar içinde tecelli etmekte ve devlet tarafından garanti edilmektedir¹⁵⁶. Seçme seçilme hakkı, kamu hizmetlerinde yer alabilme hakkı gibi haklar bu hak türüne örnek gösterilebilir.

Anayasanın bir parçası olarak temel haklar ve özgürlükler, yasalar ve yürütmenin düzenleyici işlemleri ile yürütme ve yargının müşahhas işlemlerine göre üst seviyedeki normlardır. Buna göre de anayasanın altındaki hukuki düzenlemelerin tümü ve ona dayanılarak gerçekleştirilen bütün işlemler anayasaya uygun olarak gerçekleştirilmelidir. Anayasanın bir parçası olan temel haklar ve özgürlükler ile ilgili normlarla anayasanın altındaki normlar bağdaşmadığı müddetçe, kural olarak bu alt normlar anayasaya aykırı ve geçers olacaktırlar¹⁵⁷.

Temel haklar ile ilgili bir diğer sınıflandırma ise Karel Vasak¹⁵⁸ tarafından yapılan tarihsel sınıflandırma¹⁵⁹ veya başka bir deyişle ortaya çıkış sıralarına göre yapılan sınıflandırmadır.

Birinci kuşak haklar tarihsel olarak ilk ortaya çıkan haklardır. Bu haklar birey güvenliği, konut dokunulmazlığı gibi birey haklarını ve seçme ve seçilme, siyasi faaliyette bulunma gibi siyasal hakları içerir¹⁶⁰. Bu haklar orta çağda sosyal bir sınıf olan burjuvazinin, aristokrasiye karşı vermiş olduğu mücadelenin birer ürünüdürler. 17. ve 18. yüzyılda dile getirilen ve Fransız Devrimi ile hayata geçen bu haklar liberal düşünceye dayanmaktadır. Bu düşünceye göre, bu hakları kullanabilmek için bireylerin özgür olması

¹⁵³ KABOĞLU, s.265.

¹⁵⁴ GÖZLER, s.412.

¹⁵⁵ GÖREN, s.50.

¹⁵⁶ GÖREN, s.50.

¹⁵⁷ GÖREN, s. 19.

¹⁵⁸ Vasak Çekoslovakya doğumlu Fransız hukukçudur. Strazburg'taki İnsan Hakları Enstitüsü'nün ilk genel sekreteridir. https://en.wikipedia.org/wiki/Karel_Vasak, (e.t. 14.10.2022).

¹⁵⁹ DOĞAN, s.22., GÖZLER, s.412., KAMA IŞIK, s.26.

¹⁶⁰ GÖZLER, s.412.

kafidir, devletin yapması gereken pasif kalmaktır¹⁶¹. Birinci kuşak hakların Fransız Devrimi'nden kaynaklanan çekiciliği, zaman içinde bu haklardan en çok burjuvazi kesiminin faydalanması ve yoksulluğun içindeki bireylerin ise bu haklardan faydalanamaması nedeniyle zayıflamıştır. Sanayi Devrimi'nin ortaya çıkması ile de bu çekiciliğini kaybetmiştir¹⁶².

Birinci kuşak olarak nitelenen haklar yukarıda da belirttiğimiz üzere devletin pasif bir tutum almasını gerektiren hak kategorileri ise de son zamanlarda kimi durumlarda devletin aktif olarak bir tutum almasının gerektiği hallerin de bulunduğu belirtilmektedir¹⁶³.

İkinci kuşak haklar, çalışma, dinlenme, emeklilik, sağlık gibi sosyal ve ekonomik haklardan oluşmaktadır. Bu haklar Birinci Dünya Savaşından sonra ortaya çıkmış ve İkinci Dünya Savaşından sonra da uygulamasına başlanmıştır¹⁶⁴.

Üçüncü kuşak haklar dayanışma hakları şeklinde de belirtilmektedir. Bu haklar, birey haklarının ön planda olduğu birinci ve ikinci kuşak haklarından bağımsız olarak yeni bir kategoridir. Bu kategoride, insan haklarının uluslararası, evrensel bir olgu olduğu, bu nedenle tüm insanlık için geçerli olan ortak bir koruma alanı olması gerektiği belirtilmektedir¹⁶⁵.

Ancak özellikle teknolojik gelişmeler başta olmak üzere meydana gelen çeşitli gelişmeler karşısında yukarıda aktarılan üçlü ayırım yetersiz gelmeye başlamıştır. Bu nedenle zaman ve nitelik yönünden, Vasak'ın üç kuşak ayırımının dışında yeni bir haklar kuşağı tanımlanması ihtiyacı doğmuştur. Böylece dördüncü kuşak haklar denilen yeni bir

¹⁶¹ DOĞAN, s.22.

¹⁶² KAMA IŞIK, s.27.

¹⁶³ KAMA IŞIK, s.27.

¹⁶⁴ GÖZLER, s.412.

¹⁶⁵ DOĞAN, s.25., GÖZLER, s.412., KAMA IŞIK, s.30.

hak kategorisi ortaya çıkmıştır¹⁶⁶. Dördüncü kuşak hakların, hangi haklardan oluştuğu net bir şekilde belirlenmiş olmamakla beraber, bu kategoride sayılan birtakım haklar bulunmaktadır. Bu haklardan biri de kişisel verilerin korunması hakkıdır¹⁶⁷. Kuşak teorisi kapsamında dördüncü kuşak haklardan sayılsın ya da sayılmasın kişisel verilerin korunması hakkının anayasal bir temel hak olduğu kanaatindeyiz. Bu nedenle devam eden kısımda bir anayasal temel hak olarak kişisel verilerin korunması hakkı ayrı bir başlık altında ele alınmıştır.

3.3 Temel Hak Olarak Kişisel Verilerin Korunması Hakkı

3.3.1 Kişisel Verilerin Korunması Hakkının Hukuki Niteliği

Kişisel verilerin korunması hakkının müstakil bir hak teşkil edip etmediği konusunda genel olarak iki görüş ileri sürülmektedir. İlk görüşe göre, kişisel verilerin korunması hakkı özel yaşamın mahremiyeti hakkının altında yer alır. Özel yaşamın mahremiyeti hakkının kendine has niteliklerini bulunduran bir şekli olarak kişisel verilerin korunması hakkı mahremiyet hakkının kapsamında değerlendirilmektedir.¹⁶⁸ Bu görüş kapsamında mahremiyet, kişisel verilerin korunması düşüncesinin kaynağı olarak ortaya çıkmaktadır. Mahremiyet Latince “privatus” sözcüğünden gelmektedir. Bu yönüyle mahremiyet kamusal olanın karşıtıdır. Dolayısıyla kapalı olan, erişilemeyen bir aile hayatını ve bir konut alanını da kapsamaktadır. Mahremiyetin mukayeseli anayasa hukuku alanında tanınır hale gelmesi ise, konut dokunulmazlığı, iletişimin gizli olması

¹⁶⁶ KAMA IŞIK, s.21., DOĞAN, s.38.

¹⁶⁷ DOĞAN, s.39.

¹⁶⁸ DÜLGER, s.81., YILMAZ, s.63., BASKIN, s.54., DENİZ, s.85., YILMAZ/ÇAVUŞOĞLU, s.62., TURAN, s.46., KÜZECİ, s.78., TEPE, s.45., BOZKURT, s.37., AYDIN, s.17., ÖZKAN, s.25., KAMA IŞIK, s.38., DOĞAN, s.85., SEVİMLİ, s.24.

gibi hususların gelişimini izleyen, geç denilebilecek bir gelişme olarak ortaya çıkmıştır. Ancak, tanınmasını müteakip artık bir üst hak olarak kabul edilmiştir¹⁶⁹.

Kişisel verileri korumaya dair hukuki düzenlemelerin temel saiki, kişilerin verilerinin hukuka aykırı biçimde toplanmasını, saklanmasını, işlenmesini ve kamuya ifşa edilmesini önlemektir. Bu amaçlar ise, mahremiyete koruma getirilmesinin temel saiki olan özel hayata hukuka aykırı müdahalelerin engellenmesine dair olan amaç ile aynıdır¹⁷⁰. Bu nedenle de kişisel verilerin korunması hakkı özel yaşam içerisinde mahremiyet hakkının korunması içinde yer almaktadır. Zaten bu niteliği ile de anayasal düzenlemeye konu olmuş ve anayasal korumadan faydalanmaya layık görülmüştür.

Özel hayatın gizliliği ve mahremiyet bağlamında değinilmesi gereken ve kişisel verilerin korunması hakkı bakımından önem arz eden bir diğer konu ise bireylerin kendi verilerinin geleceğini belirleme hakkıdır. Bu hak ile bireyin, kişisel verileri üzerinde bizzat ve münhasır olarak kendisinin yetkili olduğu ortaya konularak, kamu hukuku ve özel hukuk kapsamında temel bir hak olarak kabul edilmektedir¹⁷¹.

Dünyada henüz böyle bir hak kategorisini tanımlayan veya bundan söz eden bir hukuki düzenleme veya mahkeme kararı yok iken Federal Alman Anayasa Mahkemesi 1983 senesinde, ilk kez “*enformasyonel self determinasyon*” kavramını kullanmıştır¹⁷². Mahkeme’nin gerekçeli kararının kimi önemli bölümleri Alman düşünür Niklas Luhmann’ın yaptığı çalışmalara dayanmaktadır. Bu görüşe göre mahremiyetin rolü bireylerin bu bireyselliklerini tutarlı olarak garantiye almaktır. Çünkü, bireylerin özel yaşamlarının mahremiyeti, enformasyonel self determinasyon kapsamında bireylerin

¹⁶⁹ KAMA IŞIK, s.39., YILMAZ, s.64.

¹⁷⁰ KAMA IŞIK, s.55.

¹⁷¹ DOĞAN, s.211.

¹⁷² KÜZECİ, s.76., YILMAZ, s.162., DÜLGER, s.84., TEPE, s.50., DOĞRU, Derya: Avrupa İnsan Hakları Mahkemesi Yargılamasında Takdir Marjı Doktrini, Turhan Kitabevi, Ankara 2019, s.153.

sağlıkları, aile yaşamı gibi hassasiyete sahip verilerinin başkalarının eline geçmesini engelleyerek bireylerin özgür ve kendi kaderlerini belirleyebilecek yeterliliğe ulaşmalarını sağlamak bakımından önemli ve gereklidir¹⁷³. Ancak verilerin geleceğini belirleme hakkı, ilgili kişinin bizzatı kendisi verileri üzerinde sınırı olmayan biçimde hak sahibi olduğu olarak anlaşılmamalıdır. Bu hakkın da elbette sınırları vardır, fakat bu sınırlamaların koşulları ve kapsamı bireyler için net bir biçimde belirlenmelidir¹⁷⁴.

Bireylerin özel yaşamlarına ve aile yaşamlarına saygı gösterilmesini isteme hakkı bireysel bir olguya saygı duyulmasını isteme hakkını içermektedir. Bu hak, temelde diğer bireylerin özel yaşamlarına ve aile yaşamlarına müdahale edilmemesini gerektirir. Bir başka söyleyişle bu hak statik, negatif bir koruma içerir. Kişisel verilerin korunması hakkı ise verileri işleme metodlarının şartlarını belirler ve bu şartların yerine getirilmesi için de hukuki, idari ve teknik tedbirlerden oluşan bir tedbirler silsilesi öngörür. Yani aktif, dinamik bir koruma içerir. Bunun yanı sıra, kendine has bir mekanizması vardır, bu mekanizmanın başında da gözetim, denetim ve düzenleme ile yetkili ve sorumlu kişisel verileri koruma otoriteleri bulunmaktadır. Yani koruma, bireylerin mahkemelerde hakkını araması gibi bireylere değil, aktif olarak bir kuruma bırakılmıştır. Bu durumun ise şekillenmekte olan sosyal ve yasal güçlerin yeniden dağıtımına anlamına geldiği belirtilmektedir¹⁷⁵.

Ancak kişisel verilerin korunması hakkının özel hayatın gizliliği ve mahremiyet kavramları altında anayasal koruma bulması gerçeğini kabul etmekle birlikte, bu hakkın “sui generis” bir hak olduğu düşüncesindeyiz. Çünkü bu hakkın özellikle günümüzde

¹⁷³ YILMAZ, s.162.

¹⁷⁴ KÜZECİ, s.77.

¹⁷⁵ DÜLGER, s.83.

gelenen noktada, yapılan yasal düzenlemelerle birlikte tamamen kendine has, başka hiçbir yerde olmayan özellikleri bulunmaktadır.

Bu bakımdan “kişisel verilerin korunması” terminolojisinin de doğru olmadığını düşünüyoruz. Çünkü bir verinin korunmasından bahsedildiğinde o verinin bulunduğu yere dışarıdan bir saldırının yapılmaması, yapılsa bile o verinin elde edilememesi yahut içeriden yani o veriye erişim imkânı olmayan veya olmakla birlikte amacının dışında kullanamayacak olan içeriden olan birilerinin bu veriyi ele geçirip hukuka aykırı kullanması kastedilmektedir. Böyle olunca ise kişisel verilerin korunması daha sınırlı bir alana, tam deyimini ile “bilgi güvenliği” alanına sıkıştırılmaktadır. Oysa kişisel verinin mahremiyeti daha geniş bir kavramdır ve kendine özgü yapısı ve mekanizmaları vardır.

Konuyu birkaç örnekle daha net bir şekilde açıklamak gerekirse, bilgi güvenliği kişisel verinin korunmasına eşit değildir ama aynı zamanda kişisel verinin korunması da kişisel verinin mahremiyetine eşit değildir. Kişisel verinin korunması bilgi güvenliğinin bir alt kümesidir, kişisel verinin mahremiyeti ise “sui generis” bir kavramdır, ancak bilgi güvenliği ve kişisel verinin korunması ile paralel olan yönleri vardır. Kişisel verinin illa özel hayatın gizliliği içerisinde kalması gereken bir veri olması gerekli değildir. Örneğin bir pilotun uçuş esnasında maruz kaldığı radyasyonun otomatik olarak ölçülmesi neticesinde oluşturulan “pilot radyasyon maruziyet” değerlerini içeren bilgi havacılık sektörü düzenlemeleri gereği toplanması gereken bir bilgidir ve bu yönüyle özel hayata dair bir bilgi değildir, ama bir kişisel veridir, üstelik de sağlık verisi olduğu için özel nitelikli kişisel veridir.

Başka bir örnek vermek gerekirse, bir caddede nerede o iş koluna en uygun işyeri açılacağını belirleyebilmek için “sıcaklık haritası” denilen bir haritadan faydalanılmaktadır. Bu haritayı oluşturabilmek için, o caddede yukarı aşağı hareket eden

kalabalığın tekilleştirilmesi ve hareket desenlerinin çıkarılması gerekmektedir. Bunun için de cep telefonlarının MAC adresi denilen ve internete bağlanmak için gerekli bir donanım ögesi olan ethernet kartının üzerindeki bu MAC adreslerini okuyan bir sistem kurulmuş ise, bu sistemde kullanılan MAC adresi, üretici firmanın o ethernet kartına kodladığı ve üretici tarafından bilinen bir sayıdır ve klasik anlamda özel hayatın gizliliği kapsamında olabilecek bir veri değildir. Ancak neticede MAC adresinden yola çıkılarak bir gerçek kişiye erişilebileceği için bir kişisel veridir.

Bu verinin bir teknoloji yardımıyla caddeden gelip geçen insanların haberi ve izni olmadan toplanması ve sonra sıcaklık haritası için işlenmesi ile ilgili doğabilecek hukuki konuları, bu işlemin hukuka aykırı hale gelmemesi için yapılması gereken mahremiyet mühendisliği teknikleri gibi birçok konuyu özel hayatın gizliliği veya verinin korunması ile izah etmek mümkün değildir. Bu veriler hukuka aykırı olarak ele geçirildiğinde, bu durumun kamuoyuna ve ilgililerine duyurusuna dair izlenmesi gereken prosedürler, bir kişinin verilerinin işlenmesi ile ilgili yaptığı başvuruya cevap verirken izlenmesi gereken prosedürler, bir yazılım ya da donanım geliştirirken bilgisayar, elektrik veya elektronik mühendisliği dışında ayrıca mahremiyet mühendisliği gözü ile de kodlara veya donanım öğelerine müdahale edilmesi gerekliliği gibi çok sayıda ve kişisel veri mahremiyetine özgü düzenlemeler de yine özel hayatın gizliliği ile veya başka bir hak kategorisi ile izah edilemez. Nitekim bu gerçeği fark eden ISO dahi bilgi güvenliği standardı olan ISO 27001'den ayrı olarak mahremiyet yönetim standardı olan ISO 27701'i yayınlamıştır.

Ayrıca yine önemle belirtmemiz gerekir ki mahremiyet kavramı dahi tam olarak kişisel verilerin korunması hakkı kapsamında ele alındığında, özel hukuk veya anayasal olarak ele alındığındaki kavrama denk gelmemektedir. Örneğin bir bankada çok kıymetli bir ekran olan KRM (kredi risk merkezi) ekranına bir çalışanın erişim hakkı ve erişim

hakkının yanı sıra bu verileri işleme, silme, bir yerden bir yere gönderme gibi bir hakkı varsa, kendisine bu yetkiler tanımlanmış, görev tanımı ile de bu verileri ne şekilde kullanacağı, yetkilerinin neler olduğu tanımlanmışsa artık bu kişinin kişisel verinin mahremiyetini ihlal ettiğini söylemek, klasik “mahremiyet” söylemi içinde veya kişisel verinin korunması, özel hayatın gizliliğinin korunması gibi kavramlar içinde mümkün olmayacaktır. Kişi zaten yetkili olduğu KRM ekranı denilen ekrandaki tüm verileri görebilmekte, üzerlerinde çeşitli işlemler yapabilmektedir. Bilgi güvenliği veya veri koruma açısından bir sorun yoktur. Çünkü kişi hukuka aykırı yöntemlerle, bir erişim engelini aşp da o verilerin bulunduğu KRM ekranına erişmemektedir. O yetki kendisinde zaten vardır. Eriştiği alandaki banka müşterisine ait risk bilgilerine erişmesi özel hayatın gizliliği veya mahremiyet yönünden bir hukuka aykırılık da yaratmamaktadır. Çünkü o veriler bankanın risk değerlendirmesi yapabilmesi için BDDK düzenlemeleri kapsamında ve 6698 sayılı Kanun’un 5. maddesindeki meşru menfaat işleme şartı kapsamında hukuka uygun olarak işlenmektedir. Ancak buna rağmen mahremiyet düzenlemeleri kapsamında KRM ekranının bazı kullanım şekillerinin hukuka aykırı olduğu durumlar ortaya çıkmaktadır.

Nitekim Kişisel Verileri Koruma Kurulu’nun yayınladığı veri ihlal bildirimlerine bakıldığında bankaların tam da bu KRM ekranı ile ilgili olarak veri ihlal bildirimi yaptıkları görülmektedir. Bu veri ihlal bildirimlerinin temel nedeni ise o verinin amacının gerektirdiğinden fazla işlenmesidir, başka bir deyişle orantısız işlenmesidir.

Başka bir örnek vermek gerekirse bir kişi, kendisine hedefli reklamcılık yapılması için kişisel verilerinin toplanmasına ve bazı analitik süreçlere tabi tutularak kendisinin en çok görmek isteyeceği reklamların kendisine gösterilmesine dair açık rızasını vermiş olabilir. Ancak bu rızayı verdikten sonra işlenmesine izin verdiği kişisel verilerinin başka

verilerle zenginleştirilerek toplu bir halde işleme merkezleri yurtdışında bulunan DMP (veri yönetim platformları) denilen sistemlere gönderildiğini, burada segmentasyon denilen işleme tabi tutulduğunu, bu esnada hem zenginleştirme, hem segmentasyon hem de bunlardan anlamlı sonuçlar üretebilmek için iş zekası ekiplerinin makine öğrenimi ve yapay zeka temelli çalışan algoritmaları ile analitik süreçlere tabi tutulduğunu bilmiyorsa, yani ilgili kişi, veri sorumlusu tarafından tüm bu işleme yöntemleri ve süreçleri hakkında yeterli şekilde aydınlatılmamışsa o takdirde aydınlatma yükümlülüğüne aykırılık nedeniyle bir kişisel veri mahremiyeti ihlali meydana gelecektir.

Bu nedenle konunun bu derinlikte ele alınması, kişisel veri işlemede bugün bu kadar hukuki düzenleme yapılmasının, anayasal korunma tanınmasının gerçek sebebinin teknolojiadaki inanılmaz gelişme olduğunun her zaman göz önünde tutulması ve hukuki incelemelerin ve tartışmaların buna göre yapılması gerekmektedir. Konunun teknik boyutunu ve doğasını derinlemesine irdelemeden doğru hukuki tartışmaların yapılamayacağını ve doğru hukuki sonuçlara ulaşamayacağını düşünüyoruz.

Bütün bu nedenlerle kişisel verilerin korunması hakkı ne mülkiyet görüşündeki gibi ekonomik bir hak, ne fikri mülkiyet görüşündeki gibi bir fikri mülkiyet bahşeden bir hak, ne de tek başına mahremiyeti koruyan özel yaşamın gizliliğine ilişkin bir haktır. Bütün bunların dışında kendine özgü bir haktır¹⁷⁶. Önemine binaen de anayasa seviyesinde korunan bir haktır. Bu nedenle de kişisel verilerin korunması hakkına anayasal koruma payesi verilmesinin yerinde olduğunu düşünüyoruz.

Kaldı ki teknolojiadaki gelişmeler hız kesmeyecek, aksine artarak devam edecektir. Özellikle yarı iletken teknolojisinde şu anda kullanılan silisyum yerine, iletkenliği çok daha yüksek olan bir maddenin bulunması veya geliştirilmesi durumunda veri işleme

¹⁷⁶ YILMAZ, s.64.

kapasitesi hayal edilemeyecek derecede artacak ve kişisel verinin korunması, tamamen veri ekonomisine dayalı hale gelen bir global ekonomik sistemde en önemli konulardan biri haline gelecek ve bu nedenle de anayasal korumayı daha da fazla hak eden “sui generis” bir hak olarak tartışmasız bir biçimde temel haklar ve özgürlükler içinde yerini alacaktır.

3.3.2 Kişisel Verilerin Korunması Hakkının Anayasal Bir Hak Olma Niteliği

Kişisel veriler, özünde bir bireyin, insan olmasından kaynaklanan ve bir bireyi diğer bireylerden ayıran, onu tekilleştiren, birey olarak varlığını somutlaştıran veriler olduğu için aslında kuşak teorisi bakımından bakıldığında dördüncü kuşak hak olarak değil, insanlığın en başından veri var olan bir hak olarak da görülebilir. Tez kapsamında kuşak teorisine girilmeyecek olmakla birlikte, bu teorinin hakların çıkış sırasına göre değil, zaten var olan, insana içkin olan bu hakların sosyal, siyasal, ekonomik, kültürel ve teknolojik gelişmeler karşısında zuhur etmesi, görünür hale gelmesi ile alakalı olduğu düşüncesindeyiz.

Teknolojinin tarihi incelemesi, insanoğlunun sistemli bir şekilde bilgiyi üretme ve bu ürettiği bilgiden anlamlı ve tutarlı neticeler çıkarma ve bu elde ettiği neticeleri diğerlerine aktarabilme çabasını gösterdiği son beş bin yıllık dört dönemde yapılmaktadır. Elektriğin 19. yüzyıl başlarında keşfedilmesi ve bu keşfin üzerinde yeni teknolojilerin geliştirilmesinin öncesindeki “mekanik öncesi dönem (M.Ö. 3000 – 1450)”, bu dönemi takip eden “mekanik dönem (1450 – 1840). İnsanoğlunun bu ikinci aşamaya varması 4850 sene sürmüş iken, elektrik ile mekaniği birleştirerek geliştirdiği “elektro – mekanik dönem (1840 – 1940)” yalnız bir yüz yıl almıştır. 1940’a gelindiğinde ise sofistike

işlemleri becerebilen, tonlarca ağırlıktaki ilk bilgisayar geliştirilmiş ve günümüze kadar süren “elektronik dönem” başlamıştır¹⁷⁷.

Gerçekten de kişisel verilerin korunmasının bir anayasal hak düzeyinde tanınmasına neden olan gelişme veri işleme kapasitesinin gelişimini sağlayan ve özellikle İkinci Dünya Savaşı’ndan sonra yaşanan teknolojik gelişmelerdir. Bunlardan en önemlileri ise “lambalı” elektronik cihazlardan “transistörlü” elektronik cihazlara geçiş, ya da başka bir deyişle transistör devrimidir¹⁷⁸. Diğeri ise bugün halen kullandığımız internetin altyapısının geliştirilmiş olmasıdır¹⁷⁹. İnternetin altyapısından kastımız ise TCP/IP protokolü denilen protokoldür¹⁸⁰. Protokol, iletişimin ne şekilde yapılacağını belirleyen ve önceden belirlenmiş olan kurallar dizisidir¹⁸¹.

Bu yapı ile veri paketleri akıllı bir şekilde iletmeye başlanırken, transistörler sayesinde geliştirilmeye başlanan entegre devreler ile de işlem yapma gücü artmış ve taşınan ve işlenen veri paketlerindeki inanılmaz artış ile insanlık veri işlemede bambaşka bir seviyeye atlamıştır. Bu denli güçlü veri işleme ile birlikte de daha önce hiç olmadığı kadar insanların mahremiyeti tehdit altına girmiştir.

Özellikle web 1.0¹⁸² döneminden web 2.0¹⁸³ dönemine geçilmesiyle birlikte, yani statik internet sitelerinde ürün veya hizmet teşhirinden, karşılıklı etkileşime dayanan ve üzerinde ödeme sistemlerinin kurulabildiği döneme geçildikten sonra, tarihsel olarak

¹⁷⁷ ŞİMŞEK AKTAŞ, s. 1-2.

¹⁷⁸ Transistörlerin keşfi ve gelişimi için: https://ethw.org/Transistors_and_the_Computer_Revolution, (e.t. 16.10.2022).

¹⁷⁹ İnternetin ilk düşüncesi ve geliştirilmesi ARPA projesi isimli bir askeri araştırma projesinde Bilgi İşleme Teknikleri Ofisi Direktörü olan Joseph Carl Robnett Licklider’in 1963 yılında çalışma arkadaşlarına gönderdiği bir memoranduma dayanmaktadır. Memorandumun İngilizce metni <https://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network> adresinde yer almaktadır. (e.t. 16.10.2022).

¹⁸⁰ ÇÖLKESEN, Rifat: Network TCP/IP UNIX El Kitabı, Papatya Yayıncılık, İstanbul 2000, s.11.

¹⁸¹ ÇÖLKESEN, s.17, Dip not 1.

¹⁸² Web 1.0 için: https://en.wikipedia.org/wiki/Category:Web_1.0, (e.t. 16.10.2022).

¹⁸³ Web 2.0 için: https://en.wikipedia.org/wiki/Web_2.0, (e.t. 16.10.2022).

2000’li yıllardan sonraki dönemde, arama motorlarının¹⁸⁴ da gelişmesiyle birlikte insanların davranış biçimleri izlenebilmeye başlanmış ve çeşitli teknik yöntemlerle çeşitli kişisel veriler toplanıp bu veriler işlenerek hedefli reklamcılık dönemi başlamıştır¹⁸⁵. Kişisel veri işlemenin boyutu o noktalara gelmiştir ki, İngiltere’nin AB’den ayrılması için yapılan BREXIT oylaması ile Donald Trump’ın ABD seçimlerinde başkan seçilmesi ile ilgili olarak Cambridge Analytica isimli bir firmanın yaptığı kişisel veri işleme çalışmaları ile bu oylamalarda insanların tercihlerinin etkilendiği iddiası ortaya atılmış daha sonra da bu iddialar soruşturmaya ve davalara dönüşmüştür. Bu denli yoğun bir işleme ile insanların tercihlerinin ve hatta iradelerinin etkilenmesi, mahremiyetin yanı sıra özgür iradenin dahi tartışılmasına neden olmuştur¹⁸⁶.

Kişisel verilerin korunması hakkı, öncelikle kamu makamlarınca kişisel verilerin bir sınıra tabi olmadan toplanması, saklanması ve işlenmesi karşısında, bireylerin temel haklarının ve özgürlüklerinin anayasal düzlemde temel bir hak olarak garanti edilmesini içermektedir. Bu hakkın temel amacı, demokratik bir toplum düzeninde yaşayan bireylerin ve kendi kişisel verileri üzerinde sahip oldukları hakların korunmasıdır¹⁸⁷.

Anayasa Mahkemesi’nin 6475 sayılı Posta Hizmetleri Kanunu’nun bazı maddelerinin iptali ile ilgili açılan iptal davasında da belirttiği gibi, kişisel verilerin korunması hakkı, bireylerin insan onurunun korunması ve kişiliklerinin hür bir biçimde

¹⁸⁴ Arama motoru için: https://en.wikipedia.org/wiki/Search_engine, (e.t. 16.10.2022).

¹⁸⁵ Verilerin toplanıp işlendiği ve kategorize edildiği, profileme ve segmentasyon çalışmalarının yapıldığı sistemlere DMP (data management platform) denilmektedir. https://en.wikipedia.org/wiki/Data_management_platform, (e.t. 16.10.2022).

¹⁸⁶ Cambridge Analytica Skandalının detayı için https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal, (e.t.16.10.2022).

¹⁸⁷ YILMAZ, s.65-66.

geliştirilmesinin özel bir biçimi olarak, kişilerin haklarını ve özgürlüklerini kişisel verilerin işlenmesi sırasında korunmasını içermektedir¹⁸⁸.

Kişisel verilerin korunması hakkı anayasal bir hak olarak Türk hukukuna 2010 yılında Anayasa'nın 20. maddesine eklenen 3. fıkra ile girmiştir. Ancak anayasa değişikliğinden önce Türk hukukunda bu hakkın hiç korunmadığı söylenemez. Medeni Kanun'un kişilik haklarını koruyan hükümleri, Türk Ceza Kanunu'nun¹⁸⁹, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun bazı hükümleri gibi çeşitli yasal düzenlemeler kapsamında kişisel veriler bazen doğrudan, bazen de diğer hak kategorileri ile ilişki kurularak korunmaktaydı. Ancak Türk hukukunda açık bir şekilde kişilerin maddi ve manevi varlığını geliştirmeye yönelik anayasal bir hak olarak tanınması ancak 1982 Anayasasında yapılan değişiklik ile mümkün olmuştur.

1982 Anayasası'nın ilk metninde kişisel verilerin korunması ile alakalı doğrudan bir hüküm bulunmamaktaydı. Ancak açık bir düzenleme olmasa da konunun özel hayatın gizliliği ve mahremiyet bağlamında değerlendirilmesi ile Anayasa'nın bazı maddeleri ile ilişkilendirilerek kişisel verilere hukuki bir koruma verilmekteydi. Çünkü kişisel verilerin korunması hakkı başta özel hayatın gizliliği ve mahremiyet olmak üzere, hukuk devletinin bir gereği olarak bireylerin maddi ve manevi varlıklarının korunması, insan onuru gibi haklarla doğrudan ilintilidir. Bu ilintili olma durumu nedeniyle de 1982 Anayasası'ndaki değişiklikten önce dahi Anayasa'nın 2., 17. ve 20. maddelerinin kişisel verilerin korunması için yasal dayanak teşkil ettiği belirtilmektedir¹⁹⁰.

¹⁸⁸ Anayasa Mahkemesi'nin 2013/84 E., 2014/183 K. sayılı ve 4.12.2014 tarihli kararı: <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-183-nrm.pdf>, (e.t.19.10.2022).

¹⁸⁹ Türkiye'de kişisel verilerin korunmasının tarihçesi için bkz. TOPALOĞLU, s.179.

¹⁹⁰ DOĞAN, s.87.

Kişisel Verileri Koruma Kurulu’nun yayınladığı “Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı” isimli rehberde de bu durum; “*Anayasanın 20. maddesinin 3. fıkrasında kişisel verilerin korunması öngörülmektedir. Ayrıca kişisel verilerin hukuka aykırı olarak işlenmesi, Anayasanın 17. maddesi ile güvence altına alınan kişi dokunulmazlığı, kişinin 5 maddi ve manevi varlığını koruma ve geliştirme hakkı ile Anayasanın 20. ve 22. maddelerinde düzenlenen özel hayatın gizliliği ve korunması hakkının ihlali anlamına da gelmektedir.*” denilmek suretiyle belirtilmiştir¹⁹¹.

Anayasada yapılan değişikliğin gerekçesinde, Anayasada kişisel verilerin korunması ile alakalı dolaylı düzenlemeler olmakla beraber koruma için yeterli düzeyde bulunmadığı, karşılaştırmalı hukukta ve Türkiye’nin taraf olduğu uluslararası sözleşmelerde kişisel verilerin korunmasının öneminin vurgulandığı, bu nedenle de bu madde ile herkesin kendisi ile alakalı kişisel verilerin korunmasını talep etmek hakkının anayasal bir hak olarak güvenceye alındığı belirtilmiştir¹⁹². Bu şekilde kişisel verilerin korunması hakkı, özel hayatın gizliliği başlığı altında temel bir hak olarak anayasal teminata kavuşturulmuştur.

Kişisel verilerin korunması hakkı anayasal teminata kavuşturulunca, Anayasa Mahkemesi’ne bireysel başvuru yolu da açılmış ve böylece bu hakkın anayasal bir hak olarak düzenlenmesi, bireylerin uğradıklarını düşündükleri hak ihlallerine karşı başvuru yapabilmeleri ile de günlük yaşamda pratik karşılığını bulmuştur¹⁹³.

Kişisel verilerin korunması hakkının kapsamı Anayasa Mahkemesi’nin çeşitli kararları ile doldurulmaktadır. Bu kararlardan en önemlilerinden biri Danıştay İdari Dava

¹⁹¹ Kişisel Verileri Koruma Kurumu: Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı Rehberi, <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/11931dc2-233d-45b0-892c-5debcc9bc9a1.pdf>, (e.t. 19.10.2022).

¹⁹² DÜLGER, s.110.

¹⁹³ DÜLGER, s.138.

Daireleri Kurulu'nun 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin Anayasanın 2, 7, 13 ve 20. maddelerine aykırı olduğu gerekçesiyle iptali için Anayasa Mahkemesi'ne yaptığı başvuru neticesinde verdiği karardır. Bu kararda hem kişisel verilerin tanımı ve kapsamı ile ilgili değerlendirmeler yapılmış hem de kişisel verilerin korunması hakkının kapsamı ve anayasal bir hak olarak korunmasının sebepleri açıklanmıştır. Kararda şu ifadeler kullanılmıştır¹⁹⁴:

“Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör

¹⁹⁴ Anayasa Mahkemesi'nin 2013/122 E., 2014/74 K. Sayılı ve 9.4.2014 tarihli kararı: <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf>, (e.t. 19.10.2022)

unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfî müdahalelerine karşı koruma altına alınmıştır."

Dikkat edileceği üzere Anayasa Mahkemesi öncelikle kişisel veri kavramını ele almıştır. Yukarıda MAC adresi örneğinde veya pilotların radyasyon maruziyet oranı örneğinde olduğu gibi kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişi ile ilgili tüm veriler olduğu örnekler de verilerek bir kez daha vurgulanmıştır. Bu tanımın içeriğinin bu kadar geniş olduğunun vurgulanması çok önemlidir. Çünkü ısrarla belirttiğimiz üzere bu hakkın bir anayasal hak olarak kabul edilmesinde teknolojinin önemi çok büyüktür ve teknoloji geliştikçe bugün aklımıza gelmeyen çok çeşitli veriler de kişisel veri olarak ortaya çıkacak ve kişisel verilerin korunması hakkının koruma kapsamı daha da genişleyecektir. Bu durum ise yine ısrarla belirttiğimiz üzere bu hakkın "sui generis" bir hak olma niteliğini ve bu nedenle de ayrı bir hak kategorisi olarak ele alınması gerekliliğini daha da güçlendirecektir.

Anayasa Mahkemesi tanımın içeriğini bu şekilde doldurduktan sonra bu kez de temel bir anayasal hak olmasının içini daha da doldurmakta ve kişisel verilerin korunması hakkının doğrudan insan onuru ile ilişkili olduğunu ve bireyin kendi kişiliğini geliştirebilme hakkının özel bir görünüm biçimi olduğunu vurgulamaktadır. Ayrıca yukarıda da vurguladığımız teknolojik gelişme vurgusunu Anayasa Mahkemesi de

yapmakta ve teknolojik gelişmeler nedeniyle kişisel verilerin korunmasının en üst seviyede yapılmasının zorunlu olduğuna vurgu yapmaktadır.

Anayasa Mahkemesi'nin son yaptığı “kamu makamlarının keyfi müdahalelerine karşı anayasal bir koruma” sağlanmış olması vurgusu da tezimizin ana fikri açısından çok önemlidir. Çünkü ileride ele alacağımız hukuki güvenlik ilkesi aynı zamanda idarenin keyfi eylemlerine karşı gerçek ve tüzel kişilerin korunmasını da içermektedir. Anayasa Mahkemesi yaptığı bu vurgu ile aynı zamanda Anayasadan kaynaklanan hukuki güvenlik ilkesine de atıf yapmış olmaktadır. Hukuki güvenlik ilkesinin bu anayasal niteliği ve akreditasyon sertifikasyon sistemleri ile ilişkisi ilerleyen kısımlarda ele alınacaktır.

Ülkemize doğrudan etkisi olan uluslararası alandaki düzenlemelerden ise özellikle AİHS’de kişisel verilerin korunması hakkı ayrı bir hak olarak yer almamış olsa da AİHM kişisel verilerin korunması hakkını AİHS’nin 8. maddesi kapsamında özel hayata ve aile hayatına saygı hakkı içinde değerlendirmiş ve çeşitli ihlal kararları ile de bu hakkı koruma altına almıştır¹⁹⁵. Bu kapsamda AİHM, özel hayatın gizliliği ile ilgili verdiği kararlarda kabul ettiği gibi, kişisel verilerin korunması ile ilgili olarak da devletin hem negatif hem de pozitif yükümlülüklerinin bulunduğunu belirterek devletlerin kişisel verilerin korunması hakkına yönelik keyfi müdahaleler yapmalarını AİHS’nin 8. maddesinin ihlali olarak kabul etmiştir¹⁹⁶.

Negatif ve pozitif yükümlülükler yönünden AİHM’nin yaptığı denetim; ana olarak Avrupa Konseyi üyesi devletlerin yapmış oldukları veri işleme faaliyetlerinin, AİHS m.8’e uygunluğuna ilişkin negatif yükümlülüklerin denetlenmesi ve üye

¹⁹⁵ DOĞAN, s.86., DÜLGER, s.83.

¹⁹⁶ YILMAZ, s.178., TEPE, s.135., KAMA IŞIK, s.84.

devletlerin kendi hükümlerlik alanlarında üçüncü kişilerin yaptıkları veri işleme faaliyetlerindeki pozitif yükümlülüklerin denetimi şeklinde işlemektedir¹⁹⁷.

En genel anlamı ile bireylere, kişiliklerine bağlı bütün verileri üzerinde tasarruf etme imkânı veren kişisel verilerin korunması hakkı, bireylerin özel yaşamlarının korunması demektir. Bu nedenle de kişisel verilerin korunması hakkının temelinde aynen özel yaşamın korunmasındaki gibi insan onuru, bireysel özerklik ve kişilik hakları bulunmaktadır¹⁹⁸.

AİHS m.8’de özel yaşam, aile yaşamı, konut dokunulmazlığı ve iletişim olmak üzere dört koruma alanı düzenlenmiştir. Özel yaşamın korunması bu koruma alanları içinde en kapsamlı olanıdır¹⁹⁹. Ancak özel yaşamın mahremiyeti mutlak bir hak olmayıp, kamu makamlarınca maddede belirtilen maksatlarla sınırlandırılabilir. Bu çerçevede AİHM bu sınırlandırmalar ile alakalı olarak kanunilik, meşru amaç ve yapılan sınırlandırmanın demokratik bir toplumun gereği olup olmadığını değerlendirmektedir²⁰⁰.

AİHM, kişisel verilerin korunması hakkına dair başvuruları 8. madde kapsamında ele alırken genel olarak Avrupa Konseyi’nin 1981 tarihli ve 108 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Konvansiyon”u esas almaktadır. Çünkü, 108 sayılı Konvansiyon, günümüzde kişisel verilerin korunmasında bağlayıcı nitelik taşıyan tek uluslararası düzenlemedir²⁰¹.

AİHS kapsamında 8. madde AİHM tarafından en geniş biçimde yorumlanmakta olan maddelerdendir. Birbirinden farklı çeşitli konular 8. madde içinde değerlendirilebilmektedir. AİHM 8. madde ile ilgili verdiği çeşitli kararlarında genişletici

¹⁹⁷ TEPE, s.140.

¹⁹⁸ YILMAZ, s.81.

¹⁹⁹ DOĞAN, s.91., YILMAZ, s.180.

²⁰⁰ YILMAZ, s.180., DÜLGER, s.93.

²⁰¹ DOĞRU, s.153.

bir yöntem takip etmiştir²⁰². Bu kapsamda AİHM, özel yaşam kapsamında hem bireyler arasındaki ilişkileri hem de özel alan ile kamusal alanda kişisel verilerle ilgili meydana gelen çeşitli durumları ele almaktadır. AİHM'nin bu genişletici yorumu neticesinde de veriye erişme hakkı gibi bazı hakların kabul edilmesi temel olarak yukarıda ele aldığımız devletin pozitif yükümlülükleri sayesinde mümkün olabilmektedir.

Bu pozitif yükümlülükler temelinde de devletler, özel sektördeki veri sorumlularının veya veri işleyenlerin meydana getirdikleri kişisel veri ihlallerinden dolayı mahkemece sorumlu tutulabilmişlerdir²⁰³. Gerek negatif yükümlülükler gerekse pozitif yükümlülükler açısından çok önemli olan bir husus ise, kişisel verilerin korunması hakkının tam olarak bireylere sağlanabildiğinden bahsedebilmek için, bireylerin etkili başvuru yapabilmeleri ve bu başvuru ile ilgili gerekli altyapının oluşturulmuş olması gerekliliğidir. Böylece bireyler, kişisel verilerinin hukuka aykırı olarak işlenmesi ile ilgili gerek devletin gerekse üçüncü kişilerin keyfi müdahalelerine karşı korunabilecektir²⁰⁴.

Bu etkin başvuru ve bunun altyapısının oluşturulması da tez boyunca dile getirdiğimiz bir mekanizmanın kurulmuş olması ile alakalıdır. Bir başka deyişle, kişisel veriler ilgili bölümlerde de açıkladığımız gibi çeşitli yasal düzenlemelerle hukuki güvence altına alınmıştır, ancak burada öngörülen tek yol, bu hakka bir saldırı olduktan sonra devreye giren mahkemelerde dava açma yoluyla hakkını koruma yoludur. Oysa kişisel verilerle ilgili hukuki düzenlemelerde de görüldüğü üzere haklar henüz saldırıya uğramadan, örneğin veri işlemeden önce aydınlatma yükümlülüğünün yerine getirilmesi, verinin işlendiği herhangi bir anda bireylerin kişisel verilerinin hangi amaçla, hangi metotlarla işlendiğini, kimlerle paylaşıldığını sorabilme hakkı gibi çeşitli haklarını

²⁰² DÜLGER, s.120.

²⁰³ KAMA IŞIK, m.86.

²⁰⁴ DOĞAN, s.92.

kullanabilecekleri bir hukuki, teknik ve idari mekanizma oluřturulmakta ve bu mekanizma da kapsamlı bir organizasyon řemasına sahip olan kiřisel verileri koruma kurumlarınca yönetilmektedir.



4. KİŞİSEL VERİLERİN KORUNMASINDA AKREDİTASYON VE SERTİFİKASYON

4.1 Genel Olarak

Yukarıda ele alındığı üzere akreditasyon ve sertifikasyon daha çok ürünler, hizmetler, süreçler ve sistemler için işletilmektedir. Ancak bu anlamdaki akreditasyon ve sertifikasyon kişisel verilerin korunması alanında kastettiğimiz akreditasyon ve sertifikasyona dair sadece genel bir çerçeve vermektedir. Bu genel çerçevenin içinin kişisel verileri koruma hukuku düzenlemelerine ve uygulamalarına göre doldurulması ve özelleştirilmesi gerekmektedir.

Kişisel verilerin korunmasında geniş kapsamda uygulanan sertifikasyon süreci ISO'nun 27000 ailesinden yayınladığı ISO 27701 Veri Mahremiyeti Yönetimi standardıdır. Ancak konumuz ISO standartlarını doğrudan kapsamadığı için burada ISO 27701 ele alınmayacaktır.

Bu nedenle tezin ana odak noktasını GDPR'nın 42. ve 43. maddeleri ile düzenlenen akreditasyon ve sertifikasyon sistemi oluşturacaktır. AB tarafında bu maddelerin hayata geçirilmesine dair çalışmalar yapılmış, halihazırda konuyla ilgili bazı rehberler, görüşler ve raporlar yayınlanmış ve nihayetinde sistem EUROPRIVACY adı ile hayata geçirilmiştir. EUROPRIVACY sistemi aşağıda ayrı bir başlık altında incelenmiştir. Ayrıca çeşitli ülkeler de kendi içlerinde bazı çalışmalar yapmaktadır. Lüksemburg GDPR kapsamında sertifikasyon mekanizmasını hayata geçiren ilk ülke olmuştur. Ayrıca İngiltere'de ICO, Fransa'da CNIL, İrlanda'da DPC, Polonya'da Kişisel Verileri Koruma Otoritesi akreditasyon ve sertifikasyon hazırlıklarını sürdürmektedir²⁰⁵.

²⁰⁵ LACHAUD, s.3.

4.2 GDPR m.42 ve 43. Kapsamında Akreditasyon ve Sertifikasyon

GDPR, AB’de veri koruması için günün koşullarına ve teknolojik gelişmelere uygun, hesap verebilirlik ve şeffaflık temelinde temel haklar ve özgürlüklerden olan kişisel verilerin korunması hakkı için bir yasal çerçeve sağlamıştır. GDPR kapsamında veri sorumlularının ve veri işleyenlerin uyumunu kolaylaştırma amacını güden bir dizi önlem, bu yeni çerçevenin merkezinde yer almaktadır. Bunlar, belirli şartlar gerçekleşmiş ise veri koruma görevlilerinin atanması, veri koruma etki analizlerinin yapılması ile akreditasyon ve sertifikasyon sistemi gibi düzenlemelerdir.

GDPR’ın yürürlüğe girmesinden önce, 29. Madde Çalışma Grubu (WP29) olarak adlandırılan çalışma grubu, sertifikasyonun veri korumaya yönelik hesap verebilirlik çerçevesinde önemli bir rol oynayabileceğini tespit etmiş bulunmaktaydı²⁰⁶.

WP29’un çalışmaları ve sonrasında da GDPR m.42 ve 43 ile kişisel verilerin korunmasında akreditasyon ve sertifikasyon konusunda düzenlemeler getirilmiştir. Aşağıda önce 42 ve 43. maddeler ele alınacak, ardından bu düzenlemelerin detayları ile ilgili değerlendirmeler yapılarak, EDPB’nin yayınladığı rehberler de göz önüne alınarak konu derinlemesine ele alınacaktır.

4.2.1 GDPR 42. Madde Düzenlemeleri

GDPR 42 ve 43. maddeleri ile GDPR’ın uygulama alanında bir akreditasyon ve sertifikasyon düzenlemesi getirilmiştir. GDPR m.42/3 bu sertifikasyonun gönüllü olacağını ve şeffaf bir süreç ile yürütüleceğini düzenlemektedir. Buradan hareketle, sertifikasyon sisteminin veri sahiplerinin, verilerini işleyen veri sorumluları ve veri işleyenlerin verilerin işlenmesinde gerekli ve yeterli tedbirleri alıp almadıklarını kontrol

²⁰⁶ 29. Madde Çalışma Grubunun Sertifikasyon hakkındaki görüşü için: https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877 , (e.t. 8.2.2024).

edebilecekleri, bu sayede de şeffaflaşmanın sağlanacağı ve aynı zamanda GDPR'ın ana ilkelerinden olan hesap verebilirlik kriterinin de yerine getirilmiş olacağı belirtilmektedir²⁰⁷.

GDPR m.42'de veri sorumluları ve veri işleyenlerin veri işleme süreçlerinin GDPR ile uyumlu olduğunu gösterebilmeleri bakımından mahremiyet mühürleri ve işaretlerini de içine alan sertifikasyon mekanizmalarının teşvik edildiği belirtilmektedir. Dolayısıyla burada ilk tespit edilen husus bir önceki bölümde ele alınan akreditasyon ve sertifikasyondan farklı olarak burada bir ürün ya da hizmetin değil GDPR düzenlemelerine uyum düzeyinin sertifikasyona konu olduğudur.

Bir de yine dikkat edilirse mahremiyet işaretleri ve mahremiyet mühürlerinden bahsedilmektedir. 95/46 sayılı Yönerge döneminde AB'de özellikle bir yazılımın, bir internet sitesinin veya mobil uygulamanın kişisel veri koruma düzenlemelerine uygun olup olmadığına ilişkin uygulaması olan mahremiyet işaretleri ve mahremiyet mühürleri sisteminin GDPR'da da devam ettirileceği açıkça düzenleme altına alınmıştır. Sertifikalandırmada mikro, küçük ve orta boy işletmeler için ise spesifik ihtiyaçların gözetileceği ayrıca vurgulanmıştır. Çünkü bu işletmelerin GDPR'ın gerektirdiği teknik, hukuki ve idari tedbirleri tam anlamıyla yerine getirebilmesi, bunlara bütçe ayırabilmesi çok mümkün görülmediği için AB çapında veri koruma otoriteleri bu işletmelere özgü düzenlemeler çıkarmakta, bu işletmelerin uyumunu kolaylaştırabilecek rehberler ve araçlar hazırlamakta ve bunları ücretsiz olarak bu işletmelere sunmaktadırlar²⁰⁸.

²⁰⁷ Ireland Data Protection Commision: Guidance Note: GDPR Certification, September 2020, s.2, https://dataprotection.ie/sites/default/files/uploads/2020-09/GDPR%20Certification%20Guidance_0.pdf, (e.t. 8.2.2024).

²⁰⁸ Ücretsiz yayınlanan rehberlere örnek için bkz. İngiliz Veri Koruma Otoritesi ICO uygulamaları, <https://ico.org.uk/for-organisations/sme-web-hub/>, (e.t. 22.10.2022).

GDPR m.42/4 ile tezin ana konusunu oluşturan konulara çok yakından değinen bir düzenlemeye yer verilmiştir. Maddeye göre, bir veri sorumlusu veya veri işleyenin sertifikalandırılmış olması, onun GDPR kapsamındaki sorumluluklarının azaldığı veya veri koruma otoritelerinin görevlerine ve yetkilerine halel geldiği anlamına gelmez. Dolayısıyla sertifikasyonun anayasal hukuki güvenlik ilkesi kapsamında sayılması durumunda temel bir hak olarak kişisel verilerin korunması hakkı ile çatışması durumunda, konunun tartıştığımız teorik içeriğinden bağımsız olarak, pratikte ne yapılacağına dair aslında GDPR ile bir düzenleme yapılmış olmaktadır.

Bu konu çok önemlidir. Zira özellikle AB'nin “yeni yaklaşım yönergeleri”²⁰⁹ adını verdiği sisteme geçerek, zorunlu standartlar yerine, bir ürünün piyasaya arzından evvel temel sağlık ve güvenlik gereklerinin karşılayıp karşılamadığının tespit edilmesi, bu tespitin ise “onaylanmış kuruluşlar” denilen, bu incelemeleri ve tespitleri yapmak için akredite edilmiş olan sertifikasyon kuruluşları tarafından yapılması ve ürünlerin piyasaya arzı sonrasında ise bir piyasa gözetimi ve denetimi (PGD) sistemi kurulması düzenleme altına alınmış ve hayata geçirilmiştir.

Bu sistem kurulduktan sonra ise örneğin asansör sektöründeki yeşil/mavi/sarı/kırmızı etiket uygulamasında olduğu gibi, bu etiketleri veren muayene kuruluşlarının, yeşil etiket vermiş olmasına rağmen ölümlü kaza meydana gelmesinde bu muayene kuruluşlarının veya bunları akredite eden kuruluşun sorumluluğu söz konusu olabilir²¹⁰. Bu yaşanan durumun aynısı, kişisel verilerle ilgili kurulacak bir akreditasyon

²⁰⁹ AB'nin Yeni Yaklaşım Yönergeleri hakkında detaylı bilgi için bkz. <https://sesei.eu/european-standardization/new-approach-legislation/>, (e.t. 22.10.2022).

²¹⁰ A Tipi Muayene Kuruluşlarının asansörleri periyodik kontrole tabi tutmalarında bir hatalarının olması durumunda sorumlu olup olmayacaklarına dair Asansör Periyodik Kontrol Yönetmeliği'nde doğrudan bir hüküm bulunmamaktadır. Yönetmelik kapsamında muayene kuruluşları sadece muayeneyi icra ederken verdikleri zarardan sorumlu tutulmaktadırlar. Ancak Yönetmeliğin 7. maddesi ile yönetmeliğe aykırı hareket eden muayene kuruluşuna bakanlık tarafından idari tedbirler uygulanacağı hükme bağlanmıştır. Yine Yönetmeliğin 37. maddesi ile Yönetmeliğe aykırı hareket eden muayene kuruluşuna idari para cezası verileceği veya yetkisinin geri alınabileceği düzenlenmiştir. Uygulamada, asansör kazalarından veya idari

ve sertifikasyon sisteminde de meydana gelebileceği için GDPR bu tür durumların önüne en baştan geçebilmek için böyle bir hükmü sevk etmiştir.

Tabii bu hükmün, akreditasyon ve sertifikasyon kuruluşlarının sorumlulukları iddiasıyla yargı önüne götürülmesinden daha derin olan ve dikkatli bir incelemeyi gerektiren kısmı, yukarıda da kısaca değindiğimiz veri sahibi gerçek kişilerin anayasalardan kaynaklanan kişisel verilerinin korunması ile ilgili haklarına bu tür mekanizmalar aracılığıyla hanel getirilip getirilemeyeceği, bir sınırlamanın söz konusu olup olamayacağı; veri sorumlularının ve veri işleyenlerin hukuki güvenlik ilkesini gerekçe göstererek gerek veri sahibi gerçek kişilerin taleplerine, ceza ve tazminat davalarına gerekse de veri koruma otoriteleri başta olmak üzere yetkili kurum, kuruluş, yargı organı gibi otoritelerin yaptırımlarına, eylem ve işlemlerine karşı bir güvenli liman oluşturup oluşturamayacakları kısmıdır.

GDPR m.42/5 hükmü uyarınca sertifikasyon sadece 43. maddeye göre yetkilendirilmiş sertifikasyon kuruluşları veya ilgili ülkelerin veri koruma otoriteleri²¹¹ tarafından ve ilgili ülke veri koruma otoritesinin veya EDPB'nin belirleyeceği kriterlere uygun olarak yapılabilir. Eğer EDPB tarafından kriterler onaylanırsa bu durum “Avrupa Veri Koruma Mührü” olarak ortak bir sertifikasyon ile sonuçlanabilir²¹².

GDPR m.42/6 uyarınca, veri sorumluları veya veri işleyenler, sertifikasyon mekanizmasına sertifikalandırılmak için başvuru yaptıklarında, bu kişisel veri işleme faaliyetlerinin izlenebilmesi ve sertifikasyon sürecinin yürütülebilmesi için tüm kişisel veri işleme süreçleri hakkındaki bilgiyi ve gerekli erişimi sertifikasyon kuruluşlarına veya

para cezalarından doğan davalarda muayene kuruluşlarına da davanın ihbar edildiği belirtilmekle beraber bu konuda verilmiş bir karar tarafımızca elde edilememiştir.

²¹¹ VOIGT, Paul/BUSSCHE von dem, Axel: The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer International Publishing, Switzerland 2017, s. 189.

²¹² CAREY, Peter/DEIGHTON, Alison: Enforcement and the Role of the Regulator, Oxford University Press, Oxford 2018, s.162.

ilgili ülkenin veri koruma otoritesine vermekle yükümlüdürler. Yani şeffaf bir şekilde ilgili kişisel veri işleme süreçlerinin tümünü bu otoritelere veya kuruluşlara açmaları gerekir ki ileride sertifikaya hak kazanılabilsin ve şeffaflık ilkesinin karşılandığı söylenebilsin.

GDPR m.42/7 uyarınca bir veri sorumlusu veya veri işleyen, bu süre zarfında tüm kriterleri karşılamaya devam etmek kaydıyla, azami üç yıl için sertifikalandırılabilir. Üçüncü yılın sonunda yenileme sürecine gidilmesi ve tekrar sertifikalandırılmaya hak kazanıp kazanmadığının tespit edilmesi gerekir. Aksi takdirde, yani artık gerekliliklerin karşılanmadığının tespit edilmesi durumunda sertifikasyon geri çekilir.

Nihayet GDPR m.42/8 ile EDPB'nin AB'de mevcut tüm sertifikasyon, mahremiyet mührü ve mahremiyet işaretlerini bir kayıta toplayacağı ve bunlara kamuoyunun erişimine açacağı düzenlenmiştir. Bunun neticesinde de EUROPRIVACY sistemi kurulup hayata geçirilmiştir.

4.2.2 GDPR 43. Madde Düzenlemeleri, Sertifikasyon Kuruluşları ve Akredite Edilmeleri

GDPR m.42²¹³ ile sertifikasyon mekanizmasına dair ilkeler düzenlenmiş, 43.

²¹³ GDPR m.42: (1) Üye devletler, denetim makamları, Kurul ve Komisyon, kontrolörler ve işleyiciler tarafından gerçekleştirilen işleme faaliyetlerinin bu Tüzük'le uyumluluğunun gösterilmesi amacıyla, özellikle Birlik düzeyinde, veri koruma sertifikasyon mekanizmaları ve veri koruma mühürleri ve işaretlerinin oluşturulmasını teşvik eder. Mikro, küçük ve orta ölçekli işletmelerin spesifik ihtiyaçları dikkate alınır. (2) Bu Tüzük'e tabi kontrolörler veya işleyicilerin uygun hareket etmesine ek olarak, bu maddenin 5. paragrafı uyarınca onaylanan veri koruma sertifikasyon mekanizmaları, mühürler ya da işaretler 46(2) maddesinin (f) bendinde atıfta bulunulan koşullar uyarınca üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları çerçevesinde 3. madde uyarınca bu Tüzük'e tabi olmayan kontroller veya işleyiciler tarafından sağlanan uygun güvencelerin var olduğunun gösterilmesi amacıyla oluşturulabilir. Söz konusu kontrolörler veya işleyiciler, veri sahiplerinin hakları ile ilgili olanlar da dahil olmak üzere uygun güvenceleri uygulamak üzere sözleşmeye bağlı veya diğer bağlayıcı belgeler vasıtasıyla bağlayıcı ve uygulanabilir taahhütlerde bulunur. (3) Sertifikasyon gönüllülük esasına dayanır ve şeffaf bir süreç vasıtasıyla sağlanır. (4) Bu madde uyarınca sağlanan bir sertifikasyon kontrolör ya da işleyicinin bu Tüzük'e uyma sorumluluğunu azaltmaz ve bu sertifikasyon ile 55 veya 56. madde uyarınca yetkin olan denetim makamlarının görevleri ve yetkilerine halel gelmez. (5) Bu madde uyarınca sağlanan bir

Madde²¹⁴ ile ise sertifikasyon kuruluşları düzenleme altına alınmıştır. Aşağıda madde

sertifikasyon 43. maddede atıfta bulunulan sertifikasyon organları veya yetkin denetim makamı tarafından 58(3) madde uyarınca söz konusu yetkin denetim makamı veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere dayalı olarak sağlanır. Kriterlerin Kurul tarafından onaylandığı hallerde, ortak bir sertifikasyon olan Avrupa Veri Koruma Mührü verilebilir. (6) İşleme faaliyetlerini sertifikasyon mekanizmasına sunan kontrolör veya işleyici sertifikasyon usulünün gerçekleştirilmesi için gereken tüm bilgiler ve işleme faaliyetlerine erişimi 43. maddede atıfta bulunulan sertifikasyon organına veya uygun olduğu hallerde, yetkin denetim makamına sağlar. (7) Sertifikasyon bir kontrolör veya işleyiciye azami üç yıllık bir süre için sağlanır ve ilgili gerekliliklerin yerine getirilmesine devam edilmesi koşuluyla, aynı koşullar altında, yenilenebilir. Sertifikasyon gerekliliklerinin yerine getirilmediği veya artık yerine getirilmediği hallerde, sertifikasyon uygun olduğu hallerde, 43. maddede atıfta bulunulan sertifikasyon organları veya yetkin denetim makamı tarafından geri çekilebilir. (8) Kurul tüm sertifikasyon mekanizmaları ve veri koruma mühürleri ile işaretlerini bir sicilde toplar ve uygun yollarla kamuoyuna açıklar.

²¹⁴ GDPR m.43: (1) Yetkin denetim makamının 57 ve 58. maddeler kapsamındaki görevleri ve yetkilerine halel gelmeksizin, veri koruma ile ilgili uygun bir uzmanlık seviyesine sahip olan sertifikasyon organları, gerekmesi halinde 58(2) maddesinin (h) bendi uyarınca yetkilerinin kullanılmasını sağlamak üzere denetim makamını bilgilendirdikten sonra, sertifikasyon sağlar ve sertifikasyonu yeniler. Üye devletler bu sertifikasyon organlarının aşağıdakilerin biri veya her ikisi tarafından akredite edilmesini sağlar:

- (a) 55 veya 56. maddeler uyarınca yetkin olan denetim makamı;
- (b) EN-ISO/IEC 17065/2012'ye uygun olarak (AT) 765/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü² uyarınca ve 55 ya da 56. madde uyarınca yetkin olan denetim makamı tarafından belirlenen ek gereklilikler uyarınca tayin edilen ulusal akreditasyon organı.
- (2)1. paragrafta atıfta bulunulan sertifikasyon organları, ancak aşağıdaki özellikleri taşımaları halinde, bu paragraf uyarınca akredite edilir:
 - (a) sertifikasyon konusuna ilişkin bağımsızlıkları ve uzmanlıklarını yetkin denetim makamını tatmin edecek şekilde göstermiş olmaları;
 - (b) 42(5) maddesinde atıfta bulunulan ve 55 veya 56. madde uyarınca yetkin olan denetim makamı tarafından veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere riayet etmeyi taahhüt etmiş olmaları;
 - (c) veri koruma sertifikasyonu, mühürleri ve işaretlerinin verilmesi, düzenli aralıklarla gözden geçirilmesi ve geri çekilmesine ilişkin usuller oluşturmuş olmaları;
 - (d) sertifikasyon veya sertifikasyonun bir kontrolör ya da işleyici tarafından uygulanmış olma veya uygulanma şekline ilişkin ihlallere yönelik şikayetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olmaları ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olmaları ve
 - (e) görev ve vazifelerinin bir çıkar çatışmasına neden olmadığını yetkin denetim makamını tatmin edecek şekilde göstermiş olmaları.

(3) Sertifikasyon organlarının bu maddenin 1 ve 2. bentlerinde atıfta bulunulan şekilde akreditasyonu 55 veya 56. madde uyarınca yetkin olan denetim makamı tarafından veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere dayalı olarak gerçekleşir. Bu maddenin 1. paragrafının (b) bendi uyarınca akreditasyon yapılması halinde, bu gereklilikler (AT) 765/2008 sayılı Tüzük'te öngörülen gereklilikleri ve sertifikasyon organlarının yöntemleri ve usullerinin açıklandığı teknik kuralları tamamlar. (4) 1. paragrafta atıfta bulunulan sertifikasyon organları, kontrolör veya işleyicinin bu Tüzük'e uyum sorumluluğuna halel gelmeksizin, sertifikasyonla sonuçlanan uygun bir değerlendirmeden veya söz konusu sertifikasyonun geri çekilmesinden sorumludur. Akreditasyon azami beş yıllık bir süre için verilir ve, sertifikasyon organının bu maddede ortaya konan gereklilikleri yerine getirmesi koşuluyla, aynı koşullar altında, yenilenebilir. (5) 1. paragrafta atıfta bulunulan sertifikasyon organları talep edilen sertifikasyonun verilmesi veya geri çekilmesine ilişkin sebepleri yetkin denetim makamına sağlar. (6) Bu maddenin 3. paragrafında atıfta bulunulan gereklilikler ve 42(5) maddesinde atıfta bulunulan kriterler denetim makamı tarafından kolayca erişilebilecek bir formatta kamuya açıklanır. Denetim makamları da bu gereklilikleri ve kriterleri Kurula

düzenlemeleri tümüyle kendi görüşlerimiz çerçevesinde ele alınacaktır. Tezim yazım tarihi itibarı ile GDPR m.42 ve 43 hakkında yazılan akademik yazılar yok denecek kadar az olduğu için maddeler tarafımızca şerh edilerek açıklamalar yapılacaktır.

Bir AB veri koruma otoritesinin GDPR 57 ve 58. maddeler kapsamında sahip olduğu görevlere ve yetkilere hâlel gelmeksizin, veri koruma ile ilgili yeterli bir uzmanlığa sahip olan sertifikasyon kuruluşları, gerekmesi halinde GDPR m.58 (2) (h) kapsamında yetkilerini kullanmak amacıyla ilgili veri koruma otoritesine bilgi vermesini müteakip, sertifikasyonu yapar veya sertifikasyonu yeniler.

GDPR m.58 (2) (h) bendi kapsamında bir AB veri koruma otoritesi 42 ve 43. maddeler uyarınca sağlanan bir sertifikasyonun geri alınması veya sertifikasyon kuruluşuna sertifikasyonun geri alınmasına dair talimat verilmesi veya sertifikasyon koşullarının karşılanmadığı yahut artık karşılanamadığı durumlarda, sertifikasyon kuruluşuna sertifikasyon yapmaması için talimat verme yetkisine haizdir.

Üye devletler bu sertifikasyon kuruluşlarının aşağıdakilerin biri veya her ikisi tarafından akredite edilmesini sağlayacaklardır:

(a) GDPR 55 veya 56. maddeler uyarınca yetkili veri koruma otoritesi,

(b) EN-ISO/IEC 17065/2012'ye uygun olarak 765/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü uyarınca ve GDPR 55 ya da 56. madde uyarınca yetkili

iletir. Kurul tüm sertifikasyon mekanizmaları ve veri koruma mühürlerini bir sicilde toplar ve uygun yollarla kamuoyuna açıklar. (7) Bölüm VIII'e hâlel gelmeksizin, akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya bir sertifikasyon organı tarafından gerçekleştirilen eylemlerin bu Tüzük'ü ihlal ettiği hallerde, yetkin denetim makamı veya ulusal akreditasyon organı bu maddenin 1. paragrafı uyarınca bir sertifikasyon organının akreditasyonunu kaldırır. (8) Komisyon 42(1) maddesinde atıfta bulunulan veri koruma sertifikasyon mekanizmalarına yönelik olarak gerekliliklerin belirtilmesi amacıyla 92. madde uyarınca yetki devrine dayanan tasarrufları kabul etmeye yetkindir., AB Başkanlığı GDPR çevirisi,

<https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf>, (e.t.: 24.4.2024)

olan veri koruma otoritesi tarafından belirlenen ek gereklilikler uyarınca tayin edilen ulusal akreditasyon mercii.

ISO/IEC 17065 ürün ve şirket sertifikasyonu ve uygunluk değerlendirmesi standardıdır. Sertifikasyon kuruluşlarının ISO/IEC 17065/2012'ye göre akredite edilmelerinde bu standard kullanılmakla birlikte standardın GDPR ile uyumlu bir şekilde uygulanması gerekmektedir. Sertifikasyon mekanizmasının kapsamı belirlenirken de hangi kriterlerin aranacağı, uzmanlık seviyesi ve değerlendirme metodolojisi de göz önüne alınmalıdır. Bu nedenle GDPR'ın kendine özgü özellikleri dikkate alınmalı ve sertifikasyon bu standarda göre yapılırken, standardın kapsamının ürünleri ve süreçleri kapsamaması nedeniyle sadece kişisel veri işleme ile ilgili olan ürünler ve süreçleri içermeli ve bunlar için değerlendirme yapılırken de GDPR gerekliliklerden daha az veya daha fazla bir gereklilik uygulanmamalıdır.

Sertifikasyon kuruluşlarının hangi şartlarda akredite edilecekleri ise maddenin 2. paragrafı ile düzenlenmiştir. Buna göre sertifikasyon kuruluşları, sertifikasyonun konusuna ilişkin bağımsızlıklarını ve yetkinliklerini ilgili veri koruma otoritesini tatmin edecek şekilde göstermek, GDPR 42(5) maddesinde atıfta bulunulan ve 55 veya 56. maddeler kapsamında yetkili olan veri koruma otoritesi tarafından veya 63. madde uyarınca EDPB tarafından onaylanmış olan ölçütlere uymayı taahhüt etmek, veri koruma sertifikasyonu, mühürleri ve işaretlerinin verilmesi, bunların periyodik olarak gözden geçirmelerinin yapılması ve sertifikasyonun geri alınmasına dair prosedürler meydana getirmek, sertifikasyon veya sertifikasyonun bir veri sorumlusu veya veri işleyen tarafından uygulanmasına ve uygulanma biçimine dair ihlal şikayetlerinin karşılanması ve yanıtlanmasına dair prosedürler ve mekanizmalar ortaya koymak ve işletiyor olmak ve bu prosedürler ve mekanizmaları ilgili kişiler için şeffaf ve erişilebilir hale getirmiş olmak

ve son olarak görevlerinin ve yetkilerinin bir menfaat çatışmasına sebebiyet vermediğini veri koruma otoritesini tatmin edecek şekilde göstermek zorundadırlar.

Sertifikasyon kuruluşlarının akreditasyonu, GDPR 55 veya 56. maddeler uyarınca yetkili olan veri koruma otoritesince veya GDPR 63. madde kapsamında EDPB tarafından belirlenmiş olan ölçütlere göre yapılır. GDPR m.43(1)(b) kapsamında akreditasyon yapılması durumunda, bu gereklilikler, akreditasyon ve piyasa gözetimine ilişkin (AT) 765/2008 sayılı Tüzük²¹⁵ ile getirilen gereklilikleri ve sertifikasyon kuruluşlarının belirtildiği teknik kuralları ve yöntemleri tamamlamaktadır. Yani aynen ISO 17065 Standardının GDPR gereklilikleri dikkate alınarak uygulanmasında olduğu gibi, 765/2008 sayılı Tüzük için de aynı husus geçerli olacaktır.

GDPR m.43(1)'de belirtilen sertifikasyon kuruluşları, veri sorumlularının ve veri işleyenlerin GDPR'a uyum ile ilgili yükümlülüklerine hanel gelmemek kaydıyla, sertifikasyonla neticelenen değerlendirmelerin yapılmasından yahut sertifikasyonun geri alınmasından sorumludurlar.

Akreditasyon azami beş yıllık bir süre için verilir ve sertifikasyon kuruluşunun GDPR m.43'de düzenlenen gereklilikleri karşılaması kaydıyla aynı şekilde yenilenebilir.

GDPR m.43(1)'de belirtilen sertifikasyon kuruluşları, talep edilen sertifikasyonun yapılması yahut geri alınmasına dair gerekçeleri ilgili veri koruma otoritesine sunmakla yükümlüdür.

GDPR m.43(3)'e göre belirlenen gereklilikler ve GDPR m.42(5) ile belirtilen ölçütler, ilgili veri koruma otoritesinin rahatlıkla ulaşabileceği bir formatta kamuoyuna sunulmalıdır. İlgili veri koruma otoriteleri bu gereklilikleri ve ölçütleri Kurul'a iletmelidir. Kurul tüm sertifikasyon mekanizmalarını ve kişisel verilerin korunmasına

²¹⁵ Akreditasyon ve Piyasaya Gözetimine Dair AT 765/2008 sayılı Tüzük için: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF>, (e.t. 22.10.2023).

dair mühürleri bir sicil sistemi içinde kayıt edecek ve bu sicile kamuoyunun erişimini sağlayacaktır.

GDPR m.43(7) uyarınca, akreditasyon şartlarının karşılanmaması yahut artık karşılanamıyor olması durumunda yahut bir sertifikasyon kuruluşunun icra ettiği faaliyetlerin GDPR hükümlerini ihlal etmesi durumunda ilgili veri koruma otoritesi veya ilgili ülkenin akreditasyon kuruluşu, bu sertifikasyon kuruluşunun akreditasyonunu iptal eder.

AB Komisyonu sertifikasyon mekanizmaları ve kişisel verilerin korunmasına dair mühürleri ve işaretleri ve bunların geçerliliği ile alakalı mekanizmalara dair teknik standartları belirlemeye yönelik kararlar alabilir.

4.2.3 GDPR ile Düzenlenen Akreditasyon ve Sertifikasyon Sistemi Hakkında Değerlendirmeler

4.2.3.1 Genel Olarak Akreditasyon

GDPR’ın kişisel verilerin korunmasında akreditasyon ve sertifikasyona dair 42 ve 43. maddelerindeki düzenlemeleri yukarıdaki şekilde açıkladıktan sonra, bu maddelerdeki düzenlemelerin ve bunların hayata geçirilmesi konusundaki detaylı değerlendirmelerin yapılması gerekmektedir.

GDPR veya herhangi bir ülkenin kişisel veri koruma mevzuatı ile düzenlenecek olan bir akreditasyon ve sertifikasyon sistemi öncelikle, ilgili kişisel verilerin korunması mevzuatına uyum sağlaması gereken veri sorumluları ve veri işleyenlerin hem uyum düzeylerini arttıracak hem de bu veri sorumluları ve veri işleyenler yetkili organların keyfi eylem ve işlemlerine karşı ve veri sahiplerinin yine keyfi başvuruları ve taleplerine karşı bir koruma sağlayacaktır. Ancak bu konu özellikle anayasal haklar bağlamında

hukuki güvenlik ilkesi ve temel hak ve özgürlüklere dair bir konu olduğu için ilerleyen bölümlerde anayasa hukuku açısından da ele alınacaktır.

Bunların yanı sıra kurulacak bir akreditasyon ve sertifikasyon sistemi şeffaflık ve hesap verebilirliği arttıracaktır. Bağımsız kuruluşlarca gerçekleştirilecek sertifikasyon sürecinde iş süreçlerini şeffaf bir şekilde açmak ve veri koruma mevzuatı ile uyumlu olduğunu göstermek ve bu uyumluluğun dış dünyaya duyurulması anlamına gelen sertifikasyona hak kazanmak şeffaflık gereğini yerine getirecek, veri işleme süreçlerinin kapsamının, sınırlarının, politika ve prosedürlerinin belirlenmiş olması, şikayet alma ve karşılama mekanizmalarının kurulmuş olması, belli bir kayıt sisteminin kurulmuş olması ve nihayet tüm bu süreçlere dahil sorumluların ve yönetim modelinin belirlenmiş olması da hesap verebilirliği sağlayacaktır.

Akreditasyon ve sertifikasyon mekanizmasının yukarıda bahsedilen kendinden beklenen işlevleri ve faydaları yerine getirebilmesi ise üst otoritelerin yönlendirmeleri ve düzenlemeleri sayesinde gerçekleşebilir. Örneğin EDPB yayınladığı rehberler ile bu mekanizmanın detaylarında neler olması gerektiğini göstermiştir. Bu rehberlerden ilki 4 Haziran 2019 tarihli 1/2018 sayılı “Sertifikasyon ve Sertifikasyon Ölçütlerinin Belirlenmesine Dair Rehber”dir²¹⁶. 6 Nisan 2021 tarihinde ise bu rehber ek olarak “Sertifikasyon Değerlendirme Kriterleri” rehberini yayınlamıştır²¹⁷. İkincisi yine 4 Haziran 2019 tarihli 4/2018 sayılı “Sertifikasyon Kuruluşlarının Akreditasyonuna Dair

²¹⁶ Haziran 2019 tarihli 1/2018 sayılı “Sertifikasyon ve Sertifikasyon Ölçütlerinin Belirlenmesine Dair Rehber: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf , (e.t. 22.10.2023)

²¹⁷ Sertifikasyon Değerlendirme Kriterleri Rehber: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidance-certification-criteria-assessment_en, (e.t. 22.10.2023).

Rehber”dir²¹⁸. 14 Haziran 2022 tarih ve 07/2022 tarihinde de “Yurtdışı Veri Aktarımlarında Sertifikasyonun Bir Araç Olarak Kullanılmasına Dair” rehberiyayınlanmıştır²¹⁹. EDPB dışında İrlanda Otoritesi Eylül 2020’de “GDPR Sertifikasyonu Rehberi”ni²²⁰, Lüksemburg Otoritesi de “Sertifikasyon Kriterleri”ni²²¹ yayınlamıştır.

Bu rehberler ile GDPR kapsamında akreditasyonun amaçları, GDPR Madde 43(1) kapsamında akreditasyonun hangi yollarla yapılabileceği ve dikkate alınması gereken önemli hususlar ortaya konulmuş ve akreditasyonun ulusal akreditasyon kurumları tarafından yapıldığı durumlarda veri korumaya dair hukuki düzenlemelerin getirdiği ek gerekliliklere dair çerçeve oluşturulmuş olmaktadır.

Burada dikkat edilmesi gereken noktalardan biri bu rehberlerin, adım adım sistemin kuruluşunu ve işleyişini tariflemediği, akreditasyon ve sertifikasyon konusunda yeni bir teknik veya öneri getirmediği, sadece GDPR gerekliliklerinin de dikkate alındığı bir çerçeve sunduğudur.

Sistemin sadece bir sertifikasyon mekanizması olarak değil de akreditasyon ile birlikte kurulan bir sertifikasyon sistemi olması çok önemlidir. Bu sayede, kamuoyunda bir güven unsuru oluşturulmakta ve diğer yandan sistem üst perdeden bir yetkili kurumun güvencesinde ve denetiminde olmaktadır.

²¹⁸ 4 Haziran 2019 tarihli 4/2018 sayılı “Sertifikasyon Kuruluşlarının Akreditasyonuna Dair Rehber: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en, (e.t. 22.10.2023).

²¹⁹ Yurtdışı Veri Aktarımlarında Sertifikasyonun Bir Araç Olarak Kullanılmasına Dair” Rehber: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en, (e.t.: 22.10.2023).

²²⁰ İrlanda Otoritesi’nin GDPR Sertifikasyonu Rehberi: https://www.dataprotection.ie/sites/default/files/uploads/2020-09/GDPR%20Certification%20Guidance_0.pdf, (e.t. 22.10.2023)

²²¹ Lüksemburg Otoritesinin Sertifikasyon Kriterleri: <https://cnpd.public.lu/dam-assets/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf>, (e.t. 22.10.2023)

4.2.3.2 GDPR m.43 Kapsamında Akreditasyon

GDPR’ın yukarıda da incelediğimiz 42 ve 43. maddelerinde akreditasyonun bir tanımı yapılmamıştır. Buna karşın 765/2008 sayılı Tüzük m.2(10) akreditasyon için gerekenleri sayarken, akreditasyonu “ulusal bir akreditasyon kuruluşu tarafından, bir sertifikasyon kuruluşunun, belirli bir uygunluk değerlendirme faaliyetini yürütmek için uyumlaştırılmış standartlar tarafından belirlenen gereklilikleri ve uygulanabilir olduğunda, ilgili sektörel düzenlemelerinde belirtilenler de dahil olmak üzere herhangi bir ek gerekliliği yerine getirdiğinin onaylanması” olarak tanımlamaktadır.

Sertifikasyon kuruluşlarını akredite eden akreditasyon kuruluşları için genel şartlar standardı olan ISO/IEC 17011’de ise akreditasyon “belirli sertifikasyon görevlerini yerine getirme yetkinliğini resmi olarak gösteren bir sertifikasyon kuruluşu ile ilgili üçüncü taraf onayı” olarak tanımlanmıştır.

GDPR ile ilgili olarak, akreditasyon gerekliliklerinin atıf yapıldığı ISO/IEC 17065/2012 ve GDPR m.43 (1)(b) uyarınca, yetkili olan kişisel veri otoritesi tarafından oluşturulan “ek gereklilikler”in yerine getirilip getirilmediği, ulusal akreditasyon kuruluşu tarafından veya akreditasyonu ilgili ülkenin kişisel veri otoritesi yapmışsa onun tarafından incelenecektir.

Her iki durumda da, yani gerek ulusal akreditasyon kuruluşu ve gerekse ilgili ülkenin kişisel veri koruma otoritesinin getirdiği gereklilikler her halükarda Madde 43(2)'de belirtilen gereklilikleri kapsamalıdır.

Bu açıklamalardan yola çıkarak GDPR kapsamında akreditasyonun tanımı aşağıdaki şekilde yapılabilir:

“GDPR kapsamında akreditasyon, ulusal bir akreditasyon kuruluşu ve/veya bir veri koruma otoritesi tarafından, bir sertifikasyon kuruluşunun, ISO/IEC 17065/2012 ve

belirlenebilecek diğer gereklilikler de dikkate alınarak, GDPR Madde 42 ve 43 uyarınca sertifikasyon yapmaya yetkin olduğuna dair verilen onaydır.”

GDPR m.43(1), Üye Devletlerin sertifikasyon kuruluşlarının akredite etmelerini sağlayacak düzenlemeleri yapmalarını gerektirmektedir. Böylece her Üye Devlet, akreditasyon değerlendirmesini yapmak ile kimin sorumlu olacağını belirleme yükümlülüğü altındadır.

GDPR m43(1) kapsamında akreditasyon, yalnızca veri koruma otoritesi tarafından, kendi belirleyeceği gereklilikler temelinde, 765/2008 Tüzüğü uyarınca ve ISO/IEC 17065/2012 çerçevesinde ve ilgili kişisel veri koruma otoritesi tarafından belirlenen ek gereklilikler kapsamında ulusal akreditasyon kuruluşu tarafından ve hem ilgili veri koruma otoritesi hem de ulusal akreditasyon kuruluşu tarafından yapılabilir.

4.2.3.3 765/2008 Sayılı Tüzük ile GDPR m.43 Kapsamındaki Düzenleme Arasındaki İlişki

765/2008 Sayılı Tüzüğün 2(11) maddesi ulusal bir akreditasyon kuruluşunu “Üye Devlette, devletten alınan yetkiyle akreditasyon gerçekleştiren tek kuruluş” olarak tanımlamaktadır. Bu bakımdan 765/2008 sayılı Tüzük m.2(11), Üye Devletin ulusal akreditasyon kurumu dışında bir kurum tarafından akreditasyona izin veren GDPR m.43(1) ile çelişiyor görünmektedir.

Ancak burada özel bir durum olduğu açıktır. GDPR’ın amacının, veri koruma otoritelerine, sertifikasyon kuruluşlarının akreditasyonu konusunda aynı yetkiyi vererek, akreditasyonun yalnızca ulusal akreditasyon makamı tarafından yürütülmesine ilişkin genel ilkedен sapılmıştır. Bu nedenle GDPR m.43(1)’in, 765/2008 sayılı Tüzüğün 2(11) maddesine göre “lex specialis” olduğu yani aralarında bir “özel – genel düzenleme” ilişkisi bulunduğunu söylemek mümkündür. Bu nedenle genel düzenleme olan 765/2008

karşısında özel düzenleme olan GDPR m.43(1)'in uygulanması ile yukarıdaki paragrafta bahsetmiş olduğumuz çelişki giderilebilecektir.

4.2.3.4 GDPR Kapsamında Akreditasyonda Ulusal Akreditasyon Kuruluşunun Rolü

GDPR m.43(1)(b), ulusal akreditasyon kuruluşunun, sertifikasyon kuruluşlarını ISO/IEC 17065/2012 ve yetkili veri koruma otoritesi tarafından belirlenen ek gereklilikler uyarınca akredite edeceğini hüküm altına almaktadır. Belirtmek gerekir ki, GDPR m.43(3)'te 43. maddenin 1. paragrafındaki (b) bendine yapılan atıfta belirtilen “gereklilikler”in, GDPR m.43(1) uyarınca yetkili veri koruma otoritesi tarafından oluşturulan “ek gereklilikleri” ifade ettiği tarafımızca değerlendirilmektedir. Bu nedenle de akreditasyon sürecinde, ulusal akreditasyon kuruluşları, veri koruma otoriteleri tarafından belirlenecek ek gereklilikleri uygulamakla yükümlü olacaklardır.

GDPR kapsamında sertifikasyon için akreditasyon yalnızca yetkili veri koruma otoritesi tarafından yapılıyorsa, akreditasyon için başvuran bir sertifikasyon kuruluşunun ilgili veri koruma kuruluşu tarafından belirlenen gereksinimlerin tümünü karşılaması gerekecektir. Yani ulusal akreditasyon kuruluşu nezdinde, bir kuruluş daha önce GDPR dışındaki alanlar için akredite edilmiş olsa bile, kişisel verilerle ilgili olarak kapsamını genişletmek istemesi durumunda o ülkenin veri koruma otoritesi ek gereklilikler getirmişse bu ek gereklilikleri yerine getirmediği müddetçe akredite edilmesi mümkün olmayacaktır.

4.2.3.5 GDPR Kapsamında Akreditasyonda Veri Koruma Otoritesinin Rolü

GDPR m.57(1)(q)'daki açık düzenleme ile ilgili veri koruma otoritesi, bir sertifikasyon kuruluşunun akreditasyonunu Madde 43 kapsamında denetim otoritesi vazifesi kapsamında yapma yetkisine sahiptir.

GDPR m.43(1) aslında bir miktar esneklik içeren maddedir. Bu kapsamda, veri koruma otoritesinin akreditasyon işlevini, yalnızca gerekli olduğunda yerine getireceği bir yetki olarak anlamak daha doğru olacaktır. Zaten bu yüzden ulusal akreditasyon kuruluşlarının veya ilgili ülke veri koruma otoritesinin de akreditasyon için yetkili olabileceği belirtilmiştir. Başka bir deyişle ilgili ülke veri koruma otoritesi zorunlu olarak akreditasyonu yapacaktır şeklinde bu düzenlemeler anlaşılmamalıdır. Ama tabii bu tür anlayış ve uygulama farklarının olmaması için de üye ülkeler iç hukuklarında bu durumu açıklığa kavuşturabilirler. GDPR'ın AB çapında uygulanan genel geçer bir tüzük niteliğinde olması, üye ülkelerin kendi iç hukuklarında bu tür uygulamada tereddüt duyulacak konuları düzenlemelerine engel değildir. Ancak bunu yaparken, örnekleri de görüldüğü üzere üye devletler EDPB'den görüş istemektedirler²²².

Elbetteki EDPB'nin olumlu bir görüş vermesi veya ilgili ülke veri koruma otoritesinin ek gereklilikler belirlemesi ve bunların bir sertifikasyon kuruluşu tarafından karşılanıyor oluşu, bir ulusal akreditasyon kuruluşu tarafından yapılan bir akreditasyon sürecinde, GDPR m.43(2)(a) maddesi uyarınca sertifikasyon kuruluşunun, sertifikasyon mekanizmasının konusuyla ilgili olarak veri koruma otoritesini tatmin edecek şekilde bağımsızlığını ve uzmanlığını göstermesi zorunluluğunu ortadan kaldırmamaktadır.

²²² Polonya'nın akreditasyon ile ilgili başvurusu hakkındaki 11/2022 sayılı EDPB görüşü buna örnek gösterilebilir: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112022-draft-decision-competent_sv , (e.t. 24.10.2023)

Bir Üye Devlet, sertifikasyon kuruluşlarının veri koruma otoritesi tarafından akredite edilmesini şart koşarsa, veri koruma otoritesi GDPR m.43(2)'de ayrıntıları belirtilen gereklilikler dahil ancak bunlarla sınırlı olmamak üzere, akreditasyon gereklilikleri oluşturmalıdır. Ulusal akreditasyon kuruluşları tarafından sertifikasyon kuruluşlarının akreditasyonu ile ilgili yükümlülüklerle kıyasla, GDPR m.43, veri koruma otoritesi akreditasyonu kendisi yürüttüğünde, akreditasyon gereklilikleri hakkında veri koruma otoritesine daha az yükümlülükler getirmektedir.

GDPR kapsamında AB'nin tüm üye devletlerin hukuklarını uyumlaştırma ve bu kapsamda tümüyle uyumlaştırılmış bir akreditasyon sisteminin oluşturulmasına katkıda bulunma amacıyla, veri koruma otoritesi tarafından getirilen akreditasyon ölçütlerinin belirlenme usulleri ISO/IEC 17065 ile uyumlu olmalı ve Madde 43(1)(b) uyarınca ilgili veri koruma otoritesinin belirlediği ek gereklilikler ile tamamlanmalıdır.

İlgili veri koruma otoritesi tarafından oluşturulan ek gerekliliklerin, sertifikasyon kuruluşlarının kişisel verilerin korunması ile ilgili uzmanlık seviyelerinin, örneğin kişisel verilerin, veri sorumluları ve veri işleyenler tarafından işlenmesine dair süreçlerinin, GDPR'daki veri işleme ilkeleri, veri işleme şartları ve sair teknik, hukuki ve idari gereklilikler açısından değerlendirme ve analiz edebilme yetkinlikleri gibi yetkinliklerinin değerlendirilebilmesi ve ölçülebilmesini sağlamasını gerektirmektedir. Bu gereklilikler, aynı zamanda çeşitli sektörlerdeki o sektörlerin kendine özgü durumlar bakımından da değerlendirme ve analiz yapabilmeyi gerektirmelidir. Diğer yandan bu gereklilikler ayrıca gerçek kişilerin temel hak ve özgürlüklerinin ve özellikle kişisel verilerin korunması hakkının yasal düzenlemeye uygun olarak korunmasına ilişkin olarak gerekli yetkinlikleri de ölçebilmeyi içermelidir.

Akreditasyon ve sertifikasyon konusunda ilgili  lke veri koruma otoritesinin bir dięer rol  de  effalığın saęlanması i in akreditasyon ve sertifikasyon ile ilgili t m d zenlemelerin kamuoyuna duyurulmasının saęlanmasıdır. Nitekim GDPR m43(6) uyarınca madenin 3. Paragrafında belirtilen gerekliliklerin ve 42(5) maddesinde belirtilen sertifikasyon kriterlerinin ilgili veri koruma otoritesi tarafından kamunun rahatlık ulařabileceęi bir ortamda kamunun eriřimine a ılması gerekmektedir. B ylece hem  effalık saęlanmış olunacak hem de sertifikasyon kuruluřlarına duyulan g ven artacaktır.

4.2.3.6 Veri Koruma Otoritesinin Sertifikasyon Kuruluřu Olarak Hareket Etmesi

Bu noktada sorulması gereken  nemli sorulardan biri GDPR’da d zenlenen rejim kapsamında bir veri koruma otoritesinin doęrudan kendisinin bir sertifikasyon kuruluřu olarak hareket edip edemeyeceęidir. GDPR m.42(5), bir veri koruma otoritesinin sertifikasyon yapabileceęini d zenlemektedir. Ancak bu durumda GDPR, veri koruma otoritesinin kendisinin 765/2008 sayılı T z k kapsamındaki gereklilikleri karřılamak i in ayrıca akredite edilmesini zorunlu kılmamaktadır. GDPR m.43(1)(a) ve  zellikle Madde 58(2)(h), 3(a, e-f) kapsamında veri koruma otoritelerine hem akreditasyon yapma hem de sertifikasyon yapma ve aynı zamanda da tavsiye verme yetkisi vermekte ve gerektiğinde de veri koruma otoritesine sertifikasyonu geri alma veya sertifikasyon kuruluřlarına sertifikasyon yapmamaları konusunda emir verme yetkisi de vermektedir.

Akreditasyon ve sertifikasyon yapma rollerinin ve g revlerinin ayrılmasının gerekli olacaęı durumlar olabilir.  rneğin, bir veri koruma otoritesi ile dięer sertifikasyon kuruluřlarının bir  ye Devlette bir arada bulunması ve her ikisinin de aynı belgeyi verebilme yetkisine sahip olması gibi bir durum ortaya  ıkabilir. Bu nedenle, veri koruma otoriteleri, bu t r durumların ortaya  ıkarabileceęi menfaat  atıřmalarını  nlemek i in

önlemler almalı, ve sertifikasyon mekanizmasının sağlıklı bir şekilde kurulabilmesi ve işleyebilmesi için GDPR kapsamındaki görevleri ayracağı önlemleri almalıdır. Buna ek olarak, Üye Devletler ve veri koruma otoriteleri, GDPR'a uygun olarak akreditasyon ve sertifikasyonla ilgili ulusal yasaları ve uygulanacak kriterleri ve prosedürleri hayata geçirirken AB'nin mevzuatların uyumlaştırılmasına dair hedefini mutlaka göz önünde bulundurmalıdır. Aksi takdirde 95/46 sayılı Yönerge zamanında olduğu gibi Avrupa çapında birbirinden çok farklı uygulamalar ortaya çıkabilir ve bu durum hem temel hak ve özgürlükler için zararlı olabilir hem de tek pazar ilkesine ve çabalarına zarar verebilir. Veri temelli bir ekonomi içinde yaşamaya başladığımızı düşündüğümüzde bu harmonizasyonun Avrupa için hayati bir önemi olduğu da açıktır.

4.2.4 Akreditasyon Gereklilikleri

4.2.4.1 Genel Olarak

Yukarıda belirtildiği üzere, sertifikasyon kuruluşlarının 765/2008 sayılı Tüzük kapsamında ulusal akreditasyon kuruluşu tarafından akredite edildiği durumlarda, ISO/IEC 17065/2012, yine yukarıda ayrıntılı olarak anlatıldığı üzere veri koruma otoritesi tarafından belirlenen ek gereklilikler ile tamamlanan ilgili akreditasyon standardı olacaktır. GDPR m.43(2) kapsamında yapılan düzenleme aslında ISO/IEC 17065/2012 standardının genel hükümlerini yansıtmaktadır. Bu nedenle, akreditasyon gereklilikleri ortaya konulurken gerekliliklerin belirlenmesi için, bir temel olarak GDPR m.43(2) ve ISO/IEC 17065/2012 kullanılacaktır. Ayrıca sertifikasyon kuruluşunun veri koruma uzmanlığının seviyesinin belirlenmesinde ve değerlendirilmesinde ve böylece gerçek kişilerin kişisel verilerinin işlenmesinde, onların anayasal bir hak olarak temel haklarını

ve özgürlüklerini koruma yönündeki yetkinliklerine ilişkin de ilgili ülke veri koruma otoritesinin getireceği gereklilikler dikkate alınacaktır.

İlgili ülkenin veri koruma otoritesi tarafından belirlenecek olan ek akreditasyon gereklilikleri, akreditasyon talebinde bulunan tüm sertifikasyon kuruluşlarına, önceki tecrübelerine, uzmanlık alanlarına, çalıştırdıkları uzman sayılarına vb diğer kriterlere göre herhangi bir ayırım gözetilmeden uygulanacaktır Akreditasyon kuruluşu, yukarıda belirtilen hususları da göz önünde tutarak söz konusu sertifikasyon kuruluşunun ek gereklilikler ve sertifikasyon konusu doğrultusunda sertifikasyon faaliyetini yürütmek için yetkin olup olmadığını değerlendirecektir.

Ancak ilgili ülke veri koruma otoritelerinin, akreditasyon için başvuran sertifikasyon kuruluşunun sahip olduğu sektörel uzmanlıklara veya ürün, hizmet, süreç gibi kırımlardaki sahip oldukları uzmanlıkları göz önüne alarak belirli sektörlerle, ürün, hizmet veya süreçlere göre bir yetkilendirmeye gidebilecekleri tarafımızca düşünülmektedir.

Üzerinde durulması gereken bir diğer konu ise, sertifikasyon kuruluşları akredite edilirken sadece kendi sahip oldukları yeteneklerin mi göz önüne alınacağı yoksa bu kuruluşların sertifikasyon faaliyetlerini yerine getirirken işbirliği yaptıkları, destek aldıkları laboratuvarlar gibi dış kaynak hizmeti sağlayan işbirliği yaptığı kuruluşlarla birlikte olan yeteneklerinin mi göz önüne alınacağıdır.

Laboratuvarlar veya denetçiler gibi diğer dış kaynak kuruluşları, sertifikasyon faaliyetlerinin bazı kısımlarını sertifikasyon kuruluşu adına gerçekleştiriyorsa, ISO/IEC 17065/2012 gerekliliklerine ek olarak, bunların veri koruma alanındaki özel uzmanlıklarının da ispatlanması gerekmektedir. Bu gibi durumlarda, bu tip dış kaynak

tedarikçisi niteliğindeki kuruluşların GDPR kapsamında akreditasyonunun mümkün olmadığını düşünüyoruz.

Zaten bir kuruluş sertifikasyon için akredite edilmiş ise bu kuruluşa bir takım hizmetler sağlayan alt yüklenici diyebileceğimiz kuruluşların da GDPR kapsamında akredite edilmeleri söz konusu olmayacaktır. Ancak, bu kuruluşların akredite sertifikasyon kuruluşları adına faaliyet göstermeleri durumunda, bu alt yüklenicinin akredite sertifikasyon kuruluşuna akreditasyon verilebilmesi için gerekli olan veri koruma uzmanlığı seviyesinde uzmanlığa sahip olduğunu bu sertifikasyon kuruluşunun göstermesi, bunu kanıtlaması gerekir.

4.2.4.2 Akreditasyon İçin Genel Şartlar

Bir sertifikasyon kuruluşu ulusal akreditasyon kuruluşuna veya ilgili ülke veri koruma otoritesine, ilgili ülke veri koruma otoritesi tarafından çıkarılacak ek gereklilikler de dahil olmak üzere akreditasyon için gerekli yasal şartlara ve bu şartların uygulanmasına uyduğunu gösteren güncel politikalara, prosedürlere ve sair belgelere sahip olduğunu gösterebilmelidir.

Sertifikasyon kuruluşunun kendisi de bir veri sorumlusu ve veri işleyen olduğu için GDPR'a uyumlu olduğunu da gösterebilmelidir. Bu bakımdan ilgili ülke veri koruma otoritesi akreditasyon öncesinde, sertifikasyon kuruluşlarının GDPR uyumluluğunu kontrol etmek amacıyla sertifikasyon kuruluşuna ek yükümlülükler ve gereklilikler getirebilir.

4.2.4.3 Akreditasyon için Yasal Şartlar

4.2.4.3.1 Sertifikasyon Sözleşmesi

Akredite olmak isteyen bir sertifikasyon kuruluşunun ulusal akreditasyon kuruluşu ile veya ilgili ülke veri koruma otoritesi ile bir sözleşme yapması gerekmektedir. Sertifikasyon kuruluşu, ISO/IEC 17065/2012 gerekliliklerine ek olarak, sertifikasyon sözleşmelerinin ISO/IEC 17065/2012, GDPR m.43(2)(b) ve GDPR m.42(5) uyarınca ilgili ülke veri koruma otoritesi veya EDPB tarafından getirilen kriterleri, GDPR m.42(7) ve GDPR m.58(1)(c) uyarınca ilgili ülke veri koruma otoritesinin denetimini ve şeffaflığı sağlayacak hükümler, sözleşmenin yapılmış olmasının veya akreditasyonun yapılmış olmasının sertifikasyon kuruluşunun GDPR'a uyum yükümlülüğünü ortadan kaldırmadığına ve ayrıca GDPR m.42(5) uyarınca yetkili olan ilgili ülke veri koruma otoritelerinin görevlerine ve yetkilerine hanel getirmedigine dair hükümleri, GDPR m.42(6) uyarınca sertifikasyon sürecini yürütmek için gerekli olan tüm bilgileri ve işleme faaliyetlerine erişimi sağlamayı, başvuru yapan sertifikasyon kuruluşunun geçerli son tarihlere ve prosedürlere uymasını şart koşmalıdır.

Ayrıca sertifikasyon sözleşmesi; ISO/IEC 17065/2012, GDPR m.42(7) ve GDPR m.43(4) uyarınca verilecek sertifikaların geçerlilik, yenileme ve geri alınmasına dair kuralları belirlemeli ve bunlara uygun olarak yeniden değerlendirme veya gözden geçirme için uygun aralıkları belirleyen kuralları, GDPR m.42(8) ve GDPR m.43(5) uyarınca sertifikasyon kuruluşunun sertifikasyon için gerekli tüm bilgilerine erişilebileceğini, şikayet yönetimine dair kuralları ve prosedürleri, ISO/IEC 17065/2012'de atıfta bulunulan minimum gerekliliklere ek olarak, sertifikasyon kuruluşu için akreditasyonun geri çekilmesi veya askıya alınmasına ve bunların sonuçlarına dair hükümleri ve son olarak sertifikasyon kuruluşunun fiili veya yasal durumunda ve

sertifikasyon ile ilgili ürünleri, süreçleri ve hizmetlerinde önemli değişiklikler olması durumunda bilgilendirmeye dair hükümler içermelidir.

4.2.4.3.2 Tarafsızlık

Akreditasyon kuruluşu, ISO/IEC 17065/2012 ve GDPR m.43(2)(a) ile uyumlu olarak, tarafsızlığını kanıtlamak zorundadır. Bu özellikle sertifikasyon kuruluşunun finansmanına ilişkin delilleri içermeli, bir çıkar çatışmasının olmadığı gösterilmelidir.

4.2.4.3.3 Sorumluluk ve Finansman

Akreditasyon kuruluşu, ISO/IEC 17065/2012'deki gerekliliğe ek olarak, sertifikasyon kuruluşunun faaliyet gösterdiği coğrafi bölgelerdeki yükümlülüklerini karşılamak için, sigorta gibi uygun önlemlerin alınmasını sağlamalıdır.

4.2.4.3.4 Kamunun Bilgilendirilmesi

Akreditasyon kuruluşu, ISO/IEC 17065/2012'deki gerekliliğe ek olarak, sertifikasyon kuruluşundan; sertifikasyon için gerekli olan ve veri koruma otoritesi tarafından onaylanmış kriterlerin tüm sürümlerinin, tüm sertifikasyon prosedürlerinin, şikayetlerin alınması ve değerlendirilmesi prosedürlerinin kamuya duyurularak kamunun bilgilendirilmesini sağlamalıdır.

4.2.4.3.5 Personel Nitelikleri

ISO/IEC 17065/2012 Bölüm 6'daki kapsamına ek olarak sertifikasyon kuruluşlarının personelleri, GDPR m.43(1) uyarınca veri korumasına ilişkin olarak bilgi ve deneyim sahibi olmalı ve bunu kanıtlayacak belgeleri göstermelidir. Bu personellerin GDPR m.43(2)(e) uyarınca çıkar çatışması olmamalıdır. Ayrıca personeller GDPR M.43(2)(b)'de atıfta bulunulan kriterlere uymayı taahhüt etmeli, teknik ve idari veri koruma önlemleri konusunda bilgi ve deneyime sahip olmalı, teknik uzmanlığa sahip

olduğunu kanıtlayabilmek için ilgili mesleki alanda en az EQF20²²³ seviye 6 uzmanlığı veya tanınmış bir diplomaya sahip olmalıdır. Bunların yanısıra personeller akademik derece olarak yüksek lisans veya eşdeğeri veya önemli mesleki deneyim dahil olmak üzere en az sekiz yarıyıl boyunca bir AB üyesi devlet tarafından tanınan üniversitede akademik çalışma yapmış olmalıdır. Son olarak da personel veri koruma hukuku alanında bilgi ve deneyim sahibi olmalıdır.

4.2.4.4 Süreç Gereklilikleri

Akreditasyon kuruluşları ISO/IEC 17065/2012'deki gerekliliklere ek olarak aşağıdakileri de sağlamalıdır:

Sertifikasyon kuruluşları, başvurularını yaparken ve sertifikasyon süreçlerini yürütürken uymaları gereken yükümlülüklerinin ve vazifelerinin GDPR m.43(2)(b) kapsamında bir menfaat çatışması oluşturmadığını taahhüt etmelidirler.

Bir sertifikasyon kuruluşu, bir Üye Devlette yeni bir onaylı Avrupa Veri Koruma Mührü verilmesiyle ilgili çalışmaya başlamadan önce ilgili ülkenin ulusal akreditasyon kuruluşunu bilgilendirmelidir.

Sertifikasyonun amacı başvuruda ayrıntılı olarak açıklanmalıdır. Bu ayrıca diğer sistemlere ve kuruluşlara, protokollere aktarımları da içermektedir.

Başvuruda, veri işleyenlerin olması durumunda veya başvuranın veri işleyen olması durumunda veri işleyenlerin yükümlülükleri açıklanmalı ve başvuruda veri sorumlusu ile veri işleyen arasındaki sözleşme de sunulmalıdır.

²²³ Avrupa Mesleki Yeterlilik Şeması hakkında bilgi için: <https://europa.eu/europass/en/european-qualifications-framework-eqf> , (e.t. 16.11.2023)

Sertifikasyon sözleşmesinde sertifikasyonun amacı ile alakalı bağlayıcı bir değerlendirme metodu yer almalı ve bu değerlendirme veri koruma ile ilgili yeterli bir teknik ve hukuki uzmanlığın bulunup bulunmadığını da içermelidir.

Yapılacak değerlendirme, sertifikasyon mekanizmalarının, veri işleme faaliyetlerinin sertifikasyon kriterlerine uygunluğunu değerlendirmek için yeterli sertifikasyon yöntemlerini tanımlamalı, amaçları ve ilgili veri sahipleriyle ilgili olarak işleme faaliyetlerinin gerekliliğini ve orantılılığını değerlendirmek için bir yöntem olmalıdır. Ayrıca GDPR'ın işleme faaliyetlerinin kaydına dair 30, kişisel veri işleme güvenliğine dair 32, veri koruma etki değerlendirmesine dair 35 ve ön istişareye dair 36. maddeleri uyarınca hukuki sonuçlara ilişkin olarak veri sorumlusu ve veri işleyen tarafından dikkate alınan tüm risklerin kapsamına, bileşimine ve değerlendirmesine ve ayrıca GDPR uyarınca teknik ve idari tedbirlerin tanımlanmasına ilişkin bir yöntem tanımlamalıdır.

Sertifikasyona konu veri işleme faaliyetleri bağlamında, kişisel verilerin korunmasını sağlamak ve kriterlerde belirtilen yasal gerekliliklerin yerine getirildiğini göstermek için garantiler, güvenceler ve prosedürler dahil olmak üzere çözüm yollarını değerlendirmek için ve sertifikasyon kuruluşunun, bu sertifikasyon yöntemlerinin standart ve genel olarak uygulanabilir olmasını sağlaması için de bir yöntem geliştirilmelidir. Bunların haricinde, ISO/IEC 17065/2012'nin 7.4.2 maddesine ek olarak, değerlendirmenin sertifikasyon kuruluşu tarafından bilinen dış uzmanlar tarafından yapılmasına izin verilmelidir.

GDPR madde 42 ve 43 uyarınca, ISO/IEC 17065/2012'nin 7.4.5 maddesine ek olarak, halihazırda sertifikasyon konusunun bir kısmını kapsayan veri koruma sertifikasının mevcut bir sertifikaya dahil edilmesi söz konusu olursa, sertifikasyon

kuruluşu mevcut sertifikanın da kriterlere uygunluğunu kontrol etmekle yükümlüdür. Tanınma, herhangi bir şekilde, eksiksiz bir değerlendirme raporunun veya önceki sertifikasyon faaliyetinin ve sonuçlarının değerlendirilmesini sağlayan bilgilerin mevcudiyetini gerektirecektir. Kanaatimizce böyle bir durumda, bir sertifikasyon beyanı veya benzer sertifikasyon sertifikaları, gereklilikler ve ek gerekliliklere göre hazırlanması gereken bir raporun yerine geçmek için yeterli görülmemelidir.

ISO/IEC 17065/2012'nin 7.4.6 maddesine ek olarak, sertifikasyon kuruluşunun sertifikasyon mekanizmasında, madde 7.4.6'da istenen bilgilerin müşteriye (belge başvuru sahibini) uygunsuzluklar hakkında nasıl bilgilendirdiğini ayrıntılı olarak belirtmesi istenmelidir.

ISO/IEC 17065/2012 madde 7.4.9'a ek olarak, belgelerin talep üzerine veri koruma otoritesinin tamamen erişimine açık hale getirilmesi gerekir.

Sertifikasyon kuruluşunun verdiği sertifikasyon kararları ile alakalı olarak tarafsızlığını nasıl sağladığına ve tarafsızlık ile ilgili sorumluluğuna dair ayrıntılı prosedürler mevcut olmalıdır.

Sertifikasyon belgelerinin ISO/IEC 17065/2012 Madde 7.7.1.e'ye ek olarak ve GDPR m. 42(7) uyarınca, geçerlilik süresinin üç yılı geçmemesi gerekir. Bu sürenin takibi mutlaka sertifikasyon kuruluşları tarafından yapılmalıdır.

Sertifikasyon kapsamına alınan süreçler, ürünler ve hizmetler kamuya açık bir ortamda tutulmalıdır. Sertifikasyon kuruluşu, halka değerlendirme raporunun yönetici özetini sunmalıdır. Bu yönetici özetinin amacı, neyin sertifikalandırıldığı ve nasıl değerlendirildiği konusunda şeffaflığa yardımcı olmaktır. Bu özetle de sertifikasyonun kapsam, ilgili sertifikasyon kriterleri, değerlendirme yöntemleri ve yürütülen testler ile sonuç kısımları yer almalıdır.

ISO/IEC 17065/2012 madde 7.8'e ek olarak ve GDPR m.43(5) uyarınca, sertifikasyon kuruluşu, sertifikasyonun verilmesi veya geri alınmasının gerçeklerini ilgili ülke veri koruma otoritesine veya ulusal akreditasyon kuruluşuna bildirmelidir.

Sertifikasyonu etkileyen değişiklikler ISO/IEC 17065/2012'nin 7.10.1 ve 7.10.2 maddelerine ek olarak, sertifikasyon kuruluşu tarafından dikkate alınmalıdır. Veri koruma mevzuatındaki değişiklikler, GDPR m. 43(8) ve m. 43(9) uyarınca Avrupa Komisyonu, Avrupa Veri Koruma Kurulu kararları ve veri korumasına ilişkin mahkeme kararları gibi durumlar sertifikasyonu etkileyen değişiklikler olarak sayılabilir.

Böyle bir durumun ortaya çıkması halinde sertifikasyon kuruluşu, bir geçiş periyodu belirleyerek bu periyod içinde ilgili veri sorumlusunun veya veri işleyenin süreçlerini bu yeni durum ile uyumlu hale getirmesini istemelidir. Bundan sonra ilgili veri sorumlusu veya veri işleyen bu değişiklikleri yaparsa bu durumu inceleyerek yeni duruma uygun olup olmadığını kontrol etmeli ve böylece sertifikasyonun devamına veya sertifikasyonun geri alınmasına karar vermelidir. Bu durumda ortaya çıkan bu yeni durumun getirdiği ek gereklilikler ve kriterlerin tanımlandığı bir prosedürün de oluşturulmasının hukuki güvenlik açısından zaruri olduğu kanaatindeyiz.

Bir sertifikasyonun değiştirilmesi, kısıtlanması, askıya alınması veya geri alınması durumunda, sertifikasyon kuruluşunun, ISO/IEC 17065/2012 Bölüm 7.11.1'e ek olarak, ilgili ülke veri koruma otoritesini veya ulusal akreditasyon kuruluşunu alanan önlemler hakkında derhal yazılı olarak bilgilendirmesi gerekir.

Sertifikasyon kuruluşu, akreditasyon ve sertifikasyon ile ilgili olarak tüm belgeleri eksiksiz, anlaşılır, güncel ve denetime uygun bir halde tutmalıdır.

Sertifikasyon kuruluşu GDPR m.43(2)(d) ve ISO/IEC 17065/2012 madde 7.13.1'e ek olarak, kimlerin şikayet veya itirazda bulunabileceğini, sertifikasyon kuruluşu adına

bu şikayet ve itirazları kimin alıp değerlendirdiğini, bu bağlamda itiraz edenlerin kimliği ve itiraz konusu ile ilgili hangi doğrulamaların gerçekleştirildiğini ve ilgili taraflarla istişare olanaklarının neler olduğunu belirlemelidir.

4.2.4.5 Yönetim Sistemleri Gereklilikleri

ISO/IEC 17065/2012 Bölüm 8'e göre yönetim sistemi gerekliliği; akredite sertifikasyon kuruluşu tarafından sertifikasyon mekanizmasının uygulanması kapsamında, standardın diğer bölümleri ile GDPR m.42 ve m.43 kapsamındaki tüm gerekliliklerin uygulanmasının belgelendirilmesi, değerlendirilmesi, kontrol edilmesi ve bağımsız olarak izlenmesi anlamına gelmektedir.

Yönetimin temel ilkesi, hedeflerinin etkin ve verimli bir şekilde belirlendiği bir sistem tanımlamaktır. Bu, akreditasyon gerekliliklerinin sertifikasyon kuruluşu tarafından yerine getirilip getirilmediğinin ve devam ettirilip ettirilmediğinin şeffaf ve doğrulanabilir bir şekilde tespitini gerektirir. Bu amaçla, yönetim sistemi, bu gereksinimlerin veri koruma düzenlemelerine uygun olarak sağlanması ve kontrol edilmesi ve bunların akredite kuruluşun kendisi ile sürekli bir şekilde kontrol edilmesi için bir metodoloji belirlemeyi içermelidir.

Bu yönetim ilkeleri ve bunların belgelenmiş uygulaması şeffaf olmalı ve GDPR m.58 atfı ile GDPR m.43 ile düzenlenen akreditasyon prosedürü uyarınca ve sonrasında veri koruma otoritesinin talebi üzerine herhangi bir zamanda, bir denetim icra edildiğinde akredite sertifikasyon kuruluşu tarafından gösterilebilmelidir.

GDPR m.58(1)(b) veya m.58(1)(c) kapsamında akredite sertifikasyon kuruluşu, hangi sertifikasyonun hangi temelde (veya sertifikasyon mekanizmaları veya şemaları dahilinde) gerçekleştirildiğini, sertifikasyonun hangi çerçeve ve koşullarda ne kadar süreyle geçerli olduğunu, kamuoyuna açıklamak zorundadır.

Sertifikasyon kuruluđu, sertifikasyon yöntemlerinin güncellenmesine rehberlik edecek prosedürler oluřturmalıdır. Güncelleme, yasal çerçevedeki değışiklikler, ilgili risklerdeki değışiklikler, teknolojideki gelişmeler ile teknik ve idari tedbirlerdeki değışiklikler şeklinde ortaya çıkabilir.

Sertifikasyon kuruluşları, yukarıdaki paragrafta belirtildiğı üzere meydana gelebilecek gelişmeleri dikkate alarak, yetkinliklerini sürekli güncel tutmak amacıyla çalışanlarının eğitimlerini ve mesleki gelişimlerini sağlamak ve aynı zamanda kullandığı teknik ve idari araçları da güncel tutmak zorundadır.

Sertifikasyon kuruluşu ile müşterileri arasındaki iletişim için uygun prosedürlerin ve iletişim yapılarının uygulanması gereklidir. Bu uygulama bir başvurunun durumu hakkında bilgiyi, ilgili veri koruma otoritesi tarafından yapılan değerlendirmeleri, geri bildirimleri ve ilgili veri koruma otoritesinin kararlarını içermelidir.

Akreditasyonun askıya alınması veya geri alınması durumunda uygulanacak prosedürler, müşteri bildirimleri de dahil olmak üzere sertifikasyon kuruluşunun yönetim sistemine entegre edilmelidir.

4.2.5 Sertifikasyon Gereklilikleri

4.2.5.1 Genel Olarak

Sertifikasyon mekanizmaları, veri sahipleri için ve veri koruma otoriteleri için şeffaflığı arttırabilir. GDPR'ın Resital kısmında (100) numaralı bendde sertifikasyon mekanizmalarının oluřturulmasının şeffaflığı ve GDPR ile uyumluluğı artırabileceğini ve veri sahiplerinin ilgili ürün ve hizmetlerin veri koruma düzeyini değerlendirmesine imkan tanıyabileceğı belirtilmiştir.

GDPR m.42(3) uyarınca sertifikasyon, GDPR'a uyumluluğun gösterilmesine yardımcı olan, gönüllülük esasına dayalı bir süreçtir. GDPR ile üye Devletler ve veri koruma otoriteleri, sertifikasyon mekanizmalarının kurulması için teşvik edilmektedir.

Ayrıca, onaylanmış sertifikasyon mekanizmalarına bağlılık, GDPR m.83.2(j) uyarınca denetim makamlarının idari para cezası vermeye karar verirken ve para cezasının miktarına karar verirken ağırlaştırıcı veya hafifletici bir faktör olarak dikkate alması gereken bir unsurdur.

4.2.5.2 Akreditasyon ve Sertifikasyon Rehberlerinin Niteliği

GDPR'ın akreditasyon ve sertifikasyon sistemine ilişkin olarak çıkarılan rehberler kapsamı sınırlı olan rehberlerdir ve GDPR kapsamındaki akreditasyon ve sertifikasyon için prosedürel bir rehber niteliğinde değildirler. Bu rehberlerin ana amacı, GDPR'ın 42 ve 43. maddeleri uyarınca düzenlenen her tür sertifikasyon mekanizmasıyla ilgili olabilecek çerçeve niteliğindeki gereklilikleri ve kriterleri belirlemektir. Bu nedenle rehberler bir hesap verebilirlik aracı olarak sertifikasyonun gerekçesini ortaya koymak, 42 ve 43. maddelerdeki akreditasyon ve sertifikasyona dair düzenlemelerdeki temel kavramları açıklamak, 42 ve 43. maddeler kapsamında nelerin sertifikasyona tabi olabileceğinin kapsamını ve sertifikasyonun amacını açıklamak ve sertifikasyon sonucunun anlamlı, açık ve sertifika verenden bağımsız olarak karşılaştırılabilir olmasını kolaylaştırmak durumundadır.

Bu sayede kurulacak akreditasyon ve sertifikasyon sistemi için adım adım sistemin kuruluşunu anlatan prosedürel kılavuzlar değil, ancak genel çerçeveyi veren birer araç niteliğindedirler ve hukuki olarak kanaatimizce ancak bir yorum aracı olarak görülebilirler. Yoksa doğrudan yaptırım gücü olan hukuki düzenlemeler olarak görülmeleri kanatimizce mümkün değildir.

GDPR, her ne kadar bir Tüzük olarak üye ülkelerde doğrudan uygulanması gereken bir hukuki düzenlemedir. Avrupa Birliği'nde direktifler, üye ülkeler için sadece bir çerçeve çizer ve bu çerçeve kapsamında düzenleme yapma özgürlüğü tanır. Ancak regülasyonlar, tüm AB çapında doğrudan uygulanması zorunlu olan düzenlemelerdir²²⁴. Ancak her ne kadar GDPR bir tüzük olsa da akreditasyon ve sertifikasyon sisteminin detaylarının düzenlenmesi iç hukuklara tabidir. Rehberler, bu kapsamda GDPR'ın 42 ve 43. maddelerindeki hükümlerin yorumlanması ve uygulanması ile ilgili tavsiye niteliğinde dökümanlardır ve Üye Devletlere, veri koruma otoritelerine ve ulusal akreditasyon kuruluşlarına yol göstermede yardımcı olma fonksiyonuna sahiptirler. Rehberler ile böylece GDPR uyarınca sertifikasyon mekanizmalarının uygulanması için birlik ölçeğinde daha tutarlı ve uyumlu bir yaklaşım oluşturması amaçlanmaktadır.

Rehberlerde yer alan tavsiyeler, GDPR Madde 42(5), Madde 58(3)(f) ve Madde 70(1)(o) kapsamındaki sertifikasyon kriterlerini onaylarken yetkili veri koruma otoriteleri ve Avrupa Veri Koruma Kurulu ("EDPB"), GDPR Madde 42(5) uyarınca onay için ilgili ülkenin veri koruma otoritesine sunulmadan önce sertifikasyon kriterlerini hazırlarken ve revize ederken sertifikasyon kuruluşları, GDPR Madde 42(5) ve 70(1)(o) kapsamında bir Avrupa Veri Koruma Mührünü onaylarken EDPB, kendi sertifikasyon kriterlerini hazırlarken ilgili ülke veri koruma otoriteleri, GDPR Madde 43(8) kapsamında sertifikasyon mekanizmaları için dikkate alınması gereken gereklilikleri belirlemek amacıyla kendisine tevdi edilmiş yetkiler kapsamında Avrupa Komisyonu, Madde 70(1)(q) ve Madde 43(8) uyarınca sertifikasyon gereklilikleri hakkında Avrupa Komisyonu'na bir görüş sunarken EDPB, sertifikasyon kuruluşlarının ISO/IEC

²²⁴ CRAIG, Paul/DE BURCA, Grainne: EU Law: Text, Cases, and Materials, Oxford University Press, Oxford, 2020, s.108-110.

17065/2012 uyarınca akreditasyonu için sertifikasyon kriterlerini ve Madde 43 uyarınca ek gereklilikleri dikkate alması gereken ulusal akreditasyon kuruluşları ve kendi GDPR uyumluluk stratejilerini tanımlarken ve sertifikayı uyumluluğu göstermenin bir yolu olarak değerlendirirken veri sorumluları ve veri işleyenler tarafından dikkate alınacaktır.

4.2.5.3 Sertifikasyon ile GDPR Uyumluluğu Arasındaki İlişki

GDPR Madde 42(1)'de sertifikasyon mekanizmalarının veri sorumluları ve veri işleyenler tarafından işleme operasyonlarının bu Tüzüğe uyumluluklarının gösterilmesi amacıyla kurulacağı belirtilmektedir.

GDPR kapsamında, veri sorumlularının ve veri işleyenlerin; GDPR Madde 24(1),(3), 25 ve 32(1), (3)'te atıfta bulunulan uygun teknik ve idari tedbirlerin uygulanması ve gösterilmesinde, GDPR Madde 28(5)'in 1. (veri işleyenden veri sorumlusuna) ve 4. paragraflarında atıfta bulunulan yeterli garantilerin gösterilmesi (alt veri işleyenden veri işleyene) gibi yükümlülüklerine uyumluluklarını göstermek için, onaylanmış sertifika mekanizmaları bir unsur olarak kullanılabilecektir.

Şu hususu vurgulamakta özel yarar vardır; sertifikasyon kendi başına hiçbir zaman bir veri sorumlusunun veya veri işleyenin GDPR ile tam uyumlu olduğunu kesin bir biçimde kanıtlamaz. Sertifikasyon ile hukuki anlamda, sertifikasyonu almış olan veri sorumlusunun veya veri işleyenin GDPR'a uyumlu olduğu noktasında bir karine meydana gelir. Bu hukuki karinenin meydana gelebilmesi tüm sertifikasyon sürecinin şeffaf bir şekilde yürütülebilmesine bağlıdır. Uygunluğun gösterilmesi, destekleyici belgeleri, özellikle kriterlerin sadece tekrar etmekle kalmayıp aynı zamanda nasıl karşılandığını ve başlangıçta karşılanmadıysa, düzeltmeleri ve düzeltici eylemleri ve bunların uygunluğunu açıklayan yazılı raporları gerektirir. Böylece sertifikasyonun verilmesi ve sürdürülmesi için de gerekli gerekçe sağlanmış olunur.

4.2.5.4 GDPR Kapsamında Kişisel Verilerin Korunmasında Sertifikasyon

Kavramı

GDPR, sertifikasyonu tanımlamamaktadır. ISO, sertifikasyonun evrensel bir tanımını “söz konusu ürün, hizmet veya sistemin belirli gereksinimleri karşıladığının bağımsız bir yazılı güvence (sertifika) kuruluşu tarafından sağlanması” olarak tanımlamaktadır. Sertifikasyon aynı zamanda "üçüncü taraf uygunluk değerlendirmesi" olarak da bilinir ve sertifikasyon kuruluşlarına "uygunluk değerlendirme kuruluşları" (CAB'ler) da denilmektedir. ISO/IEC ISO 17065'in atıfta bulunduğu 17000:2004'te “Uygunluk Değerlendirmesi” yani sertifikasyon şu şekilde tanımlanmaktadır: *“ürünler, süreçler ve hizmetlerle ilgili üçüncü taraf onayı”*. Onay, incelemenin ardından verilen bir karara dayalı olarak, belirli gerekliliklerin yerine getirildiğinin kanıtlandığı bir beyandır²²⁵.

GDPR'ın 42 ve 43. maddeleri kapsamındaki sertifikasyon bağlamında, sertifikasyon, veri sorumluları ve veri işleyenler tarafından kişisel verileri işleme faaliyetleriyle ilgili üçüncü taraf onayına atıfta bulunmaktadır.

GDPR, sertifikasyon ile ilgili bir tanım yapmadığı gibi, “sertifika mekanizmaları”, “kişisel veri mühürleri veya işaretleri” için de bir tanım yapmamıştır. Sertifika, uygunluk beyanıdır. Sertifikasyon prosedürünün başarıyla tamamlandığını belirtmek için bir mühür veya işaret kullanılabilir. Mühür veya işaret, genellikle varlığı (bir sertifikaya ek olarak) sertifikasyon konusunun bir sertifikasyon prosedüründe bağımsız olarak değerlendirildiğini ve düzenlemeler, standartlar veya teknik özellikler kapsamında getirilen gerekliliklere uygun olduğunu gösterir.

²²⁵ ISO/IEC 17000:2004 Standardı için: <https://www.iso.org/standard/29316.html>, ISO 17000:2004 Standardı Bölüm 5.2., (e.t. 23.10.2023).

GDPR kapsamında sertifikasyon bağlamındaki bu gereklilikler, EN-ISO/IEC 17065/2012'de sertifikasyon kuruluşlarının akreditasyon kurallarını ve ilgili ülke veri koruma otoritesi veya Kurul tarafından onaylanan sertifikasyon kriterlerini tamamlayan ek gerekliliklerde belirtilmiştir. GDPR kapsamındaki bir sertifika, mühür veya işaret, yalnızca akredite bir sertifikasyon kuruluşu veya ilgili ülke kişisel verileri koruma kurulu tarafından sertifikasyon kriterlerinin karşılandığını belirten bağımsız bir kanıta dayanan değerlendirmenin ardından verilebilir.

4.2.5.5 GDPR Kapsamındaki Sertifikasyonda İlgili Ülke Veri Koruma Otoritelerinin Rolü

GDPR m.42(5), sertifikasyonun akredite bir sertifikasyon kuruluşu veya ilgili ülke veri koruma otoritesi tarafından verileceğini düzenlemektedir. GDPR, sertifikaların düzenlenmesini veri koruma otoritelerinin zorunlu bir görevi haline getirmemektedir. Bunun yerine, GDPR bir dizi farklı modele izin vermiştir. Bir ülkenin veri koruma otoritesi kendi sertifikasyon düzenlemesine göre sertifikasyonu kendisinin vermesine, kendi sertifikasyon düzenlemesine göre sertifikasyonu kendisinin yapmasına, ancak değerlendirme sürecinin tamamının veya bir kısmının üçüncü taraflara devredilmesine, kendi sertifikasyon düzenlemesini oluşturmaya ve sertifikasyonu düzenleyen sertifikasyon prosedürünün uygulanmasının sertifikasyon kuruluşlarına bırakılmasına ve piyasayı sertifikasyon mekanizmaları geliştirmeye teşvik etmeye karar verebilir.

Buna göre her ilgili ülke veri koruma otoritesi, GDPR kapsamında sertifikasyon sisteminin kurulması için hangi yaklaşımın benimseneceğini belirleyecektir. Bu, yalnızca GDPR2ın 57 ve 58. maddelerindeki görev ve yetkiler bağlamında değil, aynı zamanda yapılacak olan sertifikasyonun idari para cezalarının belirlenmesinde dikkate alınması

gereken bir unsur olarak ve daha genel olarak da uyumu gösterme aracı olarak hesap verebilirlik ilkesi bağlamında değerlendirilecektir.

4.2.5.6 Sertifikasyon Kuruluşu Olarak Veri Koruma Otoritesi

Bir veri koruma otoritesinin kendisinin sertifikasyonu yapmayı seçtiği durumlarda, GDPR kapsamında kendisine verilen görevlerle ilgili olarak rolünü dikkatli bir şekilde değerlendirmesi gerekecektir. Rolü, işlevlerini yerine getirirken şeffaf olmalıdır. Herhangi bir olası çıkar çatışmasını önlemek için denetime ve yürütmeye ilişkin güçler ayrılığını özellikle dikkate alması gerekecektir.

İlgili ülke veri koruma otoritesi, bir sertifikasyon kuruluşu olarak hareket ederken, bir sertifikasyon mekanizmasının mevcut yasal düzenlemelere uygun şekilde kurulmasını sağlaması ve kendi sertifikasyon kriterlerini geliştirmesi gerekmektedir. Ek olarak, sertifikaları düzenleyen her veri koruma otoritesinin, GDPR m.57(1)(o) kapsamında sertifikaları periyodik olarak gözden geçirme görevi ve GDPR m.58(2)(h) kapsamında, sertifika gereksinimlerinin karşılanmadığı veya gerekliliklerin karşılanmasının devam ettirilemediği durumlarda sertifikaları geri alma yetkisi vardır. İlgili ülke veri koruma otoritesi bu gereksinimleri karşılamak için, bir sertifikasyon prosedürü ve süreç gereklilikleri oluşturmak ve mevzuatta aksi belirtilmedikçe, başvuru sahibi kuruluşla sertifikasyon faaliyetlerinin sağlanması için de daha önce belirtildiği şekilde bir sertifikasyon sözleşmesi yapmak durumundadır.

Bu sertifikasyon sözleşmesinin, başvuru sahibinin, değerlendirmenin yapılması için gerekli düzenlemeler, kriterlere uyumun izlenmesi ve bilgi ve/veya tesislere erişim, dokümantasyon, raporların yayınlanması, şikayetlerin ele alınması, değerlendirilmesi, sonuçlandırılması ve periyodik gözden geçirme dahil olmak üzere sertifikasyon sürecine dair başvuran taraf yükümlülüklerini mutlaka içermesi gerekir. Ayrıca, bir veri koruma

otoritesi, GDPR m.43(2) uyarınca gerekliliklere ek olarak, sertifikasyon kuruluşlarının akreditasyonu için rehberlerdeki gereklilikleri de yerine getirmesi gerekir.

Sertifikasyon kuruluşlarının faaliyete geçtiği üye devletlerde, veri koruma otoritesi kendi faaliyetlerinden bağımsız olarak GDPR Madde 42(5) uyarınca bir sertifikasyon programının kriterlerini değerlendirmek, sertifikasyon kriterlerini GDPR Madde 64(1)(c), 64(7) uyarınca onaylamak ve Kurul'un görüşünü Madde 64(1)(c) ve 70(1)(t) kapsamında almak, GDPR Madde 58(3)(f), Madde 42(5) ve 43(2)(b) kapsamında akreditasyon ve sertifikasyon gerçekleşmeden önce sertifikasyon kriterlerini onaylamak, GDPR Madde 43(6) uyarınca sertifikasyon kriterlerini yayınlamak, GDPR Madde 42(5) ve Madde 70(1)(o) kapsamında EDPB onaylı Avrupa Veri Koruma Mühürleri ile sonuçlanabilecek AB çapında sertifikasyon programları için yetkili makam olarak hareket etmek, GDPR Madde 58(2)(h) uyarınca bir sertifikasyon kuruluşuna sertifikasyon yapmamasını emretmek veya sertifikasyon gerekliliklerinin karşılanmadığı veya gerekliliklerin karşılanmasının devam ettirilemediği durumlarda sertifikasyonun geri alınmasına karar vermek yetkilerine sahiptir.

GPDR, veri koruma otoritelerine sertifika kriterlerini onaylama görevi vermiştir. GDPR m.42(5) kapsamında sertifikasyon kriterlerini onaylamak için, bir veri koruma otoritesinin, özellikle GDPR'a uygunluğun gösterilmesine yönelik kapsam ve içerik açısından ve bunları izleme ve uygulama göreviyle ilgili olarak ne beklenmesi gerektiği konusunda net bir anlayışa sahip olması gerekir.

Sertifikasyon kuruluşlarının, ilgili ülke veri koruma otoritesinin GDPR m.58(2)(h) bendi kapsamında düzeltici yetkilerini kullanabilmesi için GDPR m.43(1) kapsamında sertifikasyonları düzenlemeden veya yenilemeden önce ilgili ülke veri koruma otoritesini bilgilendirmeleri gerekir. Ek olarak, GDPR m.43(5) ayrıca,

sertifikasyon kuruluşlarının, ilgili ülke veri koruma otoritesince talep edilen sertifikasyonu verme veya geri alma nedenlerini açıklamayı da zorunlu kılmaktadır.

GDPR, veri koruma otoritelerinin bu bilgilerin operasyonel olarak nasıl alınacağını, onaylanacağını, inceleneceğini ve ele alınacağını belirlemesine izin verse de, sağlanan bilgileri ve raporları işlemek için gerekli süreç ve kriterler GDPR m.43(1) kapsamında sertifikasyon kuruluşu tarafından gösterilmelidir.

Bu bilgilere dayanarak, veri koruma otoritesi, GDPR m.58(2)(h) kapsamında sertifikasyon kuruluşuna bir sertifikasyonu yapmamasını veya yapılmış olanı geri çekmeyi emretme ve GDPR m.57(1)(a) ve 58(2)(h) kapsamında sertifikasyon gerekliliklerinin ve kriterlerinin uygulanmasını izleme yetkisini kullanabilir. Böylece, farklı sertifikasyon kuruluşları tarafından, sertifikasyon süreçlerinde uyumlaştırılmış bir yaklaşım yakalanabilecek ve bir kuruluşun sertifikasyon durumu hakkındaki bilgilerin AB kapsamında ilgili ülke veri koruma otoriteleri tarafından bilinmesini ve takip edilmesi sağlanabilecektir.

4.2.5.7 Sertifikasyon Kuruluşunun Rolü

Bir sertifikasyon kuruluşunun rolü, GDPR m.43(1) uyarınca bir sertifikasyon mekanizması ve GDPR m.42(5)(7) kapsamında onaylanmış kriterler temelinde sertifikasyon yapmak, gözden geçirmek, yenilemek ve geri almaktır. Bu, sertifikasyon kuruluşunun uyumun izlenmesi, gözden geçirilmesi, şikayetlerin ele alınması ve sertifikasyonun geri alınması için prosedürler dahil olmak üzere sertifikasyon kriterlerini ve sertifikasyon prosedürlerini belirlemesini ve oluşturmasını gerektirmektedir.

Sertifikasyon kriterleri, GDPR m.43(2)(c) uyarınca sertifikaların, mühürlerin veya işaretlerin verildiği kuralları ve prosedürleri dikkate alan akreditasyon sürecinin bir parçası olarak gözden geçirilir. Sertifikasyon kuruluşunun 43. madde kapsamında

akredite olabilmesi için yukarıda da izah edildiği üzere bir sertifikasyon mekanizmasının ve sertifikasyon kriterlerinin ortaya konulmuş olması gerekir. Belirli kriterler, örneğin, yerinde incelemeler ve kod incelemesi gibi belirli değerlendirme yöntemlerini gerektirebilir. Bu prosedürler akreditasyon için zorunludur ve akreditasyon rehberlerinde ayrıntılı olarak açıklanmıştır.

Sertifikasyon kuruluşunun GDPR m.42(7), 43(5) ve 58(2)(h) kapsamında veri koruma otoritelerine, özellikle sertifikasyon mekanizmasının uygulanmasını izlemek için gerekli olan sertifikalar hakkında bilgi vermesi gerekir.

4.2.5.8 Sertifikasyon Kriterlerinin Onaylanması

Sertifikasyon kriterleri, herhangi bir sertifikasyon mekanizmasının ayrılmaz bir parçasını oluşturur. Sonuç olarak GDPR m.42(5) ve 43(2)(b) ilgili ülke veri koruma otoritesi tarafından bir sertifikasyon mekanizmasının ve sertifikasyon kriterlerinin onaylanmasını gerektirir. Bir Avrupa Veri Koruma Mührünün söz konusu olması durumunda, sertifikasyon kriterleri GDPR m.42(5) ve 70(1)(o) uyarınca EDPB tarafından onaylanır. EDPB'nin bu onayı GDPR'da belirtilen kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunmasına ilişkin gereklilikleri ve ilkeleri gerektiği gibi yansıtmak ve GDPR'ın tutarlı bir şekilde uygulanmasına katkıda bulunmak amaçlarını gütmektedir.

Sertifikasyon kriterlerinin onayı, onay mekanizmasının, veri sorumlularının ve veri işleyenlerin GDPR ile uyumluluğunun sertifikasyon kriterlerini tam olarak yansıttığını göstermesi durumunda verilmelidir.

Sertifikasyon kriterleri, bir sertifikasyon kuruluşunun akreditasyon süreci öncesinde veya akreditasyon süreci esnasında ilgili ülke veri koruma otoritesi tarafından onaylanmalıdır. ISO 17065 kapsamında güncellenmiş veya ek düzenlemeler veya kriter

setleri için, GDPR m.42(5) ve 43(2)(b) kapsamında değiştirilmiş sertifikasyon mekanizmalarını kullanmadan önce de bu sertifikasyon kuruluşu için onay gereklidir. Veri koruma otoriteleri, sertifikasyon kriterlerinin onaylanmasına ilişkin tüm talepleri, yerine getirilmesi gereken genel koşulları ve onay sürecinin tanımını belirleyen, kamuya açık bir prosedüre göre adil ve ayırım gözetmeyen bir şekilde ele almalıdırlar.

Bir sertifikasyon kuruluşu, yalnızca belirli bir Üye Devlette, o Üye Devletteki veri koruma otoritesi tarafından onaylanan kriterlere uygun olarak sertifikasyon yapabilir. Diğer bir deyişle, sertifikasyon kuruluşunun sertifikasyonu sunmayı amaçladığı ve akreditasyonu aldığı durumlarda sertifikasyon kriterlerinin ilgili ülke veri koruma otoritesi tarafından onaylanması gerekmektedir.

Bir sertifikasyon kuruluşu, bir Avrupa Veri Koruma Mührü için EDPB tarafından onaylanan kriterlere uygun olarak da sertifikasyon yapabilir. EDPB tarafından GDPR m.63 uyarınca onaylanan sertifikasyon kriterleri, GDPR m.42(5) kapsamında bir Avrupa Veri Koruma Mührü ile sonuçlanabilir.

EDPB tarafından GDPR m. 42(5) ve 70(1)(o) uyarınca veri sorumlularına ve veri işleyenlere yönelik bir sertifikasyon mekanizmasındaki kriterlerin onaylanması için yapılacak başvuru, bir veri koruma otoritesi aracılığıyla sunulmalı ve bu başvuru program sahibi, aday veya akredite sertifikasyon kuruluşunun bu kriterleri onaya sunmasına dair niyetini belirtmelidir. İlgili ülke veri koruma otoritesi, başvuruya konu kriterlerin EDPB tarafından onaylanabileceğini düşündüğünde EDPB'ye bununla ilgili bir taslak sunmalıdır.

Kriterlerin onaylanması için başvurunun nereye yapılacağı, sertifikasyon programı sahiplerinin veya sertifikasyon kuruluşlarının genel merkezinin bulunduğu yere göre belirlenecektir.

4.2.5.9 Avrupa Veri Koruma Mührü Kriterleri

Avrupa veri koruma mühürleri ile ilgili kriterler için EDPB, kriterlerin değerlendirme sürecini koordine edecek ve kriterleri uygun görürse Avrupa Veri Koruma Mührü kriterlerini onaylayacaktır. EDPB'nin yapacağı değerlendirmede kriterlerin kapsamını ve ortak bir sertifikasyon işlevi görme yeteneğini değerlendirecektir. Kriterlerin EDPB tarafından onaylandığı durumlarda, sertifikasyon kuruluşunun AB merkezi için veri koruma otoritesinin, mekanizmanın kendisiyle ilgili şikayetleri ele alması ve diğer veri koruma otoritelerini bilgilendirmesi beklenmektedir. Bu veri koruma otoritesi ayrıca sertifikasyon kuruluşuna karşı önlem almaya da yetkilidir. Duruma göre, yetkili veri koruma otoritesi diğer veri koruma otoritelerini ve EDPB'yi bilgilendirecektir.

Ortak bir sertifikasyona yönelik sertifikasyon kriterleri AB çapında yapılacak taleplere tabidir ve bu talepleri ele almak için özel bir mekanizma sağlamalıdır. Avrupa sertifikasyon mekanizmalarının tüm Üye Devletlerde kullanılması amaçlanmalıdır. GDPR m.42(5)'e dayanarak, bir Avrupa Veri Koruma Mührü mekanizmasının yanı sıra onun kriterleri, gerekli olduğu durumlarda ulusal sektöre özel düzenlemeleri de dikkate alacak şekilde özelleştirilebilir olmalıdır.

Örneğin Birlik içindeki veri sahiplerine eğitim hizmetleri sunan uluslararası bir okul, “A” Üye Devletinde bulunmaktadır. Okul, bir Avrupa Veri Koruma Mührü kazanmak için çevrimiçi başvuru sürecini AB çapında bir sertifika programıyla onaylamak istemektedir. Bu okul, Avrupa Veri Koruma Mührü temelinde “B” Üye Devletinde kurulmuş bir sertifikasyon kuruluşu tarafından sunulan veri işleme faaliyetlerinin sertifikasyonu için başvurmayı amaçlamaktadır. İlgili mekanizmada tasarlanan ve belgelenen mühür kriterleri, “A” Üye Devletinde geçerli olan okullara yönelik düzenlemeleri de gözönüne almalıdır. Kriterler ayrıca, diğer Üye Devletlerde

farklılık gösterebilecek, ders notları veya test sonuçları, farklı saklama süreleri, finansal veya biyometrik verilerin toplanması veya işlenmesi gibi hususlara yönelik Üye Devlet veri koruma gerekliliklerini de dikkate almalıdır.

Avrupa Veri Koruma Mührü mekanizmasının onaylanması için üst düzey kriterler, Kurul tarafından onaylanan kriterleri, ulusal yasal gereklilikleri, sektöre özel düzenlemeleri yansıtan uygulama gerekliliklerini, ulusal gereklilikleri yansıtacak şekilde özelleştirilebilen uyumlaştırılmış kriterleri, Avrupa çapındaki gereklilikleri tanıyan sertifikasyon sözleşmelerini, ulusal farklılıkların giderilmesine yönelik prosedürleri ve mührün GDPR uyumluluğunun gösterilmesine yardımcı olmasını sağlamaya yönelik prosedürleri içermektedir.

Kriterlerin ortak sertifikasyon için uygun olduğu belirlendiğinde ve GDPR m.42(5) uyarınca Kurul tarafından bu şekilde onaylandığında, sertifikasyon kuruluşları bu kriterler kapsamında AB düzeyinde sertifikasyon yapmak üzere akredite edilebilirler. Yalnızca belirli Üye Devletlerde sunulması amaçlanan programlar ise AB düzeyinde veri koruma mührü adayı olmayacaktır.

Bir Avrupa Veri Koruma Mührü kapsamındaki akreditasyon, programı işletmek isteyen diğer Üye Devletlerdeki kuruluşların ve yan kuruluşlarının sertifikasyon faaliyetleri, sertifikasyon kuruluşunun genel merkezinin bulunduğu Üye Devlette akreditasyonunu gerektirecektir. Diğer kuruluşların veya yan kuruluşların sertifikaları özerk olarak yönettiği ve icra ettiği durumlarda, bu kuruluş veya yan kuruluşların her biri, bulundukları Üye Devlette ayrı akreditasyona ihtiyaç duyacaktır. Başka bir deyişle, akreditasyon, yalnızca sertifikasyon kuruluşunun merkezinin bulunduğu Üye Devlette, yalnızca merkezin sertifika düzenlediği durumlar için geçerlidir. Buna karşılık,

sertifikasyon kuruluşunun diğer kuruluşları da merkezden bağımsız olarak sertifika verdiğinde, bu kuruluşların da akredite olması gerekir.

Sonuç olarak, bir sertifikasyon kuruluşu Avrupa Veri Koruma Mührü kapsamında sertifikasyon için akredite edilmemişse, EDPB onaylı kriterler kullanılamaz ve AB Veri Koruma Mührü verilemez.

4.2.6 Sertifikasyon Kriterlerinin Geliştirilmesi

GDPR, sertifikasyon kriterlerinin geliştirilmesine yönelik çerçeveyi oluşturmuştur. Sertifikasyon prosedürüne ilişkin temel gereklilikler Madde 42 ve 43'te belirtilmiştir. Aynı zamanda sertifikasyon prosedürleri için temel kriterler GDPR ilke ve kurallarından türetilmeli ve bunların yerine getirildiğine dair de güvence sağlamalıdır.

Sertifikasyon kriterlerinin geliştirilmesi, GDPR ile uyumu göstermek için sertifikasyon kriterlerinin doğrulanabilirliğine, önemine ve uygunluğuna odaklanmalıdır. Sertifikasyon kriterleri açık ve anlaşılır olarak ve pratik uygulamaya izin verecek şekilde formüle edilmelidir.

Sertifikasyon kriterlerinin taslağı hazırlanırken, diğerlerinin yanı sıra, veri işleme faaliyetlerinin değerlendirilmesini desteklemek için GDPR Madde 6 uyarınca veri işleme şartları, Madde 5 uyarınca veri işleme ilkeleri, Madde 12-23 uyarınca veri sahiplerinin hakları, Madde 33 uyarınca veri ihlallerini bildirme yükümlülüğü, Madde 25 uyarınca mahremiyet tasarımı ve varsayılan olarak mahremiyet (PbD)²²⁶ yükümlülüğü, zorunlu olduğu durumlarda GDPR m.35(7)(d) uyarınca bir veri koruma etki analizi yapma yükümlülüğü ve GDPR m.32 uyarınca teknik ve idari tedbirleri alma yükümlülüğü dikkate alınmalıdır.

²²⁶ MAGGI/RECUPERO, s.28.

Bu hususların kriterlere ne ölçüde yansıtıldığı, veri işleme faaliyetlerinin tipini ve sertifikasyon alanını (örneğin bankacılık sektörü) içerebilen sertifikasyon kapsamına bağlı olarak değişebilir.

EDPB, odak noktası, veri sorumluları ve veri işleyenler tarafından veri işleme faaliyetlerinin GDPR'a uyumunun gösterilmesine yardımcı olmak olduğu sürece, GDPR'da yer alan düzenlemelerin, GDPR kapsamında onaylanabilecekler için geniş bir kapsam sağladığını düşünmektedir.

Bir veri işleme faaliyetini değerlendirirken kişisel veriler, kişisel verileri işlemek için kullanılan donanım ve yazılım gibi teknik altyapı ve veri işleme faaliyetleri ile ilgili süreçler ve prosedürler dikkate alınmalıdır.

Veri işleme faaliyetlerinde kullanılan her unsur, belirlenen kriterlere göre değerlendirmeye tabi olmalıdır. Bu noktada veri sorumlusunun veya veri işleyenin hukuki niteliği, veri işleme faaliyetlerinde yer alan departmanlar ve kişiler ile veri işlemenin yapıldığı ortamlar, değerlendirilecek unsurların teknik tanımı, işletim sistemleri, sanal sistemler, veri tabanları, kimlik doğrulama ve yetkilendirme sistemleri, yönlendiriciler ve güvenlik duvarları, depolama sistemleri, iletişim altyapısı veya internet erişimi ve ilgili teknik tedbirler de dahil olmak üzere veri işleme faaliyetlerinin gerçekleştirildiği bilgi teknolojileri altyapısı gibi unsurlar değerlendirmeye tabi tutulmalıdır.

GDPR m.42.7 düzenlemesinden, GDPR kapsamındaki sertifikaların yalnızca veri sorumlularına ve veri işleyenlere verildiği, örneğin veri koruma görevlilerinin sertifikasyonunun bu düzenlemeye dahil olmadığı anlaşılmaktadır. GDPR m.43(1)(b), ürünlerin, hizmetlerin ve süreçlerin uygunluğunu değerlendiren sertifikasyon kuruluşlarının akreditasyonunu sağlayan ISO 17065'e atıfta bulunmaktadır. Bir veri işleme faaliyeti veya bir dizi işlem, ISO 17065 kapsamına giren bir ürün veya hizmeti

oluşturabilir ve bu ürün veya hizmet sertifikasyona konu olabilir. Örneğin, çalışan verilerinin maaş ödemesi veya izin yönetimi amacıyla işlenmesi, GDPR anlamında bir dizi işlemdir ve ISO 17065 kapsamına giren bir ürün, süreç veya hizmetle sonuçlanabilir.

Bu değerlendirmeler temelinde, EDPB, GDPR kapsamındaki sertifikasyon kapsamının veri işleme faaliyetlerine yönelik olduğu düşüncesindedir. Bunlar, kurumsal önlemler anlamında, bir veri işleme operasyonunun ayrılmaz parçaları olarak yönetim süreçlerinden oluşabilir (örneğin, maaş ödemesi amacıyla çalışan verilerinin işlenmesinin bir parçası olarak şikayetlerin ele alınması için oluşturulan yönetim süreci).

İşleme operasyonunun sertifikasyon kriterlerine uygunluğunu değerlendirmek için bir gerçek hayat senaryosu kurgulanmalıdır. Örneğin, bir işleme operasyonunda konuşlandırılmış bir teknik altyapının kullanımının uygunluğu, işlemek için tasarlandığı veri kategorilerine bağlıdır. İdari tedbirler, işlemenin niteliği, kapsamı, içeriği ve amaçları ile veri sahiplerinin hak ve özgürlüklerine yönelik riskler dikkate alınarak, veri kategorilerine ve miktarına ve işleme için kullanılan teknik altyapıya bağlıdır.

Ayrıca, bilgi teknolojileri uygulamalarının aynı işleme amaçlarına hizmet etmesine rağmen büyük farklılıklar gösterebileceği gözden uzak tutulmamalıdır. Bu nedenle, sertifikasyon mekanizmalarının kapsamı tanımlanırken ve sertifikasyon kriterleri hazırlanırken bu husus mutlaka dikkate alınmalıdır. Sertifikasyon ve kriterlerin kapsamı, farklı tasarlanmış bilgi teknolojileri uygulamalarını dışlayacak kadar dar olmamalıdır.

Bir sertifikasyon mekanizmasının kapsamı genel olarak veya belirli bir işleme faaliyeti türü veya alanı ile ilgili olarak tanımlanabilir ve bu nedenle, sertifikasyon mekanizmasının kapsamına giren sertifikasyon nesnelerini önceden tanımlayabilir.

Her durumda, güvenilir ve anlamlı bir uyum değerlendirmesi, ancak bir sertifikasyon sürecinin münferit konusunun tam olarak tanımlanması durumunda gerçekleşebilir. Sertifikasyon konusuna hangi veri işleme faaliyetlerinin dahil olduğu ve ardından temel bileşenlerin, yani hangi verilerin, süreçlerin ve teknik altyapının değerlendirileceği ve hangilerinin değerlendirilmeyeceği açıkça tanımlanmalıdır. Bunu yaparken, diğer süreçlerin arayüzleri de her zaman dikkate alınmalı ve tanımlanmalıdır.

Bir veri işleme faaliyetinde tüm süreçler ve işlemler şeffaf ve erişilebilir durumda olmalıdır. Aksi takdirde bilinmeyen ya da müphem süreçler ve veri işleme faaliyetleri bir sertifikasyon değerlendirmesine konu olamaz ve bu nedenle de sertifikalandırılmaz. Her durumda, sertifikasyonun üzerinde yapıldığı sertifikasyonun münferit konusu ve bununla ilgili açıklamalar kullanıcıyı, müşteriye veya tüketiciyi yanıltmamalıdır.

Örneğin bir banka, müşterilerine çevrimiçi bankacılık amacıyla bir internet sitesi sunuyor olsun. Bu hizmet çerçevesinde para transferi yapma, hisse satın alma, düzenli ödeme emri verme ve bütün olarak hesabı yönetme imkanı bu internet sitesi üzerinden veriliyor olsun. Banka, genel kriterlere dayalı genel kapsamlı bir veri koruma sertifikasyon mekanizması içinde güvenli oturum açmayı sağlamalıdır. Güvenli bir oturum açılımı ilgili kişisel verilerin güvenliğinin sağlanmasında önemli bir rol oynadığından, son kullanıcıyı ilgilendiren ve veri koruma ile ilgili bir veri işleme faaliyetidir. Bu nedenle, bu veri işlemesi, güvenli oturum açma için zaruridir ve bu nedenle, sertifika yalnızca oturum açma işleme işleminin sertifikalandırıldığını açıkça belirtiyorsa, anlamlı bir değerlendirme hedefi (ToE) oluşturabilir.

İnternet sitesi kullanıcı arayüzünü kontrol eden program bölümü, her ne kadar veri koruma ve bilgi güvenliği açısından önemli ise de, son kullanıcı tarafından anlaşılabilir olmadığı için, sertifikasyon konusu ve kapsamı açısından anlamlı bir ToE olamaz. Ayrıca,

internet sitesinde hangi hizmetlerin ve dolayısıyla hangi işleme işlemlerinin sertifikasyon kapsamında olduğu da aynı şekilde son kullanıcı için net değildir.

Çevrimiçi bankacılıkta kullanıcı arayüzünü kontrol eden program bölümü ile internet sitesinin sadece yazılımcıların erişebildiği yazılım kısmının birlikte oluşturduğu internet bankacılığı sistemi üzerinden yapılan kişisel veri işleme faaliyetleri kullanıcı için anlamlı olabilecek işlemlerdir. Bu bağlamda, her ikisi de ToE'ye dahil edilmelidir. Kara para aklamanın önlenmesi amacıyla yapılan veri işleme faaliyetleri gibi çevrimiçi bankacılık hizmetinin sağlanmasıyla doğrudan bağlantılı olmayan veri işlemleri ise ToE'nin dışında tutulabilir.

Ancak, bankanın internet sitesi aracılığıyla sunduğu çevrimiçi bankacılık hizmetleri, kendi veri işleme faaliyetlerini gerektiren diğer hizmetleri de örneğin bir sigorta ürününün sunulmasını da içerebilir. Bu ek hizmet, çevrimiçi bankacılık hizmetlerinin sağlanması amacıyla doğrudan bağlantılı olmadığı için, kapsam dışında tutulabilir. Bu ek sigorta hizmeti kapsamdan hariç tutulursa, bu hizmetin internet sitesine entegre edilmiş arayüzleri kapsamın bir parçasıdır ve bu nedenle hizmetler arasında net bir ayrım yapmak için açıklanmalıdır. Bu tür bir açıklama, iki hizmet arasındaki olası veri akışlarını belirlemek ve değerlendirmek için gereklidir.

Yine bir örnek üzerinden gidecek olursak; bir banka müşterilerine, çeşitli bankalardan farklı hesaplar ve kredi kartlarıyla ilgili bilgileri toplayarak hesaplarını birleştirmelerine izin veren bir hizmet sunmaktadır. Banka, hizmetinin GDPR kapsamında sertifikalandırılmasını istemektedir. Yetkili veri koruma otoritesi, bu tür faaliyetlere odaklanan belirli bir dizi sertifikasyon kriterini onaylamıştır. Bu örnekte sertifikasyon mekanizması yalnızca kullanıcı doğrulama ve diğer

bankalardan/hizmetlerden toplanacak verileri elde etmenin kabul edilebilir yollarını kapsamaktadır.

Bu sertifikasyon mekanizmasının kapsamı, ToE'yi tek başına tanımladığı için, ToE'yi önerilen kapsam altında anlamlı bir şekilde daraltmak ve yalnızca belirli özellikleri veya tek bir işleme faaliyetinin sertifikasyonu mümkün değildir. Bu senaryoda, değerlendirme yöntemleri ve değerlendirme metodolojisi ele alındığında bir ToE belirli bir kapsama eşit olmalıdır.

Veri işleme faaliyetlerinin uyumluluğunu göstermeye yardımcı olacak bir uyum değerlendirmesi, değerlendirme yöntemlerinin ve değerlendirme metodolojisinin belirlenmesini gerektirir. Değerlendirmeye yönelik bilgilerin sadece dokümantasyondan mı (ki bu tek başına yeterli olmayacaktır) yoksa aktif olarak sahada ve doğrudan veya dolaylı erişim yoluyla mı toplandığı önemlidir. Bilginin toplanma şeklinin sertifikasyon açısından önemli sonuçları vardır ve bu nedenle de toplanma şekilleri tanımlanmalıdır. Sertifikaların düzenlenmesi ve periyodik olarak gözden geçirilmesine yönelik prosedürler, sertifika kriterlerini karşılamak için uygun değerlendirme düzeyini belirlemek için spesifikasyonları, uygulanan değerlendirme yöntemleri ve yerinde denetimler sırasında veya dokümantasyondan toplanan bulgular hakkındaki bilgileri, işleme operasyonlarına (veriler, sistemler, süreçler) ve işleme amacına odaklanan değerlendirme yöntemlerini, veri kategorilerinin, koruma ihtiyaçlarının ve veri işleme faaliyetine sadece veri işleyenlerin mi yoksa üçüncü şahısların da mı dahil olduğunun ve rollerin belirlenmesini, roller ile sorumluluklar etrafında tanımlanan bir erişim kontrol mekanizmasının varlığını içerir.

Değerlendirmenin derinliği, sertifikasyonun önemi ve değeri üzerinde bir etkiye sahiptir. Pragmatik amaçlarla veya maliyetleri azaltmak için değerlendirme derinliğini

azaltmak, bir veri koruma sertifikasının önemini azaltacaktır. Öte yandan, değerlendirmenin ayrıntı düzeyine ilişkin kararlar, başvuru sahibinin mali kapasitesini ve çoğu zaman değerlendirici ve denetçilerin kapasitesini aşabilir. Uyumluluğu göstermek amacıyla, kullanılan bilgi teknolojileri sistemlerinin çok ayrıntılı bir analizini yapmak her zaman çok gerekli ve önemli olmayabilir.

Sertifikasyon belgeleri eksiksiz ve kapsamlı olmalıdır. Belge eksikliği, uygun bir değerlendirmenin yapılamayacağı anlamına gelir. Sertifikasyon belgelerinin temel işlevi, sertifikasyon mekanizması kapsamında, değerlendirme sürecinde şeffaflık sağlamasıdır. Dokümantasyon, hukuki düzenlemelerle belirlenen gerekliliklerle ilgili soruların cevaplarını verir. Sertifikasyon mekanizmaları, standartlaştırılmış bir dokümantasyon metodolojisi sağlamalıdır. Daha sonra değerlendirme, sertifikasyon belgelerinin sahadaki gerçek durumla ve sertifikasyon kriterlerine göre karşılaştırılmasına imkan tanıyacaktır.

Nelerin sertifikalandırıldığına ve kullanılan metodolojiye ilişkin kapsamlı belgeler yukarıda da belirttiğimiz üzere şeffaflığa hizmet eder. GDPR m.43(2)(c) uyarınca, sertifikasyon mekanizmaları, sertifikasyonun gözden geçirilmesine izin veren prosedürler oluşturmalıdır. İlgili ülke veri koruma otoritesinin, resmi soruşturmalarda sertifikasyonun kabul edilip edilemeyeceğini veya ne ölçüde kabul edilebileceğini değerlendirmesine imkan sağlamak için, ayrıntılı belgelerin oluşturulması ve sunulması en uygun yol olabilir. Değerlendirme sırasında hazırlanan belgeler bu nedenle yürütülen değerlendirme yöntemlerinin tutarlılığına, sertifikasyon konusunun sertifikasyon kriterlerine ve dolayısıyla GDPR'a uygunluğunu göstermeye yönelik değerlendirme yöntemlerine ve değerlendirme sonuçlarının bağımsız ve tarafsız bir sertifikasyon kuruluşu tarafından doğrulanmış olmasına odaklanmalıdır.

GDPR’ın Resital kısmının 100 nolu bendi, sertifikasyon ile ulařılmak istenilen hedefler hakkında bilgi vermektedir. Buna gre; “*řeffaflığı ve bu Tzęe uyumu artırmak iin, veri sahiplerinin ilgili rn ve hizmetlerin veri koruma dzeyini hızlı bir řekilde deęerlendirmesine olanak tanıyan sertifikasyon mekanizmalarının ve veri koruma mhrlerinin ve iřaretlerinin oluřturulması teřvik edilmelidir.*”

řeffaflığı artırmak iin sonuların belgelenmesi ve iletilmesi nemli bir rol oynamaktadır. Veri sahiplerine ynelik sertifikasyon mekanizmaları, mhrler veya iřaretler kullanan sertifikasyon kuruluřları, sertifikalı iřleme operasyonları hakkında kolay eriřilebilir, anlařılır ve anlamlı bilgiler saęlamalıdır. Bu halka aık bilgiler en azından ToE’nin aıklamasını, belirli ToE’ye uygulanan onaylanmış kriterlere referansları, kriterlerin deęerlendirilmesi iin uygulanan metodolojiyi (yerinde deęerlendirme, dokmantasyon, vb.), sertifikanın geerlilik sresini, veri koruma otoriteleri ve dięer yetkili otoriteler ve halk iin sonuların karřılařtırılabilirlięini iermelidir.

4.2.7 Sertifikasyon Kriterlerinin Tanımlanması

Sertifikasyon kriterleri, bir sertifikasyon mekanizmasının ayrılmaz bir parasıdır. Sertifikasyon prosedr, belirli bir deęerlendirme konusu veya ToE ile ilgili olarak sertifikasyon srelerinde yer alacak deęerlendirmenin nasıl, kim tarafından, ne lde ve hangi detayda yapılacaęına dair gereklilikleri ierir. Sertifikasyon kriterleri, ToE’de tanımlanan fiili veri iřleme faaliyetlerinin deęerlendirildięi gereklilikleri saęlar. Sertifikasyon kriterlerini tanımlamaya ynelik bu prosedrler, sertifikasyon kriterlerinin deęerlendirilmesini kolaylařtıracak genel tavsiyeler saęlar.

Sertifikasyon kriterlerini onaylarken veya tanımlarken bu kriterler tek tip ve doęrulanabilir olmalıdır. Bu kriterler GDPR kapsamındaki iřleme faaliyetlerinin

değerlendirilmesini kolaylaştırmak için, özellikle amaçları ve bu amaçlara ulaşmak için uygulama kılavuzunu belirterek denetlenebilir olmalıdır. Ayrıca kriterler hedeflenen kitleyle ilgili olmak (örneğin işletmeden işletmeye (B2B) ve işletmeden müşteriye (B2C)) ve diğer standartları (ISO standartları gibi) dikkate alarak bu standartlarla birlikte çalışabilir olmalıdır. Son olarak kriterler GDPR m.42(1) uyarınca mikro, küçük ve orta ölçekli işletmeler de dahil olmak üzere farklı tür ve büyüklükteki kuruluşlara ve GDPR Resital 77. Bend uyarınca risk temelli yaklaşımın uygulanabilmesi için esnek ve ölçeklenebilir olmalıdır.

Örneğin yerel bir perakendeci şirket, genellikle büyük bir çokuluslu perakendeciden daha az karmaşık veri işleme operasyonları yürütecektir. Veri işleme faaliyetlerinin hukuka uygunluğuna ilişkin gereklilikler aynı olmakla birlikte, veri işlemenin kapsamı ve karmaşıklığı dikkate alınmalıdır. Bunun sonucu olarak, söz konusu işleme faaliyetine göre sertifikasyon mekanizmalarına ve bunların kriterlerinin de ölçeklenebilir olmasına ihtiyaç vardır.

Sertifikasyon kuruluşlarının, iyi uygulama rehberleri, teknik standartlar veya ulusal standartlar gibi belirli kriterlerin, mevcut ilgili araçları nasıl dikkate aldığını da göz önüne alması gerekecektir. İdeal olarak, ölçütler, bir veri sorumlusunun veya veri işleyenin GDPR kapsamındaki yükümlülüklerini yerine getirmesine yardımcı olabilecek mevcut standartlarla birlikte çalışabilir olmalıdır. Bununla birlikte, endüstri standartları genellikle kuruluşun tehditlere karşı korunmasına ve güvenliğine odaklanırken, GDPR, bir anayasal hak olarak gerçek kişilerin temel haklarının ve özgürlüklerinin korunmasına yöneliktir. Kriterler tasarlanırken veya kriterler veya endüstri standartlarına dayalı sertifikasyon mekanizmaları onaylanırken bu farklı bakış açısı mutlaka dikkate

alınmalıdır. Ayrıca sertifikasyon kriterleri, bir sertifikasyon mekanizmasının ortaya çıkardığı beklentilerle eşleşmelidir.

Ayrıca sertifikasyonun ismi de ilgili olduğu alanı ve kapsamı belirtecek şekilde olmalıdır. Örneğin "Sağlık Mahremiyeti İşareti" olarak isimlendirilmiş olan bir mekanizma, kapsamını sağlık sektörü ile sınırlandırmalıdır. Mühür adı, sağlık verileriyle bağlantılı veri koruma gereksinimlerinin incelendiği beklentisini artırmaktadır. Buna göre, bu mekanizmanın kriterleri, bu sektördeki veri koruma gereksinimlerini değerlendirmek için yeterli bir şekilde oluşturulmalıdır.

Bu konuda yine başka bir örnek vermek gerekirse, veri işlemede yönetim sistemlerini içeren veri işleme faaliyetlerinin sertifikasyonu ile ilgili bir mekanizma, yönetim süreçlerinin tanınmasına ve değerlendirilmesine izin veren kriterleri ve bunun destekleyici teknik ve idari tedbirlerini tanımlamalıdır.

Ya da bir bulut bilişim hizmeti söz konusu ise, bulut bilişimle ilgili bir mekanizmanın kriterleri, bulut tabanlı hizmetlerin kullanımı için gerekli olan özel teknik tedbirleri hesaba katmalıdır. Örneğin, sunucular AB dışında kullanılıyorsa, kriterler üçüncü ülkelere veri aktarımlarına ilişkin GDPR Bölüm V'de belirtilen koşulların yerine getirilip getirilmediğini mutlaka dikkate almalıdır.

Farklı sektörlerde ve/veya Üye Devletlerde farklı ToE'lere uyacak şekilde tasarlanmış kriterler farklı senaryolara uygulanmaya izin vermelidir. Sonuç olarak, kriterleri tamamlayan sertifikasyon prosedürleri bütün bu ihtiyaçlara cevap vermelidir. Kriterler, uygun teknik ve idari tedbirlerin uygulanması için yeterli garantilerin sağlanıp sağlanmadığına ilişkin bir değerlendirmeyi kolaylaştırmalıdır.

Ancak bu sertifikasyon kriterlerinin de ilanihaye aynen devam edeceğini söylemek, teknolojinin ve ihtiyaçların gelişim hızına bakıldığında mümkün değildir. Bu

nedenle bu kriterler örneğin yasal çerçevenin değişmesi, mahkeme kararları ve teknolojinin gelişimi gibi durumlarda çeşitli değişikliklere tabi olacaktır.

4.2.8 Sertifikasyon Mekanizmasının Kapsamının Belirlenmesi İçin Kriterler

4.2.8.1 Genel Olarak

Bir sertifikasyon faaliyetindeki en önemli konulardan biri sertifikasyon kapsamının belirlenmesidir. Bunun için de çeşitli kriterlerin sertifikasyon başvurusu yapan veri sorumlusunun kişisel verileri işleme süreçlerine uygulanması ve bu uygulama neticesindeki sonuçlara göre sertifikasyona karar verilmesi gerekir. Bu kriterlerden ilki sertifikasyon mekanizmasının kapsamının açıkça tanımlanıp tanımlanmadığıdır. Kapsamın net olarak tanımlanması gerekir, aksi takdirde daha en baştan sertifikasyon talebi reddedilecektir.

Sertifikasyon mekanizmasının kapsamı hitap ettiği hedef kitle için anlaşılır olması gerekir. Örneğin Bir "Güvenilir Şirket Mührü" denildiğinde sanki şirketin tüm süreçleri denetlenmiş ve tüm şirket süreçleri için mühür verilmiş gibi anlaşılmaktadır. Ancak yalnızca belirli işleme operasyonları, örneğin çevrimiçi ödeme süreci aslında sertifika kapsamında incelenmişse kapsam yanıltıcı olacaktır.

Sertifikasyon mekanizmasının kapsamının, veri işleme faaliyetlerinin tüm ilgili yönlerini yansıtmaması gerekir. Örneğin bir "Gizlilik Sağlık İşareti" denildiğinde, bunun sağlıkla ilgili tüm değerlendirme verilerini içermesi ve sağlıkla ilgili veri işleme süreçlerindeki tüm veri koruma gerekliliklerini yerine getiriyor olması gerekir.

Sertifikasyon mekanizmasının kapsamının, ilgili veri işleme faaliyetlerinin niteliğini, içeriğini ve riskini dikkate alarak belirlenmesi gerekir. Örneğin sertifikasyon mekanizmasının kapsamı, yalnızca veri toplama gibi veri işleme süreçlerinin belirli

yönlerine odaklanıyorsa, ancak reklam profilleri oluşturmak amacıyla işleme veya ilgili kişi başvurularının yönetimi gibi sonraki veri işlemlere odaklanmıyorsa bu durum ilgili kişiler için anlamlı olmayacağı gibi riskli de olacaktır. Dolayısıyla hem faaliyetin niteliği açısından hem de bu faaliyetin getirdiği risk açısından kapsamın doğru olarak tanımlanması gerekir.

Sertifikasyon mekanizmasının kapsamının, sadece ilgili başvuru ülkesindeki kişisel veri işlemeyi mi yoksa sınır ötesi işleme ve/veya aktarımları da içerip içermediği mutlaka kapsamda yer almalıdır.

Sertifikasyon kriterlerinin, ToE'nin nasıl tanımlanması gerektiğini yeterince açıklaması gerekir. Örneğin sadece, "sertifikasyona tabi işlemenin bir spesifikasyonunu" gerektiren genel bir kapsam sunan bir "Gizlilik Mührü", bir ToE'nin nasıl oluşturulacağı ve tanımlanacağı konusunda yeterince açıklık sağlamamaktadır. Başka bir örnek vermek gerekirse, güvenli depolamayı ele alan belirli bir kapsamın, "Gizlilik Kasası Mührü" olarak adlandırıldığını varsayalım. Bu mühür için kriterlerin, bu kapsamı karşılamak için gereklilikleri ayrıntılı olarak açıklaması gerekir. Örneğin kasanın tanımı, sistem gereksinimleri, zorunlu teknik ve idari tedbirler gibi. Ancak bu şekilde ayrıntılı açıklamaları içeren bir kapsam, ToE'yi açıkça tanımlayabilecektir.

Kriterlerin, ToE'nin ilgili tüm işleme operasyonlarının bir tanımlamasını, veri akışlarının gösterimini ve ToE'nin uygulama alanının belirlenmesini içermesi gerekmektedir. Örneğin bir sertifikasyon mekanizması, GDPR kapsamında veri sorumlularının veri işleme faaliyetlerinin sertifikalandırılmasını sağlıyorsa, bu mekanizma tarafından kullanılan kriterler, başvuru sahibi veri sorumlusunun, işlenen veri türleri, sistemler ve süreçler açısından hedeflenen işleme operasyonunu (ToE) belirlemesini de içermek zorundadır.

Kriterler, başvuru sahibinden değerlendirmeye tabi işlemin nereden başlayıp nerede bittiğini açıkça belirtmesini ve ToE'nin bir parçası olarak birbirine bağlı işleme operasyonlarının dahil edilmediği arayüzleri de içermelidir. Buna örnek olarak kullanıcıların kaydı, kullanıcılara hizmet sağlanması, faturalandırma, IP adreslerinin günlüğe kaydedilmesi, kullanıcılara ve üçüncü taraflara arayüzler dahil olmak üzere ve sunucu barındırma hariç olmak üzere internet tabanlı bir hizmetin verilmesi gibi bir veri işleme operasyonunu yeterli ayrıntıda açıklayan bir ToE'nin varlığı gösterilebilir.

Kriterler, ToE'lerin, ilgili kişiler de dahil olmak üzere, hedef kitlesi tarafından anlaşılabilir olmasını sağlamalıdır. Yine kriterler, kullanılan tüm ilgili terimleri (yani sertifikasyon kriterlerinin tamamı) tanımlamış, açıklamış olmalı, kapsamla ilgili tüm normatif referansları ve sertifikasyon mekanizması kapsamındaki veri koruma sorumluluklarının, prosedürlerin ve işlemlerin tanımını içermelidir.

4.2.8.2 Veri İşleme Kriterleri

Kapsam belirlendikten sonra artık bu kapsam içinde veri sorumlusu tarafından yapılacak tüm veri işlemlerin de bazı kriterlere tabi tutulması gerekmektedir.

Herşeyden önce sertifikasyon mekanizmasının kapsamı ile ilgili olarak, veri işleme faaliyetlerinin veriler, sistemler ve süreçler ile ilgili tüm bileşenlerinin kriterler tarafından ele alınmış olması gerekmektedir ve bu kriterler, ToE ile ilgili geçerli işleme şartlarının da tanımlanmasını gerektirmelidir. Başka bir deyişle herşeyden önce, bir veri işleme sürecinde bu verilerin hangi işleme şartlarına dayanılarak işlendiğinin veri sorumlusu tarafından gösterilmesi kriterler tarafından şart koşulmalıdır.

ToE ile ilgili olarak, kriterler ilgili işleme aşamalarını ve silme, yok etme ve/veya anonimleştirme dahil olmak üzere verilerin tüm yaşam döngüsünü ele almalıdır. GDPR ile getirilen önemli bir yenilik olarak veri taşınabilirliği konusundaki ToE'ler için de

kriterler belirlenmiş olmalıdır. Yine kriterler ToE ile ilgili olarak, otomatik karar verme, profillemeye, özel nitelikli kişisel verilerin belirlenmesi ve işleme şartları gibi özel türdeki işleme operasyonlarını tanımlamalıdır.

Kriterlerin içermesi gereken en önemli konulardan biri de veri işleme faaliyetlerinin riskinin ve ilgili kişilerin hak ve özgürlüklerinin korunmasının ile ilgili değerlendirmelere yer vermesidir. Böylece temel bir anayasal hak olarak kişisel verilerin korunması hakkının veri sorumluları tarafından ne şekilde kullandırıldığının sertifikasyon sürecinde net olarak tespit edilmesi sağlanabilecektir.

4.2.8.3 Veri Koruma İlkeleri ve İşleme Şartları (GDPR m.5, 6)

Kriterler, bir veri işleme sürecinde en temel olarak, veri sorumlularının veri işleme faaliyetlerinde GDPR'ın orantılı veri işleme, veriyi güncel tutma, meşru amaçlar için veriyi işleme gibi temel ilkelerine uyulup uyulmadığına dair kontrolleri ve bu işlemin yasal dayanaklarını, sözleşmenin ifası meşru menfaat, bir hakkın korunması gibi işleme şartlarını mutlaka içermelidir.

4.2.8.4 Veri Sorumlularının ve Veri İşleyenlerin Genel Yükümlülüklerine Dair Kriterler

Veri sorumlularının iş süreçlerinde kişisel verileri işlerken üçüncü tarafları kullanması durumunda bir veri sorumlusu ile veri işleyen arasındaki ilişki söz konusu olacaktır. Bu nedenle bu iki hukuk süjesi arasındaki veri işleme ilişkisine dair de çeşitli kriterlerin sertifikasyon sürecinde dikkate alınması gerekmektedir.

Kriterler, veri sorumluları ve veri işleyenler arasındaki ilişkinin bir veri işleme sözleşmesine dayanıp dayanmadığını, dayanıyorsa bu veri işleme sözleşmesinin tarafların veri sorumlusu ve veri işleyen olma sıfatlarına dair tüm yükümlülükleri ve yönleri

düzenleyip düzenlemediğini göz önünde tutmalıdır. Bu bağlamda kriterler açık bir şekilde, bu sözleşmelerde veri sorumlularının ve veri işleyenlerin yükümlülüklerinin ele alınıp alınmadığını, bu yükümlülüklerden doğan sorumlulukları, veri işlemede uygulanan teknik ve idari tedbirleri, veri işleme yöntem ve amaçlarını, veri ihlali durumunda yapılacakları, ilgili kişi başvurularının sonuçlandırılmasını, imha sürelerini ve sair veri sorumlusu ve veri işleyen arasındaki ilişkileri ele almalıdır.

Kriterler, veri sorumlularının veya veri işleyenlerin GDPR 37. madde uyarınca bir Veri Koruma Görevlisi (DPO) atamalarının gerekip gerekmediğine dair değerlendirmeleri ve eğer böyle bir gereklilik var ise atanacak olan DPO'nun GDPR'ın 37 ila 39. maddeler kapsamında hangi gereklilikleri kapsaması gerektiğini de içermelidir.

Kriterler, ayrıca Madde 30(5) uyarınca faaliyetlerin işlenmesine ilişkin kayıtların veya başka bir deyişle kişisel veri işleme envanterlerinin tutulmasının gerekli olup olmadığını ve gerekli ise bu kişisel veri işleme envanterlerinin GDPR 30. Madde gerekliliklerini karşılayıp karşılamadığına dair kontrolleri de içermelidir.

4.2.8.5 Veri Sahiplerinin Hakları

Kişisel veri koruma düzenlemelerinin belki de en önemli kısmını verileri işlenen ilgili kişilere tanınan haklar ile bu hakların veri sorumluları ve veri işleyenler tarafından nasıl kullanılacağı oluşturmaktadır. Bu nedenle kriterler, veri sahiplerinin bilgi edinme hakkı başta olmak üzere, kişisel verilere erişim hakkı, veri taşınabilirliği, kişisel verilerin düzeltilmesi, imhası gibi konularda alınması gereken hukuki, teknik ve idari tedbirleri içermelidir.

4.2.8.6 Gerçek Kişilerin Hakları ve Özgürlükleri Açısından Risk Kriterleri

Kriterlerin, gerçek kişilerin hak ve özgürlüklerine yönelik riskin değerlendirilmesinin nasıl yapılacağını içermesi gerekir. Bu kapsamda kriterlerin tanınmış bir risk değerlendirme metodolojisini dikkate alıp almadığına bakılmalıdır. Böyle bir tanınmış risk değerlendirme metodolojisine doğrudan bir atıf yok ise, bu konu muğlak bırakılıyor ise bu kriterler sertifikasyon kriterleri olarak dikkate alınamaz.

Kriterler, risk değerlendirme metodolojisinin yanısıra mahremiyet etki analizi metodolojilerini de içermelidir. Yani sertifikasyon kapsamındaki veri işlemlerin gerçek kişilerin hak ve özgürlükleri üzerindeki etkisinin değerlendirilmesinin ne şekilde yapılacağına dair bir metodoloji de içermelidir. Buna mahremiyet hukuku terminolojisinde veri koruma etki değerlendirmesi (DPIA) denilmektedir. Bu kapsamda etki değerlendirmesi yapıldıktan sonra azaltılamayan, artık riskler varsa bu risklerin de ne şekilde işleneceğine dair kriterler düzenlenmiş olmalıdır.

4.2.8.7 Veri Korumayı Garanti Eden Teknik ve İdari Tedbirler

Kriterler, kişisel veri işleme süreçlerinin gizliliğini, bütünlüğünü ve sürekliliğini sağlayan teknik ve idari tedbirleri ve bunların uygulanmasına ilişkin prosedürleri ve hesap verebilirlik ve ilgili kişilerin haklarının korunabilmesi bakımından kişisel veri işleme süreçlerinin şeffaflığını sağlayan önlemleri kapsamalıdır. Örneğin bir kredi başvurusu değerlendirme sürecinde, otomatik karar alma mekanizmaları ile başvuruya yanıt veriliyorsa, bu otomatik karar alma mekanizmasının algoritmasının şeffaflığı sağlanmalıdır.

Kriterler, aynı zamanda ilgili kişilerin haklarını garanti eden teknik ve idari tedbirlerin alınmasını ve uygulanmasını da içermelidir. Örneğin bilgi alma hakkının kullanılması durumunda bu bilgiyi verebilecek teknik alt yapı olup olmadığına veya veri

taşınabilirliği hakkının kullanılması durumunda bu hakkın gereğini yerine getirebilecek teknik düzenlemelerin yapılıp yapılmadığına bakılmalıdır. Yine kriterler, ilgili kişilerin haklarından olan kişisel verilerin düzeltilmesi veya imha edilmesi için gerekli teknik ve idari tedbirleri de içermelidir.

Kriterler, mahremiyet hukukunun önemli ilkelerinden olan veri minimizasyonu için gerekli olan teknik ve idari tedbirleri ve bunların uygulanmasını içermeli, aynı zamanda mahremiyet hukukunun çok yeni alanlarından biri olan mahremiyet tasarımının uygulanması için gerekli teknik tedbirleri de belirlemelidir.

Bunların yanısıra kriterler, eğitim, mahremiyet uygulamaları yönünden performans takibini, teknik ölçümleri ve bunların periyodik olarak gözden geçirilmesi ve takip edilmesini, mahremiyet yönünden iç denetimi, veri ihlal bildirimlerinin yapılması ve yönetimini, gelişen mahremiyet ve mahremiyetle alakalı teknolojik gelişmelerin izlenmesini ve bu gelişmelere göre veri koruma yönetim sisteminin güncellenmesine dair prosedürleri de kapsamalıdır.

4.2.8.8 Avrupa Veri Koruma Mührü İçin Ek Gereklilikler

Kriterlerin tüm Üye Devletleri kapsamı ve her üye devletin kişisel veri koruma düzenlemelerini dikkate alması gerekmektedir. Bu şekilde birlik kapsamındaki tüm devletlerin düzenlemeleri dikkate alındığında ise bu düzenlemelere uygun ToE'lerin oluşturulması gerekmektedir. Bu tüm AB'ni kapsayıcılığın bir başka sonucu ise, bir Avrupa Veri Koruma Mührü'ne müraccat eden veri sorumlularının veya veri işleyenlerin, ilgili kişilere ve ilgili taraflara Üye Devletlerin dillerinde bilgi verme yükümlülüğü altında olmalarıdır.

Avrupa Veri Koruma Mührü konusunda önemli hususlardan biri de kriterlerin, sertifikasyona güveni tesis etmek üzere, yeterli garantileri sağlamak için sertifikasyon

mekanizmasının kapsamını içermesidir. Örneğin sertifikasyon mekanizmasının kapsamı sağlık verilerini işleme operasyonlarına odaklanıyorsa, derinlemesine bir değerlendirme ve mahremiyet tasarımının uygulanmasını sağlayan kriterler tanımlanarak yüksek düzeyde bir veri koruması garanti edilmelidir.

Kriterlerin, mutlaka sertifikasyon mekanizması kapsamında ele alınan kişisel veri işleme operasyonunun büyüklüğü, bilginin hassasiyeti ve işleme riskini dikkate alması gerekir. Bir başka deyişle her veri sorumlusu veya veri işleyene aynı şekilde yaklaşılamaz. Çeşitli kriterlere göre değerlendirmeler yapılmalı, orantılılık gözetilmelidir.

Son olarak kriterler, veri sorumlularının ve veri işleyenlerin GDPR düzenlemelerine uyumluluğunu iyileştirmeye yönelik olmalıdır.

4.2.9 Europrivacy Sistemi

4.2.9.1 Europrivacy Sistemi Nedir²²⁷?

Europrivacy, GDPR ve GDPR'ı tamamlayıcı ulusal veri koruma regülasyonları kapsamında gerçekleştirilen her türlü kişisel veri işlemenin hukuka uygunluğunu değerlendirmek ve belgelemek için EDPB tarafından bir sertifikasyon mekanizması olarak kurgulanmıştır. Tüm AB üye devletlerinde resmi olarak tanınan tek GDPR sertifikasyonu olarak karşımıza çıkmaktadır.

²²⁷ Europrivacy sistemi için: https://www.europrivacy.org/en/resource,https://edpb.europa.eu/system/files/2022-10/edpb_opinion_202228_approval_of_europrivacy_certification_criteria_as_eu_data_protection_seal_en.pdf , (e.t. 16.3.2024)

Avrupa Sertifikasyon ve Gizlilik Merkezi (ECCP), Europrivacy sertifikasyon şeması yönetimi ve lisanslama sürecinden sorumludur. ECCP, Europrivacy Uluslararası Uzmanlar Kurulu'nun desteğiyle şema sahibi olarak görev üstlenmiştir.

Lüksemburg'da bulunan ECCP, veri koruma ve sertifikasyon alanlarındaki yenilikçi teknolojileri ve çözümleri desteklemeyi amaçlamaktadır. Bir dizi Avrupa araştırma projesinin bir sonucu olarak kurulmuştur. Aynı zamanda veri koruma ve sertifikasyon alanlarında uluslararası araştırma ve yeniliği destekleme konusunda doğrudan faaliyet göstermektedir.

ECCP, veri koruma, siber güvenlik ve bilgi teknolojileri uygunluk testleri ve etiketlemesinde uzmanlığı bir araya getirmekte ve birleştirmektedir. Uluslararası ortaklarının ekosistemi tarafından desteklenmektedir ve bu ortaklar, ECCP'nin gelişimine ve hizmetlerine doğrudan katkıda bulunmaktadır. Bu ortaklar Lüksemburg Üniversitesi SECAN Laboratuvarı, İtalya Mahremiyet Enstitüsü, IoT Lab, Archimede Çözümleri ve IPv6 Forumdan müteşekkildir.

Europrivacy sertifikasyonu GDPR madde 42 ve 43'e dayanmaktadır. Yukarıda sertifikasyon sistemini açıklarken belirttiğimiz üzere tam uyumluluğu garanti etmediği gibi otoriteler tarafından verilebilecek cezaları da ortadan kaldırmamaktadır. Bu kapsamda veri sorumluları ve veri işleyenler hem genel olarak uyum süreçlerine olan bağlılıklarını hem de uyum sürecindeki aktif eylemlerini gösterebilmek adına sertifikasyonu almak istemektedir.

Europrivacy sertifikası, akredite edilmiş sertifika kuruluşları tarafından verilir. Sertifika, geçerli ISO/IEC 17065 ve 17021-1 ilkeleriyle uyumludur. Dokümantasyon incelemesi, örnekleme analizi, teknik testler, teftişler ve mülakatlar gibi çeşitli metodolojileri birleştirmektedir.

4.2.9.2 Sertifikasyon Kapsamı

GDPR, kuruluşların, ürünlerin veya hizmetlerin değil direkt olarak kişisel veri işleme faaliyetlerinin sertifikalandırılmasını yapmaktadır. Bu nedenle bir çatı olarak Europrivacy, veri sorumluları ve veri işleyenlerin seçilmiş veri işleme faaliyetlerinin GDPR ile uyumlu olduğunu kanıtlayan göstergedir.

Sertifikasyon için seçilen işleme faaliyetleri, Değerlendirme Hedefi veya “ToE” olarak adlandırılmaktadır.

4.2.9.3 Sertifikasyon Aşamaları

Sertifikalandırma aşaması hazırlık aşaması, bağımsız sertifikasyon aşaması ve geçerlilik aşaması olmak üzere üç ayrı aşamadan oluşmaktadır.

4.2.9.3.1 Hazırlık Aşaması

Sertifika alabilmek için herşeyden önce başvuru yaparak mahremiyet hususlarındaki bağlılığın (çalışmaların vb.) gösterilmesi gerekir. Sonrasında, sertifika başvurusu yapan veri sorumlusu veya veri işleyeninin faaliyetlerinin yürürlükteki yasal düzenlemelere uygun olduğunu göstermesi, GDPR düzenlemelerini ölçülebilir gerekliliklere çeviren Europrivacy kriterlerinin karşılandığını kanıtlamak için Değerlendirme Hedefi (ToE) ile ilgili tüm gerekli belgeleri ve materyalleri sunması ve sertifikasyon kapsamını tanımlaması ve sertifika süreci için bir sertifikasyon kuruluşu ile sözleşme yaparak sertifikasyon planının oluşturulması gerekmektedir.

Kişisel veri işleme faaliyetlerinin temel GDPR kriterlerini karşılaması gerekmektedir (Örneğin; aktarımlar, üçüncü taraflarla ilişkiler, kişisel verilerin işlenmesine ilişkin ilkelere uygunluk vb.). Bu aşamada ulusal gereklilikler belirlenerek

kuruluşun uygunluğu Ulusal Yükümlülük Uygunluk Değerlendirme Raporu (NOCAR) ile sunulmalıdır.

Belirli durumlarda (özel nitelikli kişisel verilerin veya son teknoloji işleme faaliyetlerinin mevcut olması durumunda) ek kriterler uygulanabilmektedir. Bu aşamada, bulunan sektörde kişisel veri koruma alanındaki düzenlemelerin ve AB dışı kuralların detaylıca incelenmesi gerekebilir. Söz konusu süreç kapsamında Europrivacy kriterlerine uygunsuzluklar belirlenerek giderilmelidir.

4.2.9.3.2 Bağımsız Sertifikasyon Aşaması

Bu aşamada bağımsız bir sertifikasyon kuruluşu, ToE'lerin tüm kriterler ile uygunluğunu denetleyecektir. Eğer bir uygunsuzluk tespit edilirse sertifikasyon kuruluşunun denetçisi bir kereye mahsus olmak üzere belge değişimi için zaman tanıyabilmektedir²²⁸. Uygunsuzlukların giderilmesinin ardından sertifikasyon kriterlerinin karşılandığı kararı verilerek uygunluk sertifikasyonu tanımlanır ve çevrimiçi olarak resmi sicilde yayınlanır.

Sertifikasyon kuruluşu, kanıt ve bulguları kaydederek raporlaştırır. Sertifikasyon başvurusu yapan kuruluşlar, ilgili sertifikasyon kuruluşuna ve denetçisine, elde ettiği bilgi ve belgeleri saklaması ve arşiv faaliyetlerini yürütmesi adına açık rıza vermiş sayılır.

²²⁸ Birtakım bulgular sertifikasyon sürecini etkileyebilir. EIPACC Term and Conditions metninde önemli uygunsuzluk olarak nitelendirilen durumlarda sertifikasyon süreci iptal edilebilir veya ertelenebilir. Sertifikasyon kuruluşu, sürecin bir kısmını veya bazı durumlarda tamamını tekrarlamak zorunda kalabilir. Sertifikasyon kuruluşu belgelerde değişiklik olduğu takdirde yine de kabul etmeme hakkına sahiptir. Önemli (majör) uygunsuzluklar: Sürecin ilgili kriterleri karşılamadığına dair makul şüphe ve birtakım küçük uygunsuzlukların bir araya gelmesi durumudur. Küçük uygunsuzluk: Program gerekliliklerini ve sertifikalandırma kabiliyetini majör bir şekilde etkilemeyen uygunsuzluklardır. Normatif kapsam: Tamamlayıcı ulusal regülasyonlar ve/veya sektöre özgü düzenlemelerin sertifikasyon sürecinde bir bütün olarak değerlendirilmesidir.

4.2.9.3.3 Geçerlilik

Europrivacy sertifikaları üç yıl süreyle geçerlidir ve yıllık denetimler ile izlenmektedir. Sertifikanın verilmesini müteakip 12 ay içerisinde bir denetim ve 24 ay içerisinde bir denetim daha gerçekleştirilir.

4.3 Türk Hukukunda Kişisel Verilerin Korunmasında Akreditasyon ve Sertifikasyon ile İlgili Düzenlemeler

Türk hukukunda tezin yazım tarihine kadar GDPR m.42 ve 43 ile düzenlendiği şekilde veri sorumlularının ve veri işleyenlerin akreditasyonu ve sertifikasyonu ile ilgili bir düzenleme bulunmamaktadır. Mevcuttaki tek düzenleme gerçek kişilerin sertifikasyonu ile ilgilidir. Bu nedenle bu kısımda Kişisel Verileri Koruma Kurumu’nun “Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkındaki Tebliğ”i ele alınacaktır.

4.3.1 Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ

Kişisel Verileri Koruma Kurumu, Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ ile veri koruma görevlilerine ilişkin düzenleme yapmış ve Tebliğ kapsamında veri koruma görevlilerinin sertifikasyon sürecini düzenlenmiştir.

6 Aralık 2021 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Tebliğ, Kurum tarafından yetkilendirilen Personel Belgelendirme Kuruluşları tarafından yürütülecek sertifikasyon faaliyetleri ile veri koruma görevlileri ve adayları hakkında düzenlemelere yer vermektedir.

4.3.1.1. Personel Belgelendirme Kuruluşu

Tebliğ'in m.4/1-g bendi uyarınca Kuruluş, *“Türk Akreditasyon Kurumu tarafından (TS) EN ISO/IEC 17024 standardı ²²⁹ kapsamında akredite edilen, sertifikasyona ilişkin ilgili sınavlarda başarılı olanları belgelendirmeye yetkili kuruluş”* olarak tanımlanmıştır.

Kurum yayımladığı programın sertifikasyon kuruluşları tarafından akreditasyon başvurusu aşamasında kullanabilmesi için, Kurum'un program kullanma onayından sonra sözleşme imzalaması gerektiği ve kuruluşun programı Kurum tarafından yayımlanan güncel haliyle değişiklik yapmadan kullanmasının zorunlu olduğu düzenlenmiştir. Sertifikasyon kuruluşunun sözleşmenin imzalanmasından itibaren 6 ay içinde sözleşme ile TÜRKAK'a akreditasyon başvurusunda bulunmadığı durumda sözleşmenin hükümsüz hale geleceği belirlenmiştir. TÜRKAK tarafından akreditasyonu geri çekilen sertifikasyon kuruluşunun, bu durumu üç gün içinde Kurum'a bildirmesinin zorunlu olduğu, akreditasyonun geri çekilmesi veya sertifikasyon faaliyetine yönelik niteliği ve yeterliği ile ilgili olarak Kuruma sunulan bilgi ve belgelerin gerçeğe aykırı olduğunun tespiti ya da programın kapsamının dışında sertifikasyon faaliyetlerinin yürütüldüğünün anlaşılması hallerinde personel sertifikasyon kuruluşunun yetkilendirilmesinin Kurum tarafından iptal edileceği belirtilmiştir.

Tebliğ m.5/2 uyarınca sertifikasyon kuruluşunun sertifikasyon faaliyeti esnasında tarafsız ve şeffaf bir şekilde faaliyetlerini yürütmesi, faaliyetleri esnasında sorun yaşanmaması adına gerekli ve yeterli personele, fiziki, teknik ve idari altyapıya sahip olması gerekir.

²²⁹ ISO/IEC17024, Personel sertifikasyonu yapan veya yapmak isteyen kuruluşlarda aranan şartları ortaya koymak, yetkinliklerini sertifikalandırmak, kuruluşun uygulamalarını güvenilir, tutarlı ve karşılaştırılabilir olmasını sağlamak için hazırlanmış bir uluslararası standarttır: <https://www.iso.org/standard/52993.html> , (e.t. 16.3.2024).

4.3.1.2 Veri Koruma Görevlisi

Tebliğ'in m.4/1-n bendi uyarınca Veri Koruma Görevlisi (VKG) *“sınavda başarılı olarak VKG unvanını kullanmaya hak kazanan gerçek kişi”* olarak tanımlanmıştır. Sınavı kazanıp VKG sıfatını haiz olan gerçek kişi Tebliğ uyarınca *“kişisel verilerin korunması mevzuatı açısından yeterli bilgiye sahip olduğu kabul edilir.”* Kuruluş tarafından yapılacak değerlendirme sürecinde başarı sergilemeyen aday, katılım belgesi almaya hak kazanacaktır ancak katılım belgesi *“VKG unvanını kullanma ve VKG olarak faaliyet gösterme imkânı”* sağlamamaktadır.

VKG atanması mevzuatımız kapsamında henüz bir yükümlülük olarak düzenlenmemiş olup, Veri Sorumlusu'nun veya Veri İşleyen'in bünyesinde VKG istihdam etmesi, Veri Sorumlusu ve Veri İşleyen'in mevzuat kapsamındaki sorumluluklarını ortadan kaldırmayacaktır.

Tebliğ'in 14. maddesi uyarınca VKG, sertifikayı geçerlilik süresi olan 4 yıl boyunca kullanabilecek Kurum tarafından kurulacak ve yönetilecek Sertifika Takip ve Doğrulama Bilgi Sistemi (“SERTABİS”) ile kamuya açık bir şekilde sertifikasyon sürecine ilişkin gerekli bilgilendirmeler yapılarak sertifikasyon faaliyetinin tarafsız, şeffaf ve etkin bir şekilde sürdürülmesi temin edilecektir.

4.3.1.3 DPO ve VKG

10 Aralık 2021'de, Kurum tarafından yapılan duyuruda, VKG Sertifikası verilecek kişilerin, GDPR'da bahsi geçen ve görev, yetki ve sorumlulukları tanımlanan Veri Koruma Görevlisi (Data Protection Officer) tanımını karşılamadığı; VKG Sertifikası sahibi kişiler ve Tüzük'te yer alan DPO'nun aynı görev ve yetkilere sahip olmadığı belirtilmiştir.

4.3.2 Veri Koruma Görevlisi Belgelendirme Programı

Kurum'un 10 Aralık 2021 tarihli duyurusunda, Programın detaylarına ilişkin açıklamada bulunulmuştur. Buna göre, katılım belgesine sahip kişilerden sınavda başarılı olanların (100 puan üzerinden 70) Veri Koruma Görevlisi Sertifikası almaya hak kazanacağı; bu kişilerin, sertifika sayesinde, kişisel verilerin korunması mevzuatı açısından yeterli olduklarının kabul edileceği düzenlenmiştir. Ancak, sınav tarihinden önceki son dört yıl içerisinde Katılım Belgesi almış veya başvuru tarihinde geçerli bir VKG Sertifikasına sahip kişilerin sınava başvurabileceği belirtilmiştir. Yine ayrıca yapılacak teorik sınav kurallarına ilişkin usul ve esasların da düzenlediği görülmektedir.

Sertifika sahibi olan VKG'nin, Personel Sertifikasyon Kuruluşu tarafından bazı durumlarda söz konusu belgesi askıya alınabilir ve/veya iptal edilebilir. Bu durumlar Tebliğ'de şu şekilde sayılmıştır:

- gerekli koşullardan birini taşımamak
- gerçeğe aykırı beyanda bulunmak,
- belgeyi kötü amaçla veya yanıltıcı bir biçimde kullanmak

Sözkonusu tespitler, VKG hakkında bildirilen şikayetin değerlendirilmesi sonrasında Kurum veya ilgili mahkeme tarafından yapılabilir.

Sınavların en geç sınavdan onbeş gün önce akredite edilmiş Kuruluş tarafından ilan edilmesi gerektiği, yurt içindeki üniversitelerin veya diploma denkliği Yükseköğretim Kurulu tarafından onaylanmış olmak kaydıyla yabancı üniversitelerin, en az dört yıllık lisans eğitimi veren fakültelerinden mezun olanlardan sınav tarihinden önceki son dört yıl içerisinde Katılım Belgesi almış olan veya geçerli bir sertifika sahibi olan kişilerin bu sınavlara başvuru yapabileceği düzenlenmiştir.

4.3.3 VKG'ye İlişkin Düzenlemelerin İptali Hakkında Başvuru

Türkiye Barolar Birliği, Kişisel Verileri Koruma Kurumu tarafından yayımlanan Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ ile VKG Belgelendirme Programı'nın yürütmesinin durdurulması ve iptali istemiyle Danıştay'a başvurmuş bulunmaktadır.

TBB yapmış olduğu başvuruya, dört yıllık lisans eğitimi veren fakültelerden mezun olanların VKG olmasına imkan sağlayan bu düzenlemelerin, 1136 Sayılı Avukatlık Kanununun "Yalnız avukatların yapabileceği işler" başlıklı 35. maddesine aykırı olmasını ve hukuki danışmanlık yapma, hukuki işlemleri takip etme, dava açma ve savunma yetkisinin sadece avukatlara verilmiş olmasını dayanak yapmıştır. Kişisel Verileri Koruma alanının bir hukuk disiplini olması nedeniyle, VKG adı altında avukat olmayan kişilerce hukuki danışmanlık hizmeti verilmesinin açıkça Avukatlık Kanunu'na aykırılık teşkil ettiği ileri sürülmüştür.

4.3.4 Akreditasyon ve Sertifikasyon Sistemi Hakkında Türkiye Özelinde Değerlendirme ve Öneriler

Cumhurbaşkanlığı 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun uygulanmasında en çok ortaya çıkan sorunları dikkate alarak 2021'de kişisel verilerin korunmasına ilişkin politik hedefleri somut olarak belirlemiştir. İnsan Hakları Eylem Planı ve Uygulama Takviminde Kişisel Verilerin İşlenmesinde Özel Hayatın Korunması başlığı altında "Kişisel Verilerin Korunması Kanunu, Avrupa Birliği standartları ile uyumlu hale getirilecektir." hedefi ve aynı doğrultuda, Ekonomi Reformları Eylem Planı'nda "AB Genel Veri Koruma Tüzüğü'nün (GDPR) yurt dışına veri aktarılmasına yönelik hükümleri esas alınarak Kişisel Verilerin Korunması Kanununda gerekli

değişiklikler yapılacaktır.” hedefi belirlenmiştir. Bu hedeflerle ilgili olarak Adalet Bakanlığı görevlendirilmiş ve bu eylemin bitiş tarihi de 31.03.2022 olarak belirlenmiştir.

Ancak bu hedefler verilen sürelerde gerçekleştirilmemiştir. Daha sonra yapılan Orta Vadeli Plan’da (OVP) konu tekrar ele alınmıştır. OVP’de İş ve Yatırım Ortamını iyileştirme başlığı altında Uluslararası Normlara Uygun, Şeffaf ve Öngörülebilir Düzenlemeler alt başlığında *“Mal ve hizmet ihracatını etkileyen yönleriyle AB dijital ekonomi düzenlemeleri doğrultusunda, Kişisel Verilerin Korunması Kanunu (KVKK) ’nın Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) başta olmak üzere AB müktesebatına uyum süreci tamamlanacaktır. Doğrudan yatırımlar açısından aciliyet taşıyan hususlarda düzenlemeler daha erken gündeme alınacaktır.”* hedefi koyulmuş ve takvim olarak 2024 yılının dördüncü çeyreği belirlenmiştir²³⁰. Nihayet 8. Yargı Paketi reformu olarak gündeme gelen 2.3.2024 tarihli ve 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunla (“KVKK Reform Yasası”) ile KVKK’nın 6, 9, ve 18. maddelerinde kapsamlı değişiklikler yapılmıştır²³¹.

Yapılan bu değişiklikler ile GDPR’a tam bir uyum amaçlanmamış, tabiri caizse kangren hale gelmiş olan yurtdışına veri aktarımı, özel nitelikli kişisel verilerin korunması ve başvurulacak yargı yoluna dair değişiklikler ile bu alanlardaki sorunların çözümlenmesi amaçlanmıştır. Dolayısıyla akreditasyon veya sertifikasyon sistemine herhangi bir şekilde yer verilmemiştir. Oysa akreditasyon ve sertifikasyon sistemi aynı zamanda bir yurtdışı veri aktarımı yöntemi olarak da değerlendirilmektedir²³². Dolayısıyla Kanun’da bu değişiklikler yapılırken ve yurtdışı aktarım da ele alınmışken

²³⁰ KAYA, Mehmet Bedii: KVKK Reformu 2024 Değişiklikleri, Dijital Baskı v1.0, Mart, 2024, s.4 vd.

²³¹ KAYA, s.5.

²³² Sertifikasyon sisteminin bir veri aktarım mekanizması olarak kullanılması ile ilgili Avrupa Veri Koruma Otoritesi 07/2022 tarihli bir Rehber yayınlamıştır: https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf , (e.t.: 16.3.2024

akreditasyon ve sertifikasyon sistemi bir yurtdışı veri aktarım mekanizması olarak düşünülmeyle düzenlemenin dışında bırakılmıştır. Bu durumda yapılması planlanan kapsamlı deęişiklik ile akreditasyon ve sertifikasyon sisteminin düzenleme altına alınacağı tarafımızca düşünülmektedir.

Yapılan bu son deęişiklikte de görüldüğü gibi Türkiye, özellikle AB ile aynı düzeyde kişisel verilerin korunması için çaba sarf etmektedir. Bu kapsamda bir akreditasyon ve sertifikasyon sisteminin kurulmasının AB ile uyumlu bir kişisel verilerin korunması düzeyinin temin edilmesi için kaçınılmaz olduğu tarafımızca düşünülmektedir. Bu sistemin uygulanmasının en önemli faydası Türkiye'nin AB başta olmak üzere dünya ile tam uyumlu bir kişisel verilerin korunması rejimi uyguladığının bir göstergesi olması ve bu sayede de ülkelerin alacakları yeterlilik kararlarına pozitif etki yapacak olmasıdır. Böylece Türkiye'nin ve Türk girişimcilerinin dünya ile entegrasyonu daha da kolaylaşacak, dünyanın en büyük ekonomik faaliyet alanı olan veri ekonomisi alanında hak ettiği yeri almasına yardımcı olunacaktır.

Bu kapsamda, GDPR'da öngörüldüğü üzere bir akreditasyon kuruluşu olarak örneğin TÜRKAK akreditasyon kriterlerini belirleyip, sertifikasyonu yapacak firmaların seçiminde, görevlerini yerine getirmelerinde ve uygulamanın nasıl yapılacağı konusunda gerekli düzenlemeleri yapabilir. Böylece tezimizde savunduğumuz sert çekirdekli bir temel hak olarak kişisel verilerin korunmasına hakkına halel gelmemek kaydıyla, veri sorumluları hangi çerçeve içinde neler yapmaları gerektiğine, ne şekilde hareket etmeleri gerektiğine ve doğabilecek sorumluluklarına dair somut bir çerçeve elde edebileceklerdir. Bu sayede idarenin keyfi hareket etmesinin önüne geçilebilecek ve hukuki güvenlik ilkesi de garanti altına alınabilecektir.

5. HUKUKİ GÜVENLİK İLKESİ

5.1 Genel Olarak Hukuk Devleti Kavramı ve Hukuki Güvenlik İlkesi ile İlişkisi

Hukuki güvenlik ilkesi kavramını incelemeye başlamadan önce hukuk devleti kavramını ele almak gerekir. Hukuk devleti kavramı, tarihsel olarak sırasıyla mülk devleti ve polis devleti anlayışlarını takiben Kara Avrupası'nda Fransız Devrimi sonrasında ortaya çıkmıştır²³³. Almanya'da "Rechtstaat", Fransa'da "Etat de droit" kavramları ve Anglo – Sakson ülkelerde de "Rule of law" yani Türkçe'ye "hukukun üstünlüğü veya hukukun hükümlerliği" olarak çevrilebilecek kavramlarla ifade edilmektedir²³⁴. Hukuk devleti, devletin egemenlik unsurunun teknik ifadesiyle kamu kudretinin meşru ve dengeli organlara verilmesi anlayışının bir ürünüdür. Hukuk devletinde kurumlar ve idare hukuka tabidir²³⁵.

Demokratik ve liberal devletlerde, iktidarın hukuk kurallarına bağlı olmasına dair düzenlemeler yapılmasındaki amaç, yöneticilerin keyfi hareketlerini engellemektir. Hukuki bakış açısından bakıldığında, hangi işlemlerin hangi organlar tarafından yapılacağını ifade eden güçler ayrılığı ilkesi, hakların ve özgürlüklerin yargı bağımsızlığı ile güvenceye alınmasına dair olan hukuk devletinin zeminini oluşturmaktadır. Bu bakımdan, hukuk devletinde kuralların kademelenmesi zorunlu olup, kural olarak hiçbir işlemin denetimsiz kalmaması temel bir ilkedir²³⁶.

²³³ GÖZÜBÜYÜK, A. Şeref/TAN, Turgut: İdare Hukuku, Cilt 1: Genel Esaslar, Turhan Kitabevi, Güncelleştirilmiş 6. Bası, Ankara 2008, s. 38.

²³⁴ ATAY, Ender Ethem: İdare Hukuku, Turhan Kitabevi, Ankara 2019, s.87., GÖZLER, Kemal/KAPLAN, Gürsel: İdare Hukuku Dersleri, Ekin Yayınevi, Güncellenmiş 20. Baskı, Bursa 2018, s.61.

²³⁵ ATAY, "Anayasa Hukuku", s.167.

²³⁶ TEZİÇ, s.162.

Bu kavram, en özet tanımı ile vatandaşların hukuki güvenlik içinde bulundukları, devletin eylemlerinin ve işlemlerinin hukuk kurallarına tabi olduğu bir sistemi ifade eder²³⁷.

Hukuk devleti, yürürlükteki hukuk normlarının açık bir şekilde bilinebildiği ve kurallara riayet etmenin hukuki yaptırımlar ile sağlandığı bir sistemdir. Hangi tür ve biçimde olursa olsun, hiçbir hukuki işlem, hukuki denetimin dışında bırakılamaz. Hukuk kuralı fikri, hukuki güvenlik prensibinin gereklerine cevap verebilecek, açık, belirli bir çerçeve oluşturma, insanların hareketlerinin sonuçlarını öngörme gibi özellikleri ortaya koymalıdır. Hukuk devleti kavramı, idare edilenlere hukuki güvenlik tesis eden devlet düzenini ifade eder. Hukuk devletini, polis devletinden ayıran başlıca hususiyet, devlet görevlerinin belli hukuk kuralları içinde icra edilmesidir²³⁸. Keyfiliğin karşıtı olarak hukuki güvenlik, hukuk devletinin temel bir gereği olarak ortaya çıkar²³⁹.

Hukuki güvenlik ilkesi, hukuk devleti modeline dayalı devletlerde ortak bir özellik oluşturur ve bu da onun normlar hiyerarşisinde özel bir yere sahip olmasını açıklar. Bu anlamda, 'hukuki güvenlik sadece hukukun özgün bir niteliği değil, modern toplumların aksiyomatik bir gerçeği, hukuk devletinin dogmatik bir önermesi değil, aynı zamanda çoğu hukuk düzeni tarafından benimsenen ve uygulanan bir prensiptir²⁴⁰.

Buna göre hukuk devletinin unsurları şu şekilde gösterilebilir²⁴¹:

- Devletin hukuka ve demokratik bir anayasaya uygunluğunu sağlayan ilkeler ve kurallar,

²³⁷ ÖZBUDUN, s.124.

²³⁸ GÖZÜBÜYÜK/TAN, s.38.

²³⁹ KABOĞLU, s.18.

²⁴⁰ HARDY, Hélène: Le principe de sécurité juridique au sens du droit de la Convention européenne des droits de l'homme Droit", Université Montpellier 2019, s.64., <https://tel.archives-ouvertes.fr/tel-02890546>, (e.t. 18.2.2024)

²⁴¹ TANÖR/YÜZBAŞIOĞLU, s.116

- Bu uygunluğu pekiştirecek yargı denetimi
- Bu denetimin etkin bir şekilde yapılabilmesi için yargı bağımsızlığı
- Adil yargılama ilkesinin gerektirdiği güvenceler

Hukuk devleti ile hukuki güvenlik arasındaki ilişki yapısal ve amaçsal olmak üzere iki kısma ayrılabilir²⁴². Yapısal ilişki hukuki güvenliğin, hukuk devleti prensibinin bir alt ilkesi olarak ele alınabilmesini ifade eder. Başka bir ifadeyle hukuk devletinin asgari şartları içinde, genel olarak hukuki güvenlik ilkesi de bulunmaktadır. Bu iki ilkenin arasındaki amaçsal ilişki ise, iki ilkenin amaçlarının temelde devleti hukuk ile sınırlandırarak bireyleri korumaya yönelik amaca dayanmaktadır²⁴³.

5.2 Hukuki Güvenlik İlkesinin Tanımı

AİHM, Fransızca kararlarında “la securité juridique”, İngilizce kararlarında ise çoğunlukla “legal certainty” ifadesini, Alman “rechtssicherheit” teriminin İngilizce çevirisinde yine “legal certainty” ifadesini kullanmıştır. Fakat “legal uncertainty” ve “legal security” ifadesini de kullanmaktadır. Mahkemenin Türkçe kararlarında ilke, hukuk güvenliği/hukuki güvenlik ve hukuki kesinlik, yasal kesinlik, yargı güvencesi terimleri ile ifade edilmiştir. Yabancı doktrinde ilke, “legal certainty”, “legal indeterminacy”, “legal security”, “legal uncertainty”, “legal determinacy”, “uncertainty in law/ uncertainty”, “legal insecurity”, “legal complexity” terimleri ile dilbilimsel farklı kavramlarla ifade edilmektedir²⁴⁴.

²⁴² KORDELA, Marzena, “(2008) The Principle of Legal Certainty as a Fundamental Element of the Formal Concept of the Rule of Law” *Revue du notariat*, 110(2), 587–605. <https://doi.org/10.7202/1045553ar>, (e.t. 18.2.2024)

²⁴³ KÖKÜSARI, İsmail, “Anayasa Hukukunda Hukuki Güvenlik İlkesi”, Adalet Yayınevi, Ankara, 2015 s.25

²⁴⁴ MERCİMEK, Fulya, “Hukuki Güvenlik İlkesi ve Karşılaştırmalı Vergi Hukuku Bağlamında Değerlendirilmesi”, Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Maliye Ana Bilim Dalı Mali Hukuk Bilim Dalı, Doktora Tezi, Bursa 2019, s.15

Türk hukukunda ise kavram, “hukuk güvenliği”, “hukuki güvenlik” şeklinde kullanıldığı gibi, “hukuka güven ilkesi”, “hukuksal güvenlik” veya “hukuksal güven” olarak da ifade edildiği görülmektedir. Bunların yanısıra bazı daha eski kaynaklarda, hukuki güvenlik kavramı “hukuki emniyet” olarak da ifade edilmiştir. Özellikle Anayasa Mahkemesi, kavramı çoğunlukla “hukuk güvenliği”, bazen “hukuki güvenlik” az sayıda olarak da “hukuksal güvenlik” olarak kullanmaktadır. Ayrıca diğer dillerden çeviri yoluyla alınarak kullanıldığında ise “hukuki kesinlik”, “hukuki belirlilik” kavramlarının da kullanıldığı görülmektedir²⁴⁵.

Hukuki güvenlik, emniyette olmanın, güvende olmanın bir unsuru olarak kabul edilir. Bu bağlamda, kökeni 1789 Bildirisi'nin 2. maddesinde yer alan, özgürlük, mülkiyet ve baskıya karşı direnme gibi doğal ve vazgeçilmez insan hakları arasına emniyeti yerleştiren hükümlerdedir. Çoğu zaman, devrim dönemindeki insanların “emniyet/güven” sözcükleriyle yalnızca insanların ve malların korunmasını düşündükleri düşünülmüştür. Bu bir yanılgıdır, 1789 Fransız Devrimcileri için güven, hakların korunmasını da kapsamaktaydı. Girondist Bildirisi'nin 10. maddesi ve Jakoben Bildirisi'nin 8. maddesi bunu açıkça doğrulamaktadır²⁴⁶.

Hukukun beşeri münasebetlerde düzen tesis etme, kişilerin davranışlarına kılavuzluk etme gibi hususları icra edebilmesi için çeşitli özelliklere sahip olması gerekir. Bu özelliklerden bir kısmı da hukuki güvenliğe taalluk eder. Hukuk kurallarının açık olması, bireylere uygulanacak hukuk kurallarının belirli olması, bu kuralların ilan edilmiş

²⁴⁵ KÖKÜSARI, s.16

²⁴⁶ DE SALVIA, Michele, Cahiers du Conseil constitutionnel n° 11 (Dossier : Le principe de sécurité juridique), décembre 2001, <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-securite-juridique-en-droit-constitutionnel-francais>, (e.t. 20.2.2024).

olması, hareketlerin sonuçlarına bağlanabilecek hukuki neticelerin neler olacağının bilinmesi gibi hususlar bunlardan bazılarıdır²⁴⁷.

Hukuki güvenlik, ekseriyetle hukuk devletinin formal zorunluluklarından biri olarak görülmektedir. Hukuk devleti, yukarıda yaptığımız tanımlardan da görüleceği üzere geniş anlamda, devletin tüm faaliyetlerinde hukuka uygun davranması ve bu faaliyetlerinin hukuka uygunluğunun denetimi olarak ifade edilmektedir²⁴⁸. Ancak bu yapılırken diğer ilkelere de atıflar yapılmaktadır. İşte hukuki güvenlik ilkesi de hukuk devleti kavramı kapsamında kurallarda bulunması gereken, geçmişe yürümezlik, şeffaflık, ilan edilme, genele uygulanabilme gibi temel niteliklerle beraber düşünülmektedir²⁴⁹.

Hukuk devleti ilkesinin bir gereği olarak hukuki güvenlik, hukukun uygulanmasındaki belirsizlik veya ani değişim riskini ortadan kaldırmaya yönelik bir garanti veya koruma olarak tanımlanabilir²⁵⁰. Hukuk ve kesinlik, kavramsal olarak sıkı bir bağlantıya sahiptir. Eylemi normatif standartlara tabi tutarak, hukuk izin verilebilir davranışın alanını sınırlar, böylece toplumsal belirsizliği azaltır ve aksi takdirde daha az öngörülebilir ve hatta potansiyel olarak kaotik olabilecek insan etkileşimlerine bir düzen

²⁴⁷ HANCHER, Leigh/TALUS, Kim/WÜSTENBERG, Moritz: “(2021) Retrospective application of legal rules in the European Union: recent practice in the energy sector”, *Journal of Energy & Natural Resources Law*, 39:1, <https://cadmus.eui.eu/handle/1814/1949/browse?authority=e58f7271-44bb-4312-972e-2041ed0811f8&type=author>, (e.t. 20.2.2024) s.70., GÖZLER – KAPLAN, s.68.

²⁴⁸ BRENNINKMEIJER, Alex: *Incomprehensible Government&Legal Certainty*, Dutch National Ombudsman Annual Report 2012, s.13., BRAITHWAITE, John: “Rules and Principles: A Theory of Legal Certainty”, (2002), *Australian Journal of Legal Philosophy*, s.50., VAN MEERBEECK Jeremie: “Les Principes des Legalite et de Securite Juridique: Des Faux Amis?”, <https://dial.uclouvain.be/pr/boreal/object/boreal:236382>, (e.t. 11.12.2023).

²⁴⁹ KÖKÜSARI, s.3., VAN MEERBEECK, Jeremie: “(2008) Le Principe de Securite Juridique dans La Jurisprudence Communautaire: Un Principe en Quete de Sens”, *Revue du notariat*, 110(2), 497–516. <https://doi.org/10.7202/1045549ar>, s. 678, (e.t. 11.12.2023)., GRECH, Fabien: “Le principe de sécurité juridique dans l’ordre constitutionnel français”, *Revue française de droit constitutionnel* 2015/2 (n° 102), s.410., SOULAS de Russel Dominique/RAIMBAULT Philippe: “Nature et racines du principe de sécurité juridique : une mise au point.” *Revue internationale de droit comparé*. Vol. 55 N°1, Janvier-Mars 2003. pp. 85-103; www.persee.fr/doc/ridc_0035-3337_2003_num_55_1_5561, s.99, (e.t. 11.12.2023).

²⁵⁰ ÇAPTUĞ, Mehpere: “Hukuki Güvenlik İlkesinin Kavramsal Gelişimi”, *Uyuşmazlık Mahkemesi Dergisi*, Yıl 9, Sayı 17, Haziran 2021, s.133.

dayatır. Dolayısıyla, hukuki bir düzenin kurulması, diğer unsurlar arasında hukuki güvenlik ilkesini ön plana çıkarır²⁵¹.

AB hukukunda ise hukuki güvenlik ilkesinin hukuk kurallarının net, açık ve etkileri bakımından öngörülebilir olmasını gerektirdiği, böylece AB hukuku tarafından düzenlenen durumlar ve hukuki ilişkilerdeki ilgili tarafların pozisyonlarını belirleyebilmelerine imkan tanınmasının gerektiği vurgulanmaktadır²⁵².

Hukuki güvenlik kavramı Anayasada açık bir şekilde düzenlenmemiştir. Ancak özellikle Anayasa Mahkemesi verdiği kararlar ile hukuki güvenlik ilkesini ele almış ve kavramsal bir içeriğe ve uygulama pratiğine kavuşturmuştur. Anayasa Mahkemesi Kararlarında genel olarak “hukuki güvenlik ilkesi” terimi kullanılmakla birlikte “hukuksal güvenlik” ve “hukuk güvenliği ilkesi” gibi çeşitli şekillerde de kullanılmaktadır²⁵³.

Anayasa Mahkemesi’nin tanımına göre, “hukukî güvenlik ilkesi”; “(...) *Bir kanunî düzenlemenin bireylerin davranışını ona göre düzenleyebileceği kadar kesinlik içermesi, kişinin gerektiği takdirde hukukî yardım almak suretiyle, bu kanunun düzenlediği alanda belli bir eylem nedeniyle ortaya çıkacak sonuçları makul düzeyde öngörebilmesi gerekmektedir. (...)*” anlamına gelmektedir²⁵⁴. Anayasa Mahkemesi, bu kararında; hukuk devletinin temel ilkelerinden biri olan “belirlilik” ilkesini, “*Belirli bir kesinlik içinde, hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun*

²⁵¹ BERTEA, Stefano: “Towards a New Paradigm of Legal Certainty”, *Legisprudence* 2, 2008, s.25, https://www.researchgate.net/publication/275462157_Towards_A_New_Paradigm_of_Legal_Certainty, (e.t. 16.3.2024)

²⁵² RODRIGUEZ, Pablo Martin: “The Principle of Legal Certainty and the Limits to the Applicability of EU Law”, *Cahiers de Droit Europeen Colloque* 10 Septembre 2015, 2016-1, s.117.

²⁵³ EKERYILMAZ, Şebnem: *Vergilemede Hukuki Güvenlik İlkesinin Yargı Kararları Çerçevesinde Analizi*, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Sakarya 2019, s.7

²⁵⁴ Anayasa Mahkemesi’nin hukuki güvenlik ilkesi tanımı için: https://www.anayasa.gov.tr/media/3503/adil_yargilanma.pdf, (e.t. 22.04.2024).

bağlandığını, bunların İdare'ye hangi müdahale yetkisi doğurduğunu, Kanun'dan öğrenebilme imkânına sahip olmak” şeklinde tanımlamaktadır²⁵⁵.

5.3 Hukuki Güvenlik İlkesinin Alt İlkeleri ve İlkenin Neticeleri

Hukuki güvenlik ilkesinin yukarıda ele alınan tanımlarından hareket edildiğinde, temel olarak bu ilkenin hayata geçirilebilmesini sağlamak için “belirlilik”, “istikrar” ve “öngörülebilirlik” alt ilkelerinin ele alınması gerekliliği ortaya çıkmaktadır²⁵⁶.

Hukuki belirlilik hukuk kurallarının, bu kuralların uygulanmasının ve bir uyumsuzluk durumunda mahkemelerin verecekleri kararların açık, anlaşılabilir ve buna bağlı olarak da davranışlara yön verebilir durumda olmasıdır. Bu alt ilke hukuk kurallarının, kuralların uygulanması ve mahkemelerin verecekleri kararlar bakımından, bunları yapanların ve maddi sebeplerinin başka bir deyişle içeriklerinin bilinmesi yahut bilinebilecek durumda olmasını gerektirir.

Bir kuralın kimin tarafından, hangi yetkili kurum ya da organ tarafından yapılmış olduğunun yahut yapılacağının belirli olmaması fail sebep denilen sebebin bilinmesini engelleyecektir. Yani düzenlemeyi kimin yapacağı konusunda bir belirsizlik olacaktır. Diğer taraftan içeriğin de bilinebilir veya bilinebilecek durumda olması gerekir ki belirlilik ilkesinden bahsedilebilsin²⁵⁷.

Hukuki istikrar hem hukuk kurallarının hem de bu kuralların uygulamasının devamlı surette olması anlamına gelmektedir. Bu nedenle de hukuk kurallarının ve bunların uygulamasının istikrarlı olması dolaylı olarak hukuki öngörülebilirliğin tesis edilmesine de yardımcı olur. Hukuki istikrarın iki veçhesi vardır. İlki, hukukun bir sistem

²⁵⁵ ERÇİN, Ferhat: “Hukuk Güvenliği İlkesi Açısından 4721 Sayılı Türk Medeni Kanununun Zaman Bakımından Uygulanması”, Eurasian Academy of Sciences Social Sciences Journal 2017, Volume:16, s.121.

²⁵⁶ KÖKÜSARİ, 68.

²⁵⁷ KÖKÜSARİ, s.71.

olarak devamlılık arz etmesi iken, ikincisi var olan normların ve uygulamasının istikrar arz etmesidir²⁵⁸. Hukuki öngörülebilirlik, kişilerin normların ve bu normların uygulamalarının neticelerini öngörebilmeleri ve yaşamlarını buna göre planlayabilmeleridir. Hukuki öngörülebilirlik, sadece bütünüyle ele alındığında, normların ve bu normların uygulamasının öngörülebilir olması durumunda iyi bir netice verebilir.

Hukuki öngörülebilirliğin iki görünümü bulunmaktadır. Bunlardan ilki hukukun düzenlemesi lüzumlu olanları düzenleyerek, düzenlemesi lüzumlu olmayanları dışarıda tutması ve bunların topluma uyumluluğudur. Buna maddi bağlamda öngörülebilirlik denilmektedir. İkincisi ise, normlarla ve bu normların uygulanması ile verilen hakları ve tesis edilen emniyeti süreklilik arz edecek bir şekilde korumasıdır. Buna ise şekli bağlamda öngörülebilirlik denilmektedir²⁵⁹.

Sadece şekli manada tesis edilmiş olan bir hukuki güvenliğin içeriğe yönelik olarak öngörülebilirliği sağlayamaması ihtimali vardır. Bireyler, maddi bağlamda öngörülebilirliğe aykırı düşecek şekilde düzenlemeler yapılmayacağı hususunda norm koyuculara güvenebilmelidir. Normların maddi bağlamda öngörülebilirliği, normların yapılması, içeriği ve sonucu bakımından da bireyler tarafından kabul edilebilir olmasına bağlıdır. Başka bir söyleyişle, bir normun maddi bağlamda öngörülebilir olması o normun kabul edilebilir olmasını, normun kabul edilebilir olması için ise, o normun yapılışının, içeriğinin ve neticelerinin öngörülebilir bulunması gerekir²⁶⁰.

Bu ilkelerden hareketle özetleyecek olursak hukuki güvenlik ilkesi üç alt ilkenin varlığını gerektirir. Bunlar belirlilik, istikrar ve öngörülebilirliktir. İşte bu alt ilkelerin

²⁵⁸ KÖKÜSARİ, s.103.

²⁵⁹ KÖKÜSARİ, s.139.

²⁶⁰ KÖKÜSARİ, s.141.

hepsini saęlayan bir hukuk d zeninde ancak hukuki g venlikten bahsedilebilir. Hukuki g venlik tesis edildięinde ise, hukuk normlarının tatbik edildięi ger ek veya t zel kiřiler bu kuralların kılavuzluęu eřlięinde yollarını  izebilir, uzun vadeli planlar yapabilir ve kararlarını alabilirler.

Hukuki g venlik ilkesi liberal ve serbest piyasa ekonomilerinde ekonomik faaliyette bulunan ger ek ve t zel kiřilerin rasyonel kararlar almalarında en  nemli unsurlardan biridir. Bu ilke ve eřlik eden hukuk devleti ilkesi gibi dięer ilkeler idareye tatbik edilerek, idarelerin ani kararlar almalarını, rasyonel olmayan kararlar almalarını ve ekonomik hayatı felce uęratabilecek kararlar almalarını engelleyerek ekonomik faaliyet yapan ger ek ve t zel kiřilerin planlarını g ven i inde hayata ge ermelerine olanak saęlayacaktır.

Bu bakımdan hukuki g venlik ilkesinin en  nemli neticeleri kendini, kendi can ve mal varlıklarını g vende hisseden bireylerin yanı sıra toplumun can damarlarından olan ekonomik faaliyette bulunanlarda da g sterecektir. Bu bakımdan da hukuki g venlik ilkesinin ekonomik refahın artmasında  nemli bir rol  olduęunu s ylemek yanlış olmayacaktır.

 zellikle ekonomik faaliyetin yatırımcı tarafından konu ele alındıęında, hukuki g venlik ilkesinin bir  lkenin ekonomik refahında ne kadar  nemli bir rol  stlendięi de g r lebilecektir. Ulusal veya uluslararası yatırımcılar, yatırımlarını yaparken yatırım yapacakları  lkedeki ekonomik kořulların yanı sıra hukuki kořullara da bakmaktadırlar. Hukuki g venlięin olmadığı noktada yatırımcıların ka ınma ve  ekilme řeklinde iki davranıřı s z konusu olmaktadır. Ka ınma, yatırımcıların hukuki g venlięin bulunmadıęı yerlere yatırım yapmaması, buralardan uzak durması demektir.  ekilme ise, yatırımcıların bir yere yapmıř oldukları yatırımlarını hukuki g venlik ilkesinin

iřlememesi nedeniyle başka yerlere kaydırması veya faaliyetini tamamen sona erdirmesidir.

Hukuki güvenlik ilkesinin hayata geçirilmiş olması, kişilerin otonom hareket etmelerini de sağlayacaktır. Bu otonomi olmaksızın, bireylerin kendi kararlarını kendilerinin oluşturması veya verdiği karara uygun olarak hareket etmesi mümkün değildir²⁶¹. Bu da demokratik bir devlet anlayışından o ülkeyi uzaklaştıracak önemli bir etkidir.



²⁶¹ KÖKÜSARI, s.197.

6. AKREDİTASYON VE SERTİFİKASYON SİSTEMİNİN HUKUKİ GÜVENLİK İLKESİ KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI HAKKINA ETKİSİ

6.1 Genel Olarak

Kişisel verilerin korunmasında akreditasyon ve sertifikasyon sisteminin, anayasal hukuki güvenlik ilkesi kapsamında sayılması durumunda, bu sisteme girerek sertifika almış olan veri sorumluları ve veri işleyenlerin hukuki güvenlik ilkesi kapsamındaki hakları ile kişisel verileri işlenen gerçek kişilerin bir temel anayasal hak olarak korunan kişisel verileri kapsamındaki hakları arasında bir çatışma yaşanacaktır. Bu durum ise karşımıza anayasal normların hiyerarşisi konusunu çıkarmaktadır. Bu nedenle aşağıda öncelikle anayasal normlar arasındaki hiyerarşi konusu ele alınmıştır.

6.2 Anayasal Normlar Arasındaki Hiyerarşi

Anayasal temel haklar ile diğer anayasal haklar arasındaki çatışma denildiği zaman aslında bahsedilen “anayasal normlar arasındaki hiyerarşi” konusudur²⁶². Anayasal normlar arasında bir derecelendirme olduğuna dair çeşitli görüşler ileri sürülmüştür. Bu konuda görüşler kaleme almış olan önemli isimlerden, Fransız anayasa hukukçusu Georges Vedel, “Egemenlik ve Anayasa Üstü Olma -Souveraineté et Supraconstitutionnalité” isimli tartışmada²⁶³ bu hususu şu şekilde ifade etmektedir: “Anayasa metinlerinden kaynağını alan normlar karşılaştırıldığında, bu normlar arasında

²⁶² AL-DULAIMI, Ahmed Oudah/DEEM, Jacob/SALEH, Maher Faisal Saleh: “Are All Constitutional Rules Created Equal? Substantive Hierarchy in Constitutions in Theory and Practice”, 45(1) JMCL, s.47, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjX2vOUtOCEAxVVX_EDHcz5BkiQFnoECCgQAQ&url=https%3A%2F%2Fjournal.um.edu.my%2Findex.php%2FJMCL%2Farticle%2Fdownload%2F20926%2F10648%2F44713&usg=AOvVaw3pUXGjxUIbjKGTf3l-Avgs&opi=89978449, (e.t. 06.02.2024).

²⁶³ VEDEL, Georges: “Débat: Souveraineté et Supraconstitutionnalité”, Pouvoirs No:67, novembre 1993, p.79.

belirli bir altlık üstlük ilişkisinin, bir hiyerarşinin bulunup bulunmadığı, birinci, ikinci ve üçüncü derece normlar gibi bir ayırım olup olmadığı anayasa yargıçlarınca sorulabilir ve Anayasanın tüm yazılı olan kuralları anayasal niteliğe sahiptir, fakat bazı yazılı anayasa kuralları, diğer yazılı olan anayasa kurallarından daha anayasaldır olarak ifade edilebilir mi?” Vedel bu soruyu sormakla, tezin bu kısmında incelediğimiz anayasal normlar arasında bir hiyerarşi olup olmayacağı sorusunu gündeme getirmiş olmaktadır.

Bu noktada, eğer böyle bir normlar hiyerarşisi kabul edilecekse, normlar arasındaki bu derecelendirmede neyin esas alınacağını da belirlenmesi gerekmektedir. Sert çekirdekli temel haklar mı üstün kılınacaktır yoksa milli egemenliğe dair olan normlar mı üstün kılınacaktır²⁶⁴. Ya da başka bir deyişle anayasaların bireylerin haklarını düzenleyen normları mı üstün kılınacaktır yoksa devletin temel niteliklerine dair olan normları mı üstün kılınacaktır? Bu sorunun tezimizin konusu bakımından karşılığı, anayasal olarak kişilik hakları kapsamında korunan – ancak bize göre sui generis bir hak olarak ayrı düzenlenmesi gereken – kişisel verilerin korunmasına dair anayasal normlar ile bireyler mi, yoksa bir akreditasyon ve sertifikasyon sistemine girerek kişisel verilerin korunması alanında gerekli yeterliliğe sahip olduğunu kanıtlayıp anayasal hukuki güvenlik ilkesi kapsamında bu sertifikalara sahip olan veri sorumlularına mı üstünlük verilecektir?

Özetle, kişisel verilerin korunması ile hukuki güvenliğe dair iki anayasal norm çatıştığında hangisine üstünlük tanınacaktır ya da bu çatışma nasıl çözümlenecektir? Bu sorunun cevabı, kişisel verilerin korunmasında akreditasyon ve sertifikasyon sisteminin hukuk sistemi içerisindeki yerini ve fonksiyonunu da temelden belirleyecektir. Bu

²⁶⁴ GÖZLER, Kemal: Anayasa Normlarının Geçerliliği Sorunu, Ekin Yayınevi, Bursa 2016, s. 154.

nedenle, bu soruya bir cevap vermeden önce, anayasal normlar hiyerarşisi konusunun bir miktar daha açılması gerekmektedir.

Yargı organları ve hukuk doktrini "genel haklar" kavramını kullanırken, bazı durumlarda ise "temel haklar" kavramını kullanmaktadır. Bu, "genel haklar" teriminin "temel haklar" teriminden farklı olduğu anlamına mı gelmektedir yoksa bunlar birbirinin yerine kullanılabilen kavramlar mıdır? Temel haklar şu kriterlere göre genel haklardan ayırt edilebilir²⁶⁵:

- Genel haklar, geniş anlamda, yürütme organının müdahalesinden korunurken, temel haklar yürütme, yasama veya yargı organlarının müdahalesinden korur.
- Genel haklar idari meşruiyetle uyumlu iken, temel haklar anayasal meşruiyetle uyumludur.
- Genel haklar, sıradan yasama ve hukuk genel prensiplerine dayanırken, temel haklar anayasal değerlerle güvence altına alınır.
- Genel hakları koruma yetkisine sahip organ sıradan bir yargıçken, anayasal hakları anayasal yargıç korur. Anayasaya dahil edilen haklar anayasal değere sahiptir ve diğer anayasal hükümlerle aynı anayasa düzeyini işgal ederler. Bunları koruma görevi, anayasa mahkemelerine anayasanın üstünlüğünün güvencesi olarak verilmiştir.

Yani anayasa ile güvence altına alınmış temel haklar, diğer hukuki düzenlemeler ile koruma altına alınmış haklara göre üstün durumdadır. Ancak tez açısından tartışmak istediğimiz husus genel haklar ile anayasal temel haklar arasında bir hiyerarşi olup olmadığı değil, bizatihi anayasal temel haklar ve anayasal diğer düzenlemeler arasında bir hiyerarşi olup olmadığı hususudur.

²⁶⁵ AL-DULAIMI /DEEM/SALEH, s.58.

Temel haklar kaynağına göre bazı ayrımlara tabi tutulabilmektedir. Bunlardan ilki bir ülkenin yürürlükteki iç hukukunca belirlenmiş olan temel haklardır. Örneğin Türk hukuku açısından Türkiye Cumhuriyeti Anayasası'nın belirlediği haklar temel haklardır. Temel hakları anayasalardaki diğer haklardan ve anayasal teşkilata dair düzenlemelerden ayıran nokta, bunların bireylerin hakları olmaları ve bu nedenle devletin bireylerin sübjektif haklarını garanti etmekle yükümlendirildiği haklar olmalarıdır²⁶⁶. Diğer ayrımlar ise Avrupa İnsan Hakları Sözleşmesi gibi uluslararası belgelerden doğan temel haklar ile doğal hukuk teorisine dayanan doğal temel haklar şeklindeki ayrımdır. Temel hakların fonksiyonlarına göre ayrımını ise yukarıda özellikle Jellinek'in pozitif statü, negatif statü ve aktif statü hakları ayrımı özelinde ele almıştık. O nedenle bu kısımda tekrar etmiyoruz.

Temel haklara bu şekilde bir giriş yaptıktan sonra acaba bu temel haklar içinde de bir normlar hiyerarşisi söz konusu olabilir mi sorusu akla gelmektedir. Bir görüşe göre anayasalar ile koruma altına alınmış olan haklardan bazıları diğerlerine göre daha temel haklar niteliğindedir. Yani aynı düzeydeki haklar arasında bir derecelenme vardır. Bu derecelenmede temel haklar ile diğer anayasal haklar arasında bir altlık üstlük ilişkisi söz konusudur. Bu sebeple bu temel haklar ile diğerleri arasında bir çatışma husule gelirse bu bahsi geçen “en temel haklar” diğer haklara üstün gelmelidir²⁶⁷.

İşte tam bu noktada temel hakların özüne dokunulamayan bir grubu olarak karşımıza sert çekirdekli temel haklar çıkmaktadır. Sert çekirdekli temel haklar, olağan üstü hallerde dahi dokunulamayan haklardır. Bu haklar kişinin yaşam hakkına, maddi ve manevi varlığının tamlığına dokunulamayan hakları içerir. Bu haklar hususiyetle; yaşam hakkı, maddi ve manevi bütünlüğünü koruma hakkı ve bu hak bağlamında kişilik hakları,

²⁶⁶ GÖREN, s.36.

²⁶⁷ GÖZLER, Anayasa Normlarının Geçerliliği Sorunu, s. 154.

din, vicdan ve kanaat özgürlüğü, suç ve cezaların geriye yürümemesi, masumiyet karinesi gibi haklardır²⁶⁸. Bu sert çekirdekli temel haklar görüşüne göre, sert çekirdekli temel haklar, doğal hukuk anlayışının geçici parlamenter çoğunluğun iradeci baskıcılığı ve çoğunluk iradesini üstün kılma niyetine rağmen her zaman ona üstün gelir. Temel olarak insanın tabii ve zamanaşımına uğraması mümkün olmayan hakları bulunmaktadır. Bu hakların korunması ise tüm siyasi birliğin yegane amacıdır²⁶⁹. Bu nedenle de bir derecelendirme ile söyleyecek olursak bu sert çekirdekli birinci derece temel haklar diğer haklara üstün gelecek ve anayasal değişikliklere bir sınır oluşturacaktır.

Bunun karşısındaki diğer görüş ise anayasaların milli egemenliğe dair düzenlemelerinin, diğer anayasal düzenlemelere göre üstün olduğunu savunmaktadır. Bu görüşün temelinde milli egemenliği kuran kurucu iktidar ancak egemenliğe dair kayıtları değiştirebilir, bunun dışında kimse bu kayıtlara dokunamaz. Milli egemenlik aynı zamanda zorunlu olarak devlet egemenliğini de içerir. Bu nedenle devletin egemenliği de doğal olarak anayasanın dokunulamaz bir parçası haline gelmektedir²⁷⁰.

Tezin bu kısmı açısından önemli olan husus ise sert çekirdekli temel haklar veya milli egemenliğe ilişkin anayasal düzenlemeler arasında bir hiyerarşinin var olup olmadığı, var ise bu üstünlüğün yani hiyerarşinin ahlaki mi, siyasi mi yoksa hukuki bir hiyerarşi mi olduğudur. Bu soruyu Türk doktrininde doğrudan ele alıp karşılaştırmalı hukukla birlikte özellikle fransız hukukuna atıflarla detaylı bir şekilde incelemiş olan GÖZLER'e göre anayasa normları arasında hiyerarşi olamaz çünkü eğer bir hiyerarşi kabul edilirse -ki bu hiyerarşi hukuki hiyerarşi olarak ancak ele alınabilir – bu durumda

²⁶⁸ GÖREN, s.59.

²⁶⁹ GÖZLER, s.154.

²⁷⁰ GÖZLER, s.156.

anayasal hükümlerden birileri diğerlerinden geçerlilik alıyor olmalıdır. Oysa, anayasal düzlemde tüm normlar geçerliliklerini tek bir kurucu işlemde alırlar²⁷¹.

Ancak çeşitli ülkelerin anayasal düzenlemelerinde bu görüşün aksine, anayasal normlar arasında hiyerarşi tesis eden düzenlemeler olduğu görülmektedir. Örneğin, cumhuriyete dayalı hükûmet biçimi birçok Anayasa'da temel ilke olarak kabul edilmektedir. İtalya'da Anayasa'nın 139. maddesi, "Cumhuriyet biçimi, anayasa değişikliği konusu olamaz." hükmünü içermektedir²⁷². Aynı şekilde Türkiye Cumhuriyeti Anayasası'nın 1. maddesinde de Türkiye Devleti'nin bir Cumhuriyet olduğu, 4. maddesi ile de değiştirilemeyecek hükümler bulunduğu düzenlenmektedir. Eğer başka bir anayasal prensip veya kural bu prensiple çelişirse, anayasa mahkemeleri bu tür hükümleri üstün tutacaklardır. Bu tür bir karar, anayasadaki kurallar ve prensipler arasında bir hiyerarşi olduğunu vurgulayacaktır. Bu nedenle pozitif hukukta anayasal normlar arasında hiyerarşinin açıkça gözlendiği düzenlemeler yer almaktadır. Ancak açıkça bu tür hiyerarşinin belirtilmediği durumlarda ne yapılacaktır? GÖZLER'in savunduğu gibi anayasal normlar arasında hiyerarşi olmadığı mı kabul edilecektir, yoksa sert çekirdekli temel haklar gibi bir takım normatif düzenlemede yer almayan ayrımlara mı gidilecektir?

6.3 Akreditasyon ve Sertifikasyon Sisteminin Hukuki Güvenlik İlkesi Kapsamında Sayılması Durumunda Anayasal Bir Temel Hak Olarak Kişisel Verilerin Korunması Hakkına Etkisi

Yukarıda hukuki güvenlik ilkesini ele aldığımız bölümde de belirttiğimiz üzere, hukuki güvenlik ilkesi üç alt ilkenin varlığını gerektirir. Bunlar belirlilik, istikrar ve öngörülebilirliktir. Hukuki güvenlik tesis edildiğinde, hukuk normlarının tatbik edildiği

²⁷¹ GÖZLER, s.163.

²⁷² İtalyan Anayasası m.139 için: <https://www.senato.it/istituzione/la-costituzione/parte-ii/titolo-vi/sezione-ii/articolo-139>, (e.t. 06.03.2024).

gerçek veya tüzel kişiler bu kuralların kılavuzluğu eşliğinde yollarını çizebilir, uzun vadeli planlar yapabilir ve kararlarını alabilirler.

Hukuki güvenlik ilkesi liberal ve serbest piyasa ekonomilerinde ekonomik faaliyette bulunan gerçek ve tüzel kişilerin rasyonel kararlar almalarında en önemli unsurlardan biridir. Bu ilke ve eşlik eden hukuk devleti ilkesi gibi diğer ilkeler birlikte tatbik edilerek, idarelerin ani kararlar almalarını, rasyonel olmayan kararlar almalarını ve ekonomik hayatı felce uğratabilecek kararlar almalarını engelleyerek ekonomik faaliyet yapan gerçek ve tüzel kişilerin planlarını güven içinde hayata geçirmelerine olanak sağlanmaktadır.

İşte kişisel verilerin korunmasında GDPR ile getirilmiş olunan akreditasyon ve sertifikasyon sistemi, bir yandan kalite ve marka konusunda pozitif algı yaratırken, diğer yandan hesap verebilirlik ve şeffaflık kriterleri açısından veri sorumlularının kişisel verileri işlerken hesap verebilir ve şeffaf bir yapıda olmalarını sağlamaktadır. Ancak bunların dışında hukuki güvenlik ilkesi kapsamında da kişisel veri işleyen veri sorumlularının, başta düzenleyici otorite ve kişisel verileri işlenen ilgili kişiler olmak üzere, kendilerine uygulanabilecek özellikle keyfi idari kararlara ve keyfi ve aşırı bir şekilde kendilerine karşı girişilebilecek hukuki yollara karşı bir güvence de sağlamaktadır. İşte bu güvencenin sadece ilgili alanı düzenleyen kişisel veri koruma yasaları çerçevesinde mi olacağı yoksa bunun anayasal hukuki güvenlik ilkesi kapsamında mı olacağı tezin araştırma konularından birini oluşturmaktadır.

Kişisel verilerin korunmasında akreditasyon ve sertifikasyon sisteminin anayasal bir güvence getirip getirmediğini değerlendirmede önümüze çıkan belki de en temel sorun, anayasal güvencelerin bireylere tanınmış olduğu, bu nedenle de bir anayasal temel

hak niteliğinde olan hukuki güvenlik ilkesi bakımından, tüzel kişilerin bu ilke kapsamında değerlendirilip değerlendirilemeyeceği sorundur.

Gerçek kişilerin birtakım amaçlar için, süreklilik arz eden bir şekilde yani bir insan ömrünü de aşacak şekilde bir araya gelme istekleri, güçlerini birleştirerek belirledikleri amaçlara ve ideallere ulaşma ve hizmet etme istekleri, gerçek kişiler dışında hak ehliyetine sahip olan tüzel kişilerin ortaya çıkmasını sağlamıştır. Bu tüzel kişiler de genel olarak kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri olarak tezahür etmişlerdir.

Temel hak sahipleri, evvelemirde gerçek kişilerdir. Anayasalarda genellikle yer almakta olan “herkes”, “kimse”, “vatandaşlar” gibi sözcükler gerçek kişileri amaçlamaktadır²⁷³. Ancak bu gerçek kişiler bir tüzel kişilik çatısı altında birleştiklerinde artık temel hak sahibi olarak kalırlar mı veya bu oluşturdıkları tüzel kişilik, temel haklar yönünden kendisini meydana getiren gerçek kişilerle doğrudan veya dolaylı olarak bir bağlantı içinde sayılıp da temel hakka konu bir hukuk süjesi olarak ortaya çıkabilirler mi?

Federal Almanya Anayasası’nda 19/III maddesinde bu hususa ilişkin olarak şöyle bir düzenleme yer almaktadır; *“Temel haklar, bünyelerine göre uygulanabildiği oranda yerli tüzel kişiler için de geçerlidir”*.

Bu madde yerli tüzel kişiler için temel hakların varlığını ve geçerliliğini kabul etmektedir²⁷⁴. Türkiye Cumhuriyeti Anayasasında ise bu tür bir hüküm bulunmamaktadır. Ancak Medeni Kanun 48. maddesi ile tüzel kişilerin cins, yaş, hısımlık gereği insana özgü niteliklere bağlı olanlar dışındaki bütün haklara ve borçlara ehil olduğu düzenlemektedir.

Bu konudaki kanaatimiz, tüzel kişilerin gerçekten de insan olmaya bağlı olan bazı hususiyetler dışında temel hakların koruma alanına dahil oldukları yönündedir. Örneğin

²⁷³ GÖREN, s.83.

²⁷⁴ GÖREN, s.88.

ekonomik faaliyet özgürlüğü temelde gerçek kişilerin ekonomik özgürlüğü ile ilgili bir temel hak olarak algılansa da neticede ticari faaliyetlerin çok büyük kısmı tüzel kişilikler aracılığı ile yapılmaktadır. Bunun doğal sonucu ise ticari işletmelerin, sermaye şirketlerinin de ekonomik faaliyet özgürlüğünden yararlanması gerektiğidir. Yukarıda da belirttiğimiz gibi özellikle hukuki güvenlik ilkesi sadece gerçek kişilerin değil, tüzel kişilerin ve bu tüzel kişilerin organlarını oluşturan gerçek kişilerin önlerini görebilmelerine, yatırım kararları almalarına, rasyonel kararlar almalarına çok büyük etki eden bir ilke olması hasebiyle tüzel kişilerin hukuki güvenlik ilkesinden faydalanamayacağını söylemenin mümkün olmadığını düşünüyoruz.

Dolayısıyla, kişisel verilerin korunması alanında, iş süreçleri içerisinde kişisel veri işleme faaliyetleri olan ve bu nedenle veri sorumlusu sıfatına haiz olarak birçok yükümlülüğe tabi olan veri sorumlularının; bir yasal düzenleme ile getirilmiş olan akreditasyon ve sertifikasyon sistemine dahil olmaları ve iş süreçleri ile bu süreçlerde kişisel verileri işledikleri yazılımların, ortamların ve kullandıkları yöntemlerin mevcut hukuki düzenlemeler ile uyumlu olduğunun tevsik edilmesini istemeleri, temelde bir hukuki güvenlik ihtiyacının yansımasıdır. Bu nedenle veri sorumlusu sıfatını taşıyan tüzel kişilerin akreditasyon ve sertifikasyon sistemine dahil olup sertifikalandırılmasının anayasal hukuki güvenlik ilkesi kapsamında değerlendirilmesi gerektiği kanaatindeyim.

Ancak değerlendirme bu şekilde yapıldığı zaman, akreditasyon ve sertifikasyon sistemi, kişisel verileri koruma düzenlemeleri ile getirilen haklara ve en başta da anayasal düzeyde kişilik haklarının korunması hakkı içinde anayasal bir hak olarak düzenlenmiş olan kişisel verilerin korunması hakkına olumsuz bir etki yapabilme, kişilerin bu haklarını kullanmalarını kısıtlama veya hiç kullanamama gibi bir sonuca yol açabilir. Bu durumda

ise açık bir şekilde anayasal hukuki güvenlik ilkesi ile anayasal kişisel verilerin korunması hakkının çatışması sorunu ile karşı karşıya kalınabilir.

Bu durum uygulamada somut olarak çok farklı şekillerde karşımıza çıkabilir. Örneğin bir kişisel veri ihlali vakası yaşansa ve yetkisiz üçüncü şahısların ellerine geçirdikleri veriler yüzünden gerçek kişiler maddi veya manevi zararlara uğrasalar, veri sorumluları iş süreçlerinin kişisel veri koruma düzenlemeleriyle uyumlu olduğunun akredite edilmiş bir kuruluş tarafından tespit ve tevsik edilmiş olduğunu ileri sürerek, tazminat sorumluluğundan kaçınabilir mi veya o gerçek kişinin uğradığı zararın tazmininde tazminat miktarını azaltan bir unsur olarak kullanılabilir mi? Veya bir gerçek kişi veri sorumlusuna başvurarak kişisel verilerinin ne şekilde toplandığı, işlendiği, işleme amaçları ve dayanakları ve aktarıldığı üçüncü kişileri soran veya kişisel verilerinin imha edilmesini talep eden bir ilgili kişi başvurusu yaptığında, veri sorumluları sertifikasyona dayanarak genel bir cevap vermekle yetinebilirler mi?

Bu tür konular diğer akreditasyon ve sertifikasyon sistemlerinin uygulandığı alanlarda çok benzer sorunları ortaya çıkarmıştır. Örneğin asansör sektöründe A Tipi Muayene Kuruluşları tarafından asansörün temel sağlık ve güvenlik standartlarını karşılayıp karşılamadığı ile ilgili yapılan denetimler neticesinde verilen etiketler aslında bir sertifikasyon sistemi uygulamasıdır. Yeşil etiket verilmiş olan bir asansör, o asansörün temel sağlık ve güvenlik gereklerine ve mevzuata uygun olarak yapıldığını tevsik etmektedir. Ancak bu asansörde bir ölümlü veya yaralanmalı kaza meydana gelirse cezai sorumluluktan ve tazminat sorumluluğundan kaçınabilmek için asansör firmalarının almış oldukları bu yeşil etiketlere dayandıkları sıklıkla görülmektedir. Hatta sorumluluğun muayene kuruluşlarına da yoneltmeye çalışıldığı görülmektedir.

Dolayısıyla benzer konuların kişisel verilerin korunmasında uygulanacak akreditasyon ve sertifikasyon sisteminde de ortaya çıkması muhtemeldir.

İşte yukarıda verdiğimiz örneklerdeki gibi durumların ortaya çıkması halinde, gerçek kişiler kişisel verilerinin veri sorumlularınca korunamaması veya kişisel verileri işlenen ilgili kişi sıfatıyla yaptığı başvurulara genel cevaplar verilmesi nedeniyle temel bir hakkı ihlal edilmiş veya kullanılamamış olacaktır. Böyle bir durumda hukuki güvenlik ilkesine mi öncelik verilmelidir yoksa kişisel verilerin korunması hakkına mı?

Tezde muhtelif yerlerde savunmuş olduğumuz görüş, kişisel verilerin korunması hakkının “sui generis” bir hak olduğu bu nedenle anayasalarda da ayrı bir hak olarak düzenlenmesi gerektiği yönündedir. Ancak genel eğilim ve mevcut pozitif hukuk düzenlemeleri kişisel verilerin korunması hakkını kişilik haklarının korunması kapsamında değerlendirmektedir. Kişilerin adları, onurları gibi kişisel verileri de kişilik haklarına dahildir ve maddi ve manevi bütünlüğü sağlamaya yönelik temel haklardır. Bu haklar içinde kişisel verilerin korunması hakkının sert çekirdekli haklar kategorisi içine girdiği düşüncesindeyiz.

Hukuki güvenlik ilkesinin ise genel olarak anayasalarda doğrudan düzenlenmeyen ama çeşitli anayasal haklarla birlikte ve onların bazı durumlarda bir ön koşulu olarak kabul edilmesi ve yargı kararları ile hukuki güvenlik ilkesinin anayasal düzeyde bir ilke olduğunun kabul edilmesi karşısında, onun daha çok içtihadı ve genel bir niteliğe dayalı karakteri nedeniyle temel haklardan olduğunu, ancak kişisel verilerin korunması hakkı ile karşılaştırıldığında, bu iki hak arasında bir çatışma yaşandığında kişisel verilerin korunması hakkına üstünlük tanınması gerektiği, bu iki hak arasında anayasal norm hiyerarşisi açısından bir altlık üstlük ilişkisi bulunmadığı, bunun bir hakların yarışması konusunda olduğu gibi aynı seviyedeki iki hakkın yarışması olduğu, ancak bir tarafta sert

çekirdekli ve doğrudan gerçek kişiyi koruyan bir hak söz konusu olduğunda daha genel karakterli olan norma göre tercih edilmesi gerektiği kanaatindeyiz.

Ancak bu değerlendirmemizin sadece akreditasyon ve sertifikasyon sistemi içerisinde, kişisel verileri işleyen veri sorumlularının bu kişisel veri işlemlerinin kişisel verileri koruma mevzuatına uyumlu olduklarını gösteren aldıkları sertifikalar bakımından yapılmış olduğu gözden uzak tutulmamalıdır. Yani bu tezdeki değerlendirmemiz, çok sınırlı ve özel bir alana hasredilmiş olan bir değerlendirme olup anayasal normlar hiyerarşisi, temel haklar, sert çekirdekli haklar, hukuki güvenlik ilkesi gibi anayasa hukuku kapsamındaki genele teşmil edilebilecek değerlendirmeler değildir.

Son olarak, aslında kişisel verileri işlenen gerçek kişiler ile bu kişisel verileri işleyen veri sorumluları arasındaki ilişkinin, idari para cezaları, ceza kanunlarına yapılan atıflar gibi bazı kamu hukuku yönleri bulunsa da temel olarak özel hukuk kişileri arasındaki bir hukuki ilişki olduğu ve bu nedenle de konunun anayasal düzlemde tartışılmasının mümkün olmadığı da ileri sürülebilir. Başka bir deyişle özel hukuk alanında sonuç doğuracak bir konu olan akreditasyon ve sertifikasyon sisteminin ve bu sistem içinde alınmış olan sertifikaların neticede iki özel hukuk kişisi arasındaki ilişkiyi düzenlediği, kamu kurumları tarafından kişisel verilerin işlenmesinin konuyu kamu hukuku alanına dahil kılmayacağı, bu kamusal otoritelerin kişisel veri işlemlerinin kendi mevzuatları kapsamında değerlendirilmesi gerektiği, bu nedenle de konunun kamu hukukunu ve anayasa hukukunu ilgilendiren bir yönünün olmadığı ileri sürülebilir.

Ancak akreditasyon ve sertifikasyon sisteminin bizatihi getiriliş sebebinin kişilerin kişisel verilerinin korunması ile doğrudan alakalı olması ve kişisel verilerin korunması hakkının kişilik hakları içerisinde bir anayasal hak olarak ele alınması nedeniyle, konunun anayasal düzlemde ele alınması gerektiği tarafımızca

düşünülmektedir. Öte yandan örneğin Türkiye Cumhuriyeti Anayasası'nın 11/1 maddesinde düzenlendiği üzere anayasa normlarının sadece devlet ve vatandaşlar arasındaki ilişkilerde değil, aynı zamanda özel kişilerin kendi aralarındaki ilişkilerde de geçerli olduğu unutulmamalıdır. Üstelik bu etki, doğrudan doğruya sadece temel haklar ve özgürlükler alanında değil diğer anayasa normları için de geçerlidir²⁷⁵.



²⁷⁵ GÖREN, s.97.

7. SONUÇ

Kişisel verilerin teknolojinin gelişimine paralel olarak hem çeşitlerinin hem de işleme yöntem ve hacimlerinin gelişimi, bu verilerin bir süre sonra sadece kişilik haklarını koruyan hukuk veya ceza hükümleriyle değil, kendine özgü bir mekanizma çerçevesinde korunmasını gündeme getirmiştir. Aynı zamanda teknolojik gelişime bağlı bu durum kişisel verilerin daha üst seviyede bir koruma altına alması gerekliliği düşüncesini ortaya çıkarmış ve kişisel veriler Anayasalar kapsamında korunan haklar olarak Anayasa hukuku kapsamındaki yerini almıştır.

108 nolu, “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Avrupa Konvansiyonu” ile geniş ölçeğe yayılan kişisel verilerin korunması, Avrupa Birliği’nin 95/46 sayılı Yönergesi ve 2016 tarihli AB Genel Veri Koruma Tüzüğü ve özellikle bunu takip eden benzer düzenlemelerin artarda çeşitli ülkelerde yapılması ile küresel ölçeğe yayılmıştır.

Türkiye’de Anayasa’nın 20. maddesinde yapılan değişiklik ile kişisel verilerin korunması hakkı bir anayasal hak olarak düzenlenmiştir. 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesiyle AB ve dünya düzenlemeleri ile uyumlu bir kişisel verileri koruma hukuku düzenlemesi benimsenmiştir.

AB’de 95/46 sayılı Yönerge döneminde uygulamaları görülen “e-mahremiyet mühürleri” uygulamaları ile veri sorumluları, veri işleme süreçlerinde bir nevi sertifikasyona tabi tutularak, veri işleme süreçlerinin mevcut hukuki düzenlemelere uygun olduğu yönünde karineler meydana getirilmiştir. GDPR’ın yürürlüğe girmesinden sonra ise AB kişisel verilerin korunmasında bir akreditasyon ve sertifikasyon sistemini yürürlüğe sokmaya dair rehberler yayınlamıştır. Türkiye’de ise Kişisel Verileri Koruma Kurumu bireysel sertifikasyona dair bir karar yayınlamış ancak bu tezde bahsedilen

akreditasyon ve sertifikasyon sistemi ile ilgili bir düzenleme yapılmamıştır. Türkiye’de 8. Yargı Paketi reformu olarak gündeme gelen 2.3.2024 tarihli ve 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunla (“KVKK Reform Yasası”) ile KVKK’nın 6, 9, ve 18. maddelerinde kapsamlı değişiklikler yapılmış ancak bu değişiklikler ile de akreditasyon ve sertifikasyon sistemi hakkında herhangi bir düzenleme yapılmamıştır.

AB’de ise kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemi, “EUOPRIVACY” adı ile kurulmuş ve sistem işletilmeye başlanmıştır.

Temel haklar ve özgürlükler alanına alınmış olmasına rağmen kişisel verilerin korunması çok büyük oranda, “sui generis” şekilde ve teknolojik gerekliliklerle iç içe düzenlenmiş bir dizi hukuki düzenleme içerisinde ele alınmakta ve hukuk pratiği de bu yönde hızla gelişmektedir.

Diğer yandan AB haricinde henüz dünyada uygulaması başlamamış olan kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemini teorik ve pratik olarak inceleyen herhangi bir eser de bulunmamaktadır. Şu ana kadar var olan çalışmalar GDPR m.42 ve 43 çerçevesindeki düzenlemeler ve bu düzenlemelerle ilgili olarak AB’nin yetkili organlarının yayınladığı rehberler ve raporlardan ibarettir. Ayrıca çok az sayıda makale yayınlanmıştır.

Bu nedenle tez ile şu ana kadar bilimsel bir eserde detaylı bir incelemesine yer verilmemiş olan kişisel verilerin korunmasında akreditasyon ve sertifikasyon sistemi GDPR’daki düzenleme çerçevesinde ele alınmıştır.

Tezde, GDPR ile getirilmiş olunan akreditasyon ve sertifikasyon sisteminin detayları incelenerek, hukuki düzenlemenin somutlaşmış hali olan EUOPRIVACY sistemi de ele alınmıştır. Aynı zamanda konu, Anayasa hukuku kapsamında hukuki

güvenlik ilkesi bakımından değerlendirilmiş ve hukuki güvenlik ilkesinin tüzel kişi olan veri sorumluları ve veri işleyenler açısından mümkün olup olmayacağı, kişilerin veri koruma düzenlemeleri kapsamında sahip oldukları hakların, akredite olmuş ve gerekli sertifikasyonlara sahip olan veri sorumluları ve veri işleyenler karşısında korunmasında akreditasyon ve sertifikasyon sisteminin bir farklılık yaratıp yaratmayacağı ve sertifikasyonun hukuki güvenlik ilkesi kapsamında olması durumunda bir anayasal ilke olan hukuki güvenlik ilkesi ile bir anayasal temel hak olan kişisel verilerin korunması hakkı arasındaki çatışmada hangisine üstünlük tanınacağı veya bu çatışmanın ne şekilde çözümlenebileceği, GDPR ile düzenlenen akreditasyon ve sertifikasyon sisteminin detaylı incelenmesi ile birlikte ele alınmıştır.

Kişisel verilerin korunması alanında, iş süreçleri içerisinde kişisel veri işleme faaliyetleri olan ve bu nedenle birçok yükümlülüğe tabi olan veri sorumlularının; bir yasal düzenleme ile getirilmiş olan akreditasyon ve sertifikasyon sistemine dahil olmaları ve iş süreçleri ile bu süreçlerde kişisel verileri işledikleri yazılımların, ortamların ve kullandıkları yöntemlerin mevcut hukuki düzenlemeler ile uyumlu olduğunun tevsik edilmesini istemeleri temelde bir hukuki güvenlik ihtiyacının yansımasıdır. Bu nedenle veri sorumlusu sıfatını taşıyan tüzel kişilerin akreditasyon ve sertifikasyon sistemine dahil olup sertifikalandırılmasının anayasal hukuki güvenlik ilkesi kapsamında değerlendirilmesi gerektiği kanaatindeyiz.

Ancak bu değerlendirme bu şekilde yapıldığı zaman, akreditasyon ve sertifikasyon sistemi, kişisel verileri koruma düzenlemeleri ile getirilen haklara ve en başta da anayasal düzeyde kişilik haklarının korunması hakkı içinde anayasal bir hak olarak düzenlenmiş olan kişisel verilerin korunması hakkına olumsuz bir etki yapabilme, kişilerin bu haklarını kullanmalarını kısıtlama veya hiç kullanamama gibi bir sonuç

doğurabilir. Bu durumda ise açık bir şekilde iki anayasal normun çatışması sorunu ile karşı karşıya kalınabilir.

Bu durum uygulamada somut olarak çok farklı şekillerde karşımıza çıkabilir. Örneğin bir kişisel veri ihlali vakası neticesinde yetkisiz üçüncü şahısların ellerine geçirdikleri veriler yüzünden gerçek kişiler maddi veya manevi zararlara uğrasalar, veri sorumluları iş süreçlerinin kişisel veri koruma düzenlemeleriyle uyumlu olduğunun akredite edilmiş bir kuruluş tarafından tespit ve tevsik edilmiş olduğunu ileri sürerek, tazminat sorumluluğundan kaçınabilir mi veya o gerçek kişinin uğradığı zararın tazmininde tazminat miktarını azaltan bir unsur olarak kullanılabilir mi? Veya bir gerçek kişi veri sorumlusuna başvurarak kişisel verilerinin ne şekilde toplandığı, işlendiği, işleme amaçları ve dayanakları ve aktarıldığı üçüncü kişileri soran veya kişisel verilerinin imha edilmesini talep eden bir ilgili kişi başvurusu yaptığında, veri sorumluları sertifikasyona dayanarak genel bir cevap vermekle yetinebilirler mi?

Bu tür konular diğer akreditasyon ve sertifikasyon sistemlerinin uygulandığı alanlarda çok benzer sorunları ortaya çıkarmıştır. Örneğin asansör sektöründe A Tipi Muayene Kuruluşları tarafından asansörün temel sağlık ve güvenlik standartlarını karşılayıp karşılamadığı ile ilgili yapılan denetimler neticesinde verilen etiketler aslında bir sertifikasyon sistemi uygulamasıdır. Yeşil etiket verilmiş olan bir asansör, o asansörün temel sağlık ve güvenlik gereklerine ve mevzuata uygun olarak yapıldığını tevsik etmektedir. Ancak bu asansörde bir ölümlü veya yaralanmalı kaza meydana gelirse cezai sorumluluktan ve tazminat sorumluluktan kaçabilmek için asansör firmalarının almış oldukları bu yeşil etiketlere dayandıkları sıklıkla görülmektedir. Hatta sorumluluğun muayene kuruluşlarına da yöneltilmeye çalışıldığı görülmektedir. Dolayısıyla benzer

konuların kişisel verilerin korunmasında uygulanacak akreditasyon ve sertifikasyon sisteminde de ortaya çıkması muhtemeldir.

İşte yukarıda verdiğimiz örneklerdeki gibi durumların ortaya çıkması halinde, gerçek kişiler, kişisel verilerinin veri sorumlularınca korunamaması veya kişisel verileri işlenen ilgili kişi sıfatıyla yaptığı başvurulara genel cevaplar verilmesi nedeniyle temel bir hakkı ihlal edilmiş veya kullanılamamış olacaktır. Böyle bir durumda hukuki güvenlik ilkesine mi öncelik verilmelidir yoksa kişisel verilerin korunması hakkına mı?

Tezde muhtelif yerlerde savunmuş olduğumuz görüş, kişisel verilerin korunması hakkının “sui generis” bir hak olduğu bu nedenle anayasalarda da ayrı bir hak olarak düzenlenmesi gerektiği yönündedir. Ancak genel eğilim ve mevcut pozitif hukuk düzenlemeleri kişisel verilerin korunması hakkını kişilik haklarının korunması altında özel hayatın mahremiyeti kapsamında değerlendirmektedir. Kişilerin adları, onurları gibi kişisel verileri de kişilik haklarına dahildir ve maddi ve manevi bütünlüğü sağlamaya yönelik temel haklardandır. Kişisel verilerin korunması hakkının bu haklar içinde de sert çekirdekli haklar kategorisi içine girdiği düşüncesindeyiz.

Hukuki güvenlik ilkesinin ise genel olarak anayasalarda doğrudan norm olarak yer almamasına karşın, yargı kararları ile hukuki güvenlik ilkesinin anayasal düzeyde bir ilke olduğunun kabul edilmesi nedeniyle, onun daha çok içtihadı ve genel bir niteliğe dayalı karakteri nedeniyle temel haklardan olduğu, ancak kişisel verilerin korunması hakkı ile karşılaştırıldığında, bu iki hak arasında bir çatışma yaşandığında kişisel verilerin korunması hakkına üstünlük tanınması gerektiği, bu iki hak arasında anayasal norm hiyerarşisi açısından bir altlık üstlük ilişkisi bulunmadığı, bunun bir hakların yarışması konusunda olduğu gibi aynı seviyedeki iki hakkın yarışması olduğu, ancak bir tarafta sert

çekirdekli ve doğrudan gerçek kişiyi koruyan bir hak söz konusu olduğunda daha genel karakterli olan norma göre tercih edilmesi gerektiği kanaatindeyiz.

Türkiye, özellikle AB ile aynı düzeyde kişisel verilerin korunması için çaba sarf etmektedir. Bu kapsamda bir akreditasyon ve sertifikasyon sisteminin kurulmasının AB ile uyumlu bir kişisel verilerin korunması düzeyinin temin edilmesi için kaçınılmaz olduğu tarafımızca düşünülmektedir.

Bu sistemin uygulanmasının en önemli faydası Türkiye'nin AB başta olmak üzere dünya ile tam uyumlu bir kişisel verilerin korunması rejimi uyguladığının bir göstergesi olması ve bu sayede de ülkelerin alacakları yeterlilik kararlarına pozitif etki yapacak olmasıdır. Böylece Türkiye'nin ve Türk girişimcilerinin dünya ile entegrasyonu daha da kolaylaşacak, dünyanın en büyük ekonomik faaliyet alanı olan veri ekonomisi alanında hak ettiği yeri almasına yardımcı olacaktır.

Bu kapsamda GDPR'da öngörüldüğü üzere bir akreditasyon kuruluşu olarak örneğin TÜRKAK akreditasyon kriterlerini belirleyip, sertifikasyonu yapacak firmaların seçiminde, görevlerini yerine getirmelerinde ve uygulamanın nasıl yapılacağı konusunda gerekli düzenlemeleri yapabilir. Böylece tezimizde savunduğumuz sert çekirdekli bir temel hak olarak kişisel verilerin korunmasına hakkına hanel gelmemek kaydıyla, veri sorumluları hangi çerçeve içinde neler yapmaları gerektiğini, ne şekilde hareket etmeleri gerektiğine ve doğabilecek sorumluluklarına dair somut bir çerçeve elde edebileceklerdir. Bu sayede idarenin keyfi hareket etmesinin önüne geçilebilecek ve hukuki güvenlik ilkesi de garanti altına alınabilecektir.

KAYNAKÇA

- AKGÜL, Aydın: Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınevi, İstanbul 2014.
- AKGÜL, Aydın: Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Yayınlanmış Doktora Tezi, Kocaeli, 2013.
- AL-DULAIMI, Ahmed Oudah/DEEM, Jacob/SALEH, Maher Faisal: “Are All Constitutional Rules Created Equal? Substantive Hierarchy in Constitutions in Theory and Practice”, s.45(1) JMCL.
- ALTINDERE, Murat: Kişisel Verilerin Korunması Hukuku ve Uygulaması, Adalet Yayınevi, Ankara 2020.
- AMIRULLOH, Muhamad/RACHMADINI, Vidya Noor: “Legal Certainty in the Use of Certification of Trustworthiness by Indonesian E-Commerce Business”, Central European Journal of International and Security Studies 12, no.4, s.564–575.
- ARTUGAL, Seda Meltem: Mühendislik Eğitiminde Toplam Kalite Yönetimi ve Metalürji ve Malzeme Mühendisliği Bölümündeki ABET Uygulamaları, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 2010.
- AŞIKOĞLU, Şehriban İpek: AB ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Oniki Levha Yayınları, İstanbul 2018.
- ATAY, Ender Ethem: Anayasa Hukuku, Turhan Kitabevi, Ankara 2022.
- ATAY, Ender Ethem: İdare Hukuku, Turhan Kitabevi, Ankara 2019.
- AYDIN, Sedat Erdem: AİHM içtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, 12 Levha Yayınevi, İstanbul 2015.
- AYÖZGER, A. Çiğdem: Kişisel Verilerin Korunması, Beta Yayınevi, İstanbul 2016.
- BAKIREL, Nur Buğçe: Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk

- Paylaşımının Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi, Yayınlanmış Yüksek Lisans Tezi, Ankara, 2020.
- BALABAN, Mahmut Furkan: Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2023.
- BASKIN, Onur: Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2021.
- BAŞALP, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara 2004.
- BAŞAR, Cemal: Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, Yayınlanmış Doktora Tezi, İzmir, 2019.
- BATUM, Süheyl/YILMAZ, Didem/KÖYBAŞI Serkan: Anayasa Hukuku Temel Kavramlar ve Genel Esaslar, Oniki Levha Yayınları, İstanbul 2021.
- BATUM, Süheyl: Avrupa İnsan Hakları Sözleşmesi ve Türk Anayasal Sistemine Etkileri, İstanbul 1993.
- BERBER KESER Leyla/BİLGİLİ Ali Cem, (Editörler): “Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku”, Marmara Hukuk Bilimsel Toplantılar Serisi I, 17 Nisan 2019 Haydarpaşa, Oniki Levha Yayınları, İstanbul 2020.
- BERTEA, Stefano: “Towards a New Paradigm of Legal Certainty”, *Legisprudence* 2, 2008, s.25-45.
- BOTTINI, Fabien: “Les implications nouvelles du principe de sécurité juridique en droit administrative”, *Cahiers de la recherche sur les droits fondamentaux*, 6 | 2008, mis en ligne le 11 décembre 2020, <http://journals.openedition.org/crdf/6912>, (e.t. 18.6.2023).

- BOZKURT, Habip: Kişisel Verilerin İşlenmesinin Hukuki Boyutu, Yetkin Yayınları, Ankara 2021.
- BRAITHWAITE, John: “Rules and Principles: A Theory of Legal Certainty”, (2002) s.27 Australian Journal of Legal Philosophy.
- BRENNINKMEIJER, Alex: “Incomprehensible Government&Legal Certainty”, Dutch National Ombudsman Annual Report 2012.
- BÜK, Alaattin: Bilişim Alanında Kişisel Verilerin Korunması, Yetkin Yayınevi, Ankara 2021.
- CAREY Peter/DEIGHTON Alison: Enforcement and the Role of the Regulator, Oxford University Press, Oxford 2018.
- CASSANO Giuseppe/ COLAROCCO, Vincenzo/GALLUS Giovanni Battista/MICOZZI Francesco Paolo: Il Processo Di Adeguamento al GDPR, GIUFFRÉ Edizioni, Milano 2022.
- CASTROREALE, Renato/PONTI Chiara: Il Sistema Integrato Per La Sicurezza Delle Informazioni Ed Il GDPR, EPC Editore, Rome 2021.
- CEYLAN, Mehmet: Türkiye’de Kalite Akreditasyonu ve Türkak, Yüksek Lisans Tezi, Muğla Üniversitesi Sosyal Bilimler Enstitüsü, Muğla, 2009.
- CHATZIPOULIDIS, Aristeidis/TSIAKIS, Theodosios/KARGIDIS, Theodoros: “A Readiness Assessment Tool for GDPR Compliance Certification”, Computer Fraud&Security Journal, August 2019.
- CİVELEK, Dilek Yüksel: Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, T.C. Başbakanlık DPT Müsteşarlığı Bilgi Toplumu Daire Başkanlığı, Uzmanlık Tezi, Ankara, 2011.

- COŞKUN Cemrenur: Milletlerarası Özel Hukukta Haksız Fiil Bağlamında Kişisel Verilerin Korunması, Yetkin Yayınevi, Ankara 2023.
- CRAIG, Paul/DE BURCA, Grainne: EU Law: Text, Cases, and Materials, Oxford University Press, Oxford 2020.
- ÇAPTUĞ, Mehpere: “Hukuki Güvenlik İlkesinin Kavramsal Gelişimi”, Uyuşmazlık Mahkemesi Dergisi, Yıl 9, Sayı 17, Haziran 2021, s.133-160.
- ÇAVUŞOĞLU Gökçe Filiz/YILMAZ Süleyman: Kişisel Verileri Koruma Hukuku, Yetkin Yayınları, Ankara 2020.
- ÇAVUŞOĞLU Gökçe Filiz: Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları, Yetkin Yayınevi, Ankara 2021.
- ÇEKİN, Mesut Serdar: AB Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, Oniki Levha Yayınları, İstanbul 2020.
- ÇELİKEL Serdar: Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Doktora Tezi, Ankara, 2021.
- ÇİMEN BULUT, İpek: Avrupa Dijital Tek Pazarında Kişisel Verilerin Korunması, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Avrupa Birliği Anabilim Dalı Avrupa Çalışmaları Programı, Doktora Tezi, İzmir, 2020.
- ÇÖLKESEN, Rifat: Network TCP/IP UNIX El Kitabı, Papatya Yayıncılık, İstanbul 2000.
- DE SALVIA, Michele: Cahiers du Conseil constitutionnel n° 11 (Dossier : Le principe de sécurité juridique, <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-securite-juridique-en-droit-constitutionnel-francais>, (e.t. 20.2.2024)

- DEMİRBAŞ, Ali: Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri, Oniki Levha Yayınları, İstanbul 2023.
- DENİZ, İlknur: Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve KVKK Kapsamında Korunması, Seçkin Yayınevi, Ankara 2021.
- DEVELİOĞLU, Hüseyin Murat: AB Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması, Oniki Levha Yayınları, İstanbul 2017.
- DOĞAN, Bayram: Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, Adalet Yayınevi, Ankara 2022.
- DOĞRU, Derya: Avrupa İnsan Hakları Mahkemesi Yargılamasında Takdir Marjı Doktrini, Turhan Kitabevi, Ankara 2019.
- DUGUIT, Leon: La Regle de Droit – Le Problem de L’Etat, Tome I, , Paris 1921.
<https://gallica.bnf.fr/ark:/12148/bpt6k932656z/f9.item.r=trait%C3%A9+droit+constitutionnel+duguit.langFR>, (e.t. 18.12.2023).
- DURAN, Lütfi: İdare Hukuku, İÜHF Yayını, İstanbul 1982.
- DÜLGER, Murat Volkan: Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul 2020.
- EKERYILMAZ, Şebnem: Vergilemede Hukuki Güvenlik İlkesinin Yargı Kararları Çerçevesinde Analizi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Sakarya, 2019.
- EKİN, Beste: Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri, On İki Levha Yayıncılık, İstanbul 2021.
- ELBİR, Nazlı: Kişiliğin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, 2020.

- ERÇİN, Ferhat: “Hukuk Güvenliği İlkesi Açısından 4721 Sayılı Türk Medeni Kanununun Zaman Bakımından Uygulanması”, Eurasian Academy of Sciences Social Sciences Journal 2017, Volume:16, s.118 - 135.
- ERDOĞAN, Irmak: Yapay Zeka Teknolojilerinin Ceza Muhakemesinde Kişisel Veri Toplanmasına Etkileri, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü KamuHukuku Anabilim Dalı, Doktora Tezi, İstanbul, 2021.
- ERKUŞ, Leyla: Eğitim Fakültelerinin Akreditasyon Sürecine Hazır Olma Durumuna İlişkin Öğretim Elemanlarının Görüşlerinin Değerlendirilmesi, Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale, 2009.
- GÖREN, Zafer : Temel Hak Genel Teorisi, Geliştirilmiş ve Gözden Geçirilmiş 5. Basım, Yetkin Yayınları, Ankara 2022.
- GÖZLER, Kemal/KAPLAN, Gürsel: İdare Hukuku Dersleri, Güncellenmiş 20. Baskı, Ekin Yayınevi, Bursa 2018.
- GÖZLER, Kemal: Anayasa Hukukunun Genel Esasları, Ekin Yayınevi, Bursa 2016.
- GÖZLER, Kemal: Anayasa Normlarının Geçerliliği Sorunu, Ekin Yayınevi, Bursa 2016.
- GRECH, Fabien: “Le principe de sécurité juridique dans l’ordre constitutionnel français”, Revue française de droit constitutionnel 2015/2 (n° 102), pages 405 à 428.
- GÜREL, Begüm/BULGURCU, Berfin Helin: Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı, Platon Hukuk, İstanbul 2020.
- GÜRSES, Bekir: AB ve Türk Hukukunda Kişisel Verilerin Korunması: Mevzuat Uyumuna Yönelik Bir Değerlendirme, Platon Hukuk Yayınları, İstanbul 2022.

- HANCHER, Leigh/TALUS WÜSTENBERG, Moritz: “(2021) Retrospective application of legal rules in the European Union: recent practice in the energy sector”, *Journal of Energy & Natural Resources Law*, 39:1, s.65-81.
- HARDY, Helène: *Le principe de sécurité juridique au sens du droit de la Convention européenne des droits de l’homme Droit*, Université Montpellier 2019, <https://tel.archives-ouvertes.fr/tel-02890546>, (e.t. 18.2.2024)
- HİZARCI, Emine: 6698 Sayılı KVKK'nun AB Veri Koruma Hukuku Işığında Değerlendirilmesi, Yetkin Yayınları, Ankara 2020.
- K.LANDY Gene: *The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law*, Syngress Publishing, United States of America 2008.
- KABADAYI, Elif Sinem: *Unutulma Hakkı*, Yetkin Yayınları, Ankara 2021.
- KABOĞLU, İbrahim Ö.: *Anayasa Hukuku Dersleri – Genel Esaslar, Güncellenmiş ve sadeleştirilmiş 16. Baskı*, Legal Yayınevi, İstanbul 2021.
- KAMA IŞIK, Sezen: *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*, Oniki Levha Yayınları, İstanbul 2020.
- KAMARA, Irene/De HERT Paul: *Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape*, Information Technology and Law Series, ITLS, Volume 28, March 2018.
- KANGAL, Zeynel Temel: *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, Oniki Levha Yayınları, İstanbul 2019.
- KAYA, Mehmet Bedii: *KVKK Reformu 2024 Değişiklikleri*, Dijital Baskı v1.0, Mart 2024.

- KAYA, Semih Batur: Avrupa İnsan Hakları Sözleşmesiyle Karşılaştırmalı Olarak Anayasal Hakların Hukuki Rejimi ve Yorumu, Seçkin Yayınevi, Ankara 2021.
- KORDELA, Marzena: “(2008) The Principle of Legal Certainty as a Fundamental Element of the Formal Concept of the Rule of Law” *Revue du notariat*, 110(2), s.587–605. <https://doi.org/10.7202/1045553ar>, (e.t. 18.2.2024)
- KORKMAZ, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Seçkin Yayınevi, Ankara 2017.
- KOSTINA, Arina: Assessing the contribution of the CJEU to developing the EU fundamental right to protection of personal data, Koç Üniversitesi, Kamu Hukuku Doktora Tezi, İstanbul, 2021.
- KOTİL ÖĞRETMEN, Zeynep: Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka, Oniki Levha Yayınları, İstanbul 2022.
- KÖKÜSARI, İsmail: Anayasa Hukukunda Hukuki Güvenlik İlkesi, Adalet Yayınevi, Ankara 2015.
- KÜZECİ, Elif: Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul 2021.
- LACHAUD, Eric: “Accountability and Certification in GDPR”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3948093 , (e.t. 12.1.2024)
- LACHAUD, Eric: What GDPR Tells About Certification, *Computer Law&Security Review* 38 (2020) 105457.
- MAGGI, Michela/RECUPERO, Luigi: Privacy E Ricerca Scientifica E Sanitaria, BTT Editore, Lomazzo (CO) 2021.
- MANGIR, Şefika Demet: Uluslararası Toplumun Anayasası Jus Cogens, Nobel Yayınevi, Ankara 2015.

MERCİMEK, Fulya: Hukuki Güvenlik İlkesi ve Karşılaştırmalı Vergi Hukuku Bağlamında Değerlendirilmesi, Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Maliye Ana Bilim Dalı Mali Hukuk Bilim Dalı, Doktora Tezi, Bursa 2019.

NALDI,Maurizio/ITALIANO,Giuseppe/RANNENBER,Kai/MEDINA, Manel/BOURKA, Athena, (Eds.): “Privacy Technologies and Policy”, 7th Annual Privacy Forum (APF 2019), Rome – Italy June 13-14 2019.

NUR, Pınar: Vergi Hukuku Açısından Kişisel Verilerin Korunması, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Mali Hukuk Bilim Dalı, Doktora Tezi, Ankara 2022.

OKUR, Zeki: İş Hukukunda Elektronik Gözetleme, Legal Yayınevi, İstanbul 2013.

ÖZBUDUN, Ergun: Türk Anayasa Hukuku, Gözden Geçirilmiş 21. Baskı, Yetkin Yayınları, Ankara 2023.

ÖZKAN, Oğulcan: Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara 2020.

RODRIGUEZ, Pablo Martin: “The Principle of Legal Certainty and the Limits to the Applicability of EU Law”, Cahiers de Droit Europeen Colloque 10 Septembre 2015, 2016-1.

ROMITO CICCIA, Chiara: Il GDPR nella Micro, Piccola e Media Impresa: Un percorso di semplificazione della compliance tra protezione dei dati e adempimenti di legge, GIUFFRÉ Edizioni, Milano 2021.

SARP, Nilgün: Toplam Kalite Yönetimi Uygulamaları, Siyasal Kitabevi, Ankara 2014.

SEVİMLİ Ahmet K.: İşçinin Özel Yaşamına Müdahalenin Sınırları, Legal Yayınevi, İstanbul, 2006.

- SOULAS, Russel Dominique/RAIMBAULT, Philippe: “Nature et racines du principe desécurité juridique : une mise au point.” Revue internationale de droit comparé. Vol. 55 N°1, Janvier-mars 2003. pp. 85-103;
www.persee.fr/doc/ridc_0035- 3337_2003_num_55_1_5561, (e.t. 11.12.2023).
- SÜMER, Bilgesu: The Certification Mechanism Under The EU General Data Protection Regulation, Marmara Üniversitesi, Avrupa Araştırmaları Enstitüsü, Avrupa Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul 2019.
- ŞİMŞEK AKTAŞ, Duygu: Bilişim Teknolojilerindeki Gelişmelerin Anayasal Fonksiyonlar Üzerindeki Dönüştürücü Etkisi, Oniki Levha Yayınları, İstanbul 2020.
- TANÖR, Bülent/YÜZBAŞIOĞLU, Necmi: 1982 Anayasasına Göre Türk Anayasa Hukuku, Güncelleştirilmiş 20. Bası, Beta Yayınevi, İstanbul 2020.
- TANSUĞ, Çağla: İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması, Oniki Levha Yayınları, İstanbul 2023.
- TEKİNOĞLU, Dilara: Kişisel Verilerin Korunması Hukuku Açısından Mobil Uygulamalarda Konum Gizliliği, On İki Levha Yayıncılık, İstanbul 2020.
- TEPE, Esra: Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2021.
- TEZİÇ, Erdoğan: Anayasa Hukuku, Tıpkı 25. Bası, Beta Yayınevi, İstanbul 2021.
- THIENE, Arianna/CORSO, Stefano: La Protezione dei Dati Sanitari: Privacy e Innovazione Tecnologica tra Salute Pubblica e Diritto alla Riservatezza, Jovene Editore, Napoli 2023.
- TOPALOĞLU, Mustafa: Bilişim Hukuku, Karahan Kitabevi, Adana 2005.

- TURAN, Metin: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2019.
- UYARER GÖÇMEN, Sinem: Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara 2020.
- ÜÇÜNCÜ, Sümeyye Hilal: Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, Yayınlanmış Doktora Tezi, Ankara 2018.
- VAN MEERBEECK, Jeremie: “(2008) Le Principe de Sécurité Juridique dans La Jurisprudence Communautaire: Un Principe en Quete de Sens”, Revue du notariat, 110(2), 497–516. <https://doi.org/10.7202/1045549ar>, (e.t. 11.12.2023)
- VAN MEERBEECK, Jeremie: “Les Principes des Legalité et de Sécurité Juridique: Des Faux Amis?”, <https://dial.uclouvain.be/pr/boreal/object/boreal:236382>, (e.t.11.12.2023).
- VEDEL, Georges: “Débat: Souveraineté et Supraconstitutionnalité”, Pouvoirs No:67, novembre 1993, p.79 – 97.
- VOIGT Paul/Von Dem BUSSCHE Axel: The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer International Publishing, Switzerland 2017.
- VON GRAFENSTEIN, Maximilian: “Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the “state of the art” of data protection-by-design”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990, (e.t. 09.10.2022)
- YILDIZ, Elif: Kişisel Verilerin Korunması Hukuku, Bilge Yayınevi, Ankara 2021.
- YILDIZ, Sevil: Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, Nobel Yayınevi, Ankara 2007.

YILMAZ, Berrak: Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi

Kararları Işığında Kişisel Verilerin Korunması, Yetkin Yayınevi, Ankara 2022.

YILMAZ, Ozan Barış: Türkiye ve Avrupa Birliği'nde Kişisel Verilerin Korunması ve

Uygulanacak Hukuk, Adalet Yayınevi, Ankara 2022.

YİĞİT, Esra: İş İlişkisinde Kişisel Verilerin Korunması, Oniki Levha Yayınları,

Güncellenmiş 2. Basım, İstanbul 2023.

YÜKSEL, Birsen: Akreditasyon Süreçlerinde İş Zekası Uygulaması: Bir Kamu Kurumu

Örneği, Yayınlanmış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü,

Ankara 2019.

YÜZBAŞI TOBAZ, Firdevs: Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda

Kişisel Verilerin Korunması, Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü

Kamu Hukuku Anabilim Dalı, Doktora Tez, Trabzon 2021.



EKLER

EK A. ÖZGEÇMİŞ

İsim Soyisim: Ali Osman Özdilek

Eğitim:

- 2018 - 2024 Özyeğin Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku
Doktora Programı
- 2015 - 2017 Fribourg Üniversitesi Hukuk Fakültesi Uluslararası Sözleşmeler ve
Tahkim Tezli Yüksek Lisansı (İsviçre)
- 1994 - 1998 İstanbul Üniversitesi Hukuk Fakültesi
- 1990 -1994 Japan International Cooperation Agency (JICA) Projesi Tuzla Teknik
Lisesi Bilgisayar Bölümü

Sertifikalar:

- CIPP/E (Avrupa Sertifikalı Veri Mahremiyeti Profesyoneli)
- ISO 27001 Bilgi Güvenliği Yönetim Sistemi Baş Denetçi

İş Deneyimi:

- Ocak 2019: AKHADIA HOLDİNG B.V
JURCOM GRC SERVICES B.V.
JURCOM TEKNOLOJİ A.Ş.
IDENTECH TEKNOLOJİ A.Ş.
ALİST ELEKTRONİK HİZMETLER VE EĞİTİM LTD. ŞTİ.
Kurucu
- Eylül 2017: Özyeğin Üniversitesi
Yarı Zamanlı Öğretim Görevlisi
*Hukuk Fakültesi'nde "Bilişim Hukuku" dersi ve Uygulamalı Bilimler
Yüksek Okulunda ingilizce "Uluslararası Çalışma Hukuku" dersi*
- Nisan 2007: Özdilek Hukuk Bürosu
Avukat/Büro Ortağı
- Mart 2005 - Mayıs 2007: Digital Platform İletişim Hizmetleri A.Ş.
Hukuk Müşaviri
- Eylül 2004- Mart 2005: NET Hukuk Bürosu
Bilişim Hukuku Danışmanı

Eylül 2003 - Eylül 2004: Özdilek Hukuk Bürosu
Ortak

Mart 2000 – Temmuz 2001: Türk Silahlı Kuvvetleri
Subay

Ağustos 1999 – Mart 2000: TURHAN&TURHAN Hukuk Bürosu
Avukat

Haziran 1998 – Ağustos 1999: Av. Suat Narin
Stajyer Avukat

Kitaplar:

- “İnternet ve Hukuk”, Papatya Yayıncılık, 240 sayfa, İstanbul, 2002
- “A’dan Z’ye Uygulamalı Sözleşme Örnekleri”, 1. Baskı, Vedat Kitapçılık, 2578 sayfa, 3 cilt, İstanbul, 2004.
- “A’dan Z’ye Uygulamalı Sözleşme Örnekleri”, 2. Baskı, Vedat Kitapçılık, 3805 sayfa, 4 cilt, İstanbul, 2005.
- “Bilişim Suçları ve Hukuku”, Vedat Kitapçılık, 246 sayfa, İstanbul 2006.
- “Çin Halk Cumhuriyeti’nin Dünya Ticaret Örgütü’ne Katılım Süreci Kapsamında Çin Malları ve Damping – Haksız Rekabet Düzenlemeleri”, Asansör ve Yürüyen Merdiven Sanayicileri Derneği (AYSAD) Yayını, 250 sayfa, İstanbul, 2007.
- “Türk Asansör Hukuku”, Asansör ve Yürüyen Merdiven Sanayicileri Derneği (AYSAD) Yayını, İstanbul, 2007.
- “International Electronic Evidence”, Stephen Mason ile birlikte, British Institute of International and Comparative Law Yayını, 2008.
- “A’dan Z’ye Uygulamalı Sözleşme Örnekleri”, 3. Baskı, Bilge Yayınevi, 4521 sayfa, 4 cilt, Ankara, 2013.
- “Anonim Şirketlerde Genel Kurula Elektronik Ortamda Katılım ve Bu Katılımın Yokluk ve Butlan Açısından Değerlendirilmesi”, Seçkin Yayınevi, İstanbul, 2017.
- “A’dan Z’ye Uygulamalı Sözleşme Örnekleri”, 4. Baskı, Platon Yayınevi, 4390 sayfa, 4 cilt, İstanbul, 2023.