# ULUSLARARASI HUKUKTA

# KİŞİSEL VERİLERİN KORUNMASI

**Yüksek Lisans Tezi**

**Akif SADIK**

**Eskişehir 2020**

# ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

**Akif SADIK**

**YÜKSEK LİSANS TEZİ**

**Kamu Hukuku Anabilim Dalı**

**Danışman: Doç. Dr. Elif UZUN**

**Eskişehir**

**Anadolu Üniversitesi**

**Sosyal Bilimler Enstitüsü**

**Mayıs 2020**

**JÜRİ VE ENSTİTÜ ONAYI**

# ÖZET


ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

Akif SADIK

Kamu Hukuku Anabilim Dalı

Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Mayıs 2020

Danışman: Doç. Dr. Elif UZUN

Mahremiyet, insanlığın var oluşundan bu yana insanlığın temel sorunlarından biri haline gelmiştir. İlkçağlardaki insanlarda görülen yemek, barınmak gibi temel ihtiyaçların yanında korunma ihtiyacının da ön plana çıktığı görülmektedir. İnsanın doğal içgüdüsü gereği var olan kendini muhafaza ihtiyacı, zamanla kendisine ait bilgilerin de korunması ihtiyacına dönüşmüştür. Çalışmamızın kişisel verilerin tarihsel gelişimine yer verdiğimiz kısmında da değineceğimiz üzere kişilerin bilgilerinin korunmasına duyduğu ihtiyacın başlangıcının bazı meslek sahiplerinin sır saklama yükümlülüğü olduğu görülmektedir.

Bilgisayar teknolojisinin geliştiği tarihlere kadar insanlığın bu bilgi koruma güdüsüne ‘kişisel verilerin korunması’ adını vermedikleri görülmektedir.

Devletlerin vatandaşlarının kişisel verilerinin korunması noktasında duydukları bu kaygılara kayıtsız kalamamaları ile kişisel verilerin korunması konusunda uluslararası mevzuatın oluşmaya da başladığı görülmektedir.

Çalışmamızda kişisel verilerin korunmasına ilişkin bazı temel bilgilere, kişisel verilerin korunmasında insanlığı bugünkü seviyeye ulaştıran tarihsel sürece ve uluslararası alanda veri korumaya yönelik yasal düzenlemelere yer verilmiştir.



**Anahtar Sözcükler:** Kişisel veri, Kişisel verilerin korunması, Veri koruma yönergesi, 108 sayılı Sözleşme, AB genel veri koruma tüzüğü.

## ABSTRACT

PROTECTION OF PERSONAL DATA IN INTERNATIONAL LAW

Akif SADIK

Department of Public Law

Anadolu University, Institute of Social Sciences, May 2020

Consultant : Assoc. Prof. Elif UZUN

Privacy has become one of the main problems of humanity since the existence of humanity. It is seen that the need for protection comes to the forefront in addition to basic needs such as food and shelter seen in people in ancient times. The need for self-preservation, which is required by the natural instinct of man, has turned into the need to protect its own information over time. As we will mention in the part of our study that we include the historical development of personal data, it is seen that the beginning of the need for the protection of the information of individuals is the obligation of some professionals to keep secrets.

Until the development of computer technology, it is seen that humanity did not call this information protection motive 'protection of personal data'.

With the inability of states to remain indifferent to these concerns regarding the protection of their citizens' personal data, it is observed that international legislation on the protection of personal data has started to emerge.

In our study, some basic information about the protection of personal data, the historical process that brought humanity to the present level in the protection of personal data, and legal regulations for data protection in the international area are included.



**Keywords:** Personal data, Protection of personal data, Data protection directive, contract number 108, EU general data protection regulation.

## ÖNSÖZ

Araştırmanın temel amacı, kişisel verilerin korunması hukukunun ortaya çıkışı, tarihsel gelişimi ve uluslararası hukuktaki koruma mekanizmalarını irdelemektir.

Araştırmanın kaynakları, araştırmanın konusundan da anlaşılacağı üzere kişisel verilerin korunması konusundaki temel uluslararası mevzuattır.

Tüm eğitim hayatımda olduğu gibi yüksek lisans eğitimimde de desteklerini daima yanımda hissettiğim aileme şükranlarımı sunarım.

Kendisine duyduğum minnettarlığımı ve şükran duygumu kelimelerle anlatmamın mümkün olmadığı, tez çalışmamın her safhasında desteğini esirgemeyen, iyi bir başlangıcın iyi neticeyi doğuracağına inanmış biri olarak akademik hayatıma iyi bir başlangıç yapmama vesile olan, belirsizliklerle dolu olduğunu düşündüğüm bu yolda beni yalnız bırakmayan, akademik hayatın basamaklarını tamamlama isteğimin oluşmasının en önemli sebebi olan saygıdeğer danışman hocam Doç. Dr. Elif UZUN'a çok teşekkür ederim.

29/04/2020

## ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Akif SADIK

## İÇİNDEKİLER

**Sayfa**


**BAŞLIK** ..... **i**
**JÜRİ VE ENSTİTÜ ONAYI** ..... **ii**
**ÖZET** ..... **iii**
**ABSTRACT** ..... **iv**
**ÖNSÖZ** ..... **v**
**ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ** ..... **vi**
**İÇİNDEKİLER** ..... **vii**
**KISALTMALAR DİZİNİ** ..... **x**
**GİRİŞ** ..... **1**
**BİRİNCİ BÖLÜM** ..... **3**
**1.KİŞİSEL VERİLERİN KORUNMASI HUKUKUNA GİRİŞ** ..... **3**
**1.1.Kişi Kavramı** ..... **3**
**1.2.Kişisel Veri Kavramı** ..... **3**
**1.3.Hassas Veri Kavramı** ..... **5**
**1.4.Kişisel Verilerin İşlenmesi** ..... **5**
**1.5.Kişisel Verilerin Korunması Hukukunun Tarihsel Gelişimi** ..... **6**
**1.6.Kişisel Verilerin Korunması Hakkına İlişkin Görüşler** ..... **11**
**1.6.1.Ekonomik hak görüşü** ..... **11**
**1.6.2.İnsan hakkı görüşü** ..... **15**
**İKİNCİ BÖLÜM** ..... **19**
**2.KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN ULUSLARARASI KAYNAKLARI** ..... **19**
**2.1.Genel Olarak** ..... **19**
**2.2.İnsan Hakları Evrensel Bildirgesi** ..... **20**
**2.3. Avrupa İnsan Hakları Sözleşmesi** ..... **21**
**2.4. Uluslararası Medeni ve Siyasi Haklar Sözleşmesi** ..... **22**
**2.5. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Özel Yaşamın Korunması Ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri** ..... **23**
**2.6.108 Sayılı Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi** ..... **26**
**2.7. 45/95 sayılı Birleşmiş Milletler Bilgisayarla İşlenen Veri Dosyalarıyla İlgili Rehber İlkeler** ..... **33**

**Sayfa**

**2.8. 95/46 Sayılı Avrupa Parlamentosu ve Avrupa Konseyi Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Yönergesi (Avrupa Topluluğu Veri Koruma Yönergesi)..... 35**

**2.8.1.Veri koruma yönergesinin amacı..... 35**

**2.8.2.Temel kavramlar..... 37**

**2.8.3.Veri koruma yönergesinin uygulama alanı ve ilkeleri..... 39**

**2.8.4. Hukuka uygunluk sebepleri..... 41**

**2.8.5. Hassas verilerin işlenmesi..... 43**

**2.8.6. İlgilinin haberdar edilmesi ilkesi ve ilgilinin hakları..... 47**

**2.8.7. İstisnalar, sınırlamalar ve kişi hakkında otomatik surette verilen kararlar..... 52**

**2.8.8. Kişisel verilerin işlenmesinde usule dair ilkeler..... 53**

**2.8.9.Ön kontrol(ön denetim) ve işlem aleniyeti..... 56**

**2.8.10.Yargı yolu, sorumluluk ve yürürlüğe koyma yükümlülüğü..... 57**

**2.8.11.Üçüncü ülkelere veri transferi ve davranış kuralları..... 58**

**2.8.12.Veri koruması denetim organları ve iç hukuka aktarma..... 61**

**2.9.97/66 sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi ve 2002/58 Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi..... 63**

**2.10.OECD Küresel Ağlarda Mahremiyetin Korunması Konusunda Bakanlık Bildirgesi..... 66**

**2.11. 99/5 Sayılı Avrupa Konseyi Bakanlar Komitesi İnternet Ortamında Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı..... 66**

**2.12.2000/31 Sayılı Elektronik Ticaret Yönergesi..... 67**

**2.13.Avrupa Birliği Temel Haklar Bildirgesi..... 67**

**2.14.2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü..... 68**

**2.14.1. Amaç ve kapsam..... 69**

**2.14.2.Tanımlar..... 71**

**2.14.3.Kişisel verilerin işlenmesine ilişkin ilkeler..... 75**

**2.14.4.Kişisel verilerin işlenmesinin hukuka uygunluk şartları..... 79**

**2.14.5. Özel nitelikteki kişisel verilerin işlenmesi açısından hukuka uygunluk halleri (hassas verilerin işlenmesi)..... 86**

**Sayfa**

**2.14.6.Yurtdışına aktarım halinde hukuka uygunluk halleri ..... 88**
**2.14.7.Kişisel veri sahibinin hakları ..... 92**
**2.14.8.Veri sorumlularının yükümlülükleri ..... 102**
**2.14.9.İlgili kişilerin haklarının korunması ..... 113**
**2.14.10.Denetim makamları ..... 118**
**2.14.11. Avrupa veri koruma kurulu ..... 126**
**SONUÇ ..... 131**
**KAYNAKÇA ..... 135**
**ÖZGEÇMİŞ**

## KISALTMALAR DİZİNİ

**AB:** Avrupa Birliği

**ABAD:** Avrupa Birliği Adalet Divanı

**AİHM:** Avrupa İnsan Hakları Mahkemesi

**AİHS:** Avrupa İnsan Hakları Sözleşmesi

**AK:** Avrupa Konseyi

**AT:** Avrupa Topluluğu

**BM:** Birleşmiş Milletler

**C:** Cilt

**ETS 108:** Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Avrupa Konseyi Sözleşmesi)

**GDPR:** (AB) 2016/679 sayılı ve 27 Nisan 2016 tarihli Gerçek Kişilerin Kişisel Verilerinin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin 95/46/AT sayılı AB Yönergesi'ni Yürürlükten Kaldıran Avrupa Parlamentosu ve Konsey Tüzüğü (AB Genel Veri Koruma Tüzüğü, Tüzük)

**m:** Madde

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

**VKY:**95/46 EC sayılı Veri Koruma Yönergesi

**EİVKY:** 2002/58 Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi

**TKVKY:** 97/66 sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi

**S:** Sayı

**s:** Sayfa

**vd:** ve devamı

**bkz.:** bakınız

## GİRİŞ

İnsanlığın ortaya çıkışından bu yana temel ihtiyaçları olduğu görülmektedir. Bu ihtiyaçlardan bazıları ilkçağdan bu yana varlığını sürdürmekteyken bazıları da zamanla ihtiyaç haline gelmiş veya ihtiyaç algısı oluşturulmuştur. Örneğin yemek, barınmak, korunmak gibi ihtiyaçların medeniyetin gelişmesiyle ortadan kalktığını söylemek mümkün değildir. Belki sadece bu ihtiyaçların karşılanma süresinde ve yönteminde bir takım gelişmeler kaydedildiği söylenebilir.

Kişisel verilerin korunmasının tarihsel gelişimi irdelendiğinde bir ihtiyaç haline gelmesinin 20.yy'ın ortası olduğu görülmektedir. Çünkü bu tarihler bilgisayar teknolojisinin gelişmeye başladığı tarihlerdir. Bilgisayarın ortaya çıkışıyla ve devam eden süreçte geliştirilmesiyle veri akışlarındaki hız artmış ve kontrol edilmesi zorlaşmıştır. Ancak bu tarihler aynı zamanda veri akışının kaçınılmaz hale geldiği tarihlerdir. Zira süreç veri paylaşmanın kaçınılmaz hale gelmesine evirilmiştir. Devletlerin ekonomik kaygılarla veri aktarımını engellemekten kaçınmaları ve vatandaşların mahremiyetlerinin korunmasına yönelik taleplerinin birleşmesiyle devletler, gerek ulusal düzeyde gerekse uluslararası düzeyde kişisel verilerin korunması mevzuatı oluşturma çabasına girişmişlerdir.

Tek başına bir ülkenin kişisel verilerin korunması konusunda adım atması ile kişisel verilerin korunmasında etkili olması ve yeterli düzeyde koruma sağlaması mümkün değildir. Çünkü küreselleşen dünyada ekonomik olarak ayakta kalmanın ön şartı diğer ülkelerle etkileşim halinde olmaktır. Bu etkileşim, doğal olarak yurtdışına veri aktarımı ihtiyacını beraberinde getirecektir. Durum böyleyken bir devletin ekonomik ilişki kurduğu devletlerin veri koruma düzeyine ilişkin de önlem alması gerekir. Bir devletin diğer devletin mevzuatını oluşturması devletler hukukuna göre mümkün olmadığı için bu konudaki ihtiyacı uluslararası veri koruma mevzuatlarıyla çözmekten başka bir yol kalmamaktadır.

İşte bu eşdeğer veri koruma düzeyinin sağlanması ihtiyacı ile kişisel verilerin korunmasına ilişkin uluslararası mevzuatın da oluşmaya başladığı görülmektedir. Devletlerin kişisel verilerin korunmasına yönelik bu çabalarında insan haklarına duydukları saygıdan ziyade kişisel verilerin korunması hususunu ekonomik gelişmelerine engel görerek bu engelin kaldırılmasını istemelerinde aramak gerekir.

Ancak zamanla uluslararası mevzuattaki güncellemeler ile insan hakları odaklı bir veri koruma mevzuatının da oluşmaya başladığı görülmektedir.

Çalışmamız iki bölümden oluşmaktadır. Birinci bölümde kişisel verilerin korunmasına ilişkin temel kavramlara, kişisel verilerin korunmasına ilişkin görüşlere ve kişisel verilerin korunmasının sorun olarak ortaya çıkmasından çözüm üretilme safhasına kadar süren tarihsel gelişime yer verilmiştir. Kişisel verilere ilişkin temel kavramlar açıklanarak kişisel verilerin korunmasına ilişkin uluslararası kaynakların anlaşılması sağlanmaya çalışılmıştır. Kişisel verilerin korunmasına ilişkin görüşlerden eleştirilen yönleriyle bahsedilerek bu görüşlerin objektif bir şekilde karşılaştırılmasına imkân sağlanmak istenmiştir. Kişisel verilerin korunması hukukunun tarihsel gelişimi ile kişisel verilerin korunması sorununun ortaya çıkışından çözüm üretme safhasına kadar ilerleyen süreç ortaya konmuştur. Bu sayede kişisel verilerin korunması amacıyla hazırlanan uluslararası mevzuatların hangi gerekçelerle bugünkü halini aldığı gösterilmek istenmiştir.

İkinci bölümde kişisel verilerin işlenmesiyle ilgili belli başlı uluslararası mevzuat irdelenmiştir. Uluslararası düzenlemelerin birbiriyle ilişkisi ortaya konularak veri korumanın bugüne gelirken geçirdiği evreler göz önüne serilmiştir. Uluslararası mevzuatın kişiler verilerin korunması yolunda getirdiği yeniliklere dikkat çekilmiştir. Uluslararası mevzuatın getirilme amacı ile ilgili bilgi verilmiştir. Mevzuatın bireylerin verilerini koruma açısından devletlere ve bireylere gösterdiği usul ve esaslara yer verilmiştir.

Esasında bu çalışma ile kişisel verilerin sorun olarak ortaya çıkışı, ortaya çıktığı şartlar, ortaya çıktığı zaman ve yerler, çözüm bulunma çabaları, kişisel verileri koruma düzeyi açısından geçmiş-gelecek farkı, gelinen noktada ulaşılan seviye ve atılması gereken adımlar gözler önüne serilmiştir.

# BİRİNCİ BÖLÜM

## 1.KİŞİSEL VERİLERİN KORUNMASI HUKUKUNA GİRİŞ

### 1.1.Kişi Kavramı

Veri hukukunda kişi kavramını irdelemeden önce genel anlamda hukukta kişi kavramının karşılığına değinmek gerekir. Hukukumuzda kişi hak ehliyetine sahip varlığı ifade eder.

4721 sayılı yasanın 8. maddesinde sadece insandan bahsetse de hukukumuz, insan dışında varlıkları kişi olarak görmüş; onlara hak ehliyeti vermiştir. Burada karşımıza gerçek kişi ve tüzel kişi ayrımı çıkmaktadır. Hukukumuzda gerçek kişinin tek karşılığı insandır. İnsan dışındaki hak ehliyeti sahibi olanlara ise tüzel kişiler denir. Tüzel kişilikler mal ve kişi toplulukları olarak karşımıza çıkmaktadır. Nitekim Medeni Kanunun 47. maddesinin 1. fıkrası, "*Başlı başına bir varlığı olmak üzere örgütlenmiş kişi toplulukları ve belli bir amaca özgülenmiş olan bağımsız mal toplulukları, kendileri ile ilgili özel hükümler uyarınca tüzel kişilik kazanırlar*." ve 48. maddesi "*Tüzel kişiler, cins, yaş, hısımlık gibi yaradılış gereği insana özgü niteliklere bağlı olanlar dışındaki bütün haklara ve borçlara ehildirler*." şeklinde düzenlenmiştir.

Çalışmanın ilerleyen bölümlerinde de görülecektir ki uluslararası hukukta kişisel verilerin korunması mevzuatının da kişi kavramına bakışı yukarıdaki açıklamalar doğrultusundadır.

### 1.2.Kişisel Veri Kavramı

Kişisel sözcüğünün Türk Dil Kurumu(TDK) Türkçe sözlüğünde "*Kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan*" şeklinde anlamları karşımıza çıkmaktadır.[1] Veri sözcüğünün ise TDK'nin sözlüğündeki anlamlarından biri bilgidir.[2] Bu iki tanımdan yola çıkarak kişisel verinin kişiye ait, kişiye ilişkin, kişinin malı olan her türlü bilgi şeklinde tanımını yapılabilir. Fakat bu tanımın bu çalışmanın konusu olan kişiler verilerin korunması hukuku açısından kişisel veri kavramını tam olarak karşıladığı söylenemez.

[1]http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5bd5c87b20ae83.54428221 (Erişim Tarihi:28.10.2018)
[2]http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5bd5c48c0f5de8.54075063 (Erişim Tarihi:28.10.2018)

Kişisel veriyi koruma altına alan yerel ve milletlerarası düzenlemelerde kişisel veri için belirli bir tanım yapıldığı görülmektedir. Avrupa Konseyi(AK)'nin verilerin korunması için yürürlüğe koyduğu 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nde[3] kişisel veriler, "*kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm veriler*" olarak tanımlanmıştır (M.2).[4] 95/46 sayılı Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Yönergesi[5] tarafından benzer bir tanım yapıldığı görülmektedir.[6]

Kişisel verinin 2016/679 sayılı Tüzük'teki tarifi "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" şeklindedir(M.4). Tüzük'ün 4. maddesinde belirlenebilir gerçek kişinin tanımı, "*bir tanımlayıcıya, örneğin ismine, kimlik numarasına, konum bilgisine, bir çevrimiçi tanımlayıcıya ya da bu kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ilişkin bir veya birden fazla etkene referans yaparak doğrudan veya dolaylı olarak belirlenebilen kişi*" şeklindedir.[7]

Veri koruma hukukunun temel konusunu belirli yahut belirlenebilir gerçek şahısların verileri oluşturmaktadır. Çünkü veri koruma hukukunun ortaya çıkışında gerçek kişi olan insanın temel insan haklarını koruma güdüsü etkili olmuştur. Uluslararası hukukta kişisel veri koruma mevzuatı incelendiğinde de esasen korunma altına alınmak istenenin belirli veya belirlenebilir gerçek kişilere ait veriler olduğu görülmektedir.

Bir gerçek kişinin belirlenebilir olması o kişi hakkındaki bazı bilgilerle o kişinin kimliğinin belirlenebilir olması anlamına gelmektedir. Diğer bir anlatımla kişisel veriler; veri sahibine özgü, veri sahibinin kimliğinin ek bir araştırma çabasına girmeden tespitini mümkün kılan verilerdir. Belirlenebilir bir gerçek kişinin tespit edilmesiyle de bu kişinin belirli bir kişi haline geldiğini söylemek mümkündür.

---

[3]Çalışmanın devamında kısaca "Sözleşme" olarak atıfta bulunulacaktır.
[4]Sözleşme metni için bkz. 17 Mart 2016 Tarihli ve 29656 Sayılı Resmî Gazete
[5]Çalışmanın devamında kısaca "Yönerge" olarak atıfta bulunulacaktır.
[6]https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (Erişim Tarihi:5.11.2018) Bu Yönerge'de veri , "*bireye ait tanımlanmış yahut tanımlanabilir herhangi bir bilgi*" olarak tarif edilmiştir.
[7]Tüzük'ün Türkçe çevirisi için bkz. H. M. Develioğlu (2017) . 6698 sayılı Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku. İstanbul : On İki Levha Yayıncılık, 173-286.

### 1.3.Hassas Veri Kavramı

Hassas veri, mahiyeti gereği daha fazla korumaya tabi tutulan kişisel verilerdir.[8]

Hassas veri, kişisel verilerin korunmasına yönelik uluslararası belgelerde çeşitli şekillerde düzenlenmiştir. Hassas veri, bu belgelerde çeşitli isimler altında düzenleme altına alınmıştır.

Hassas veri; Sözleşme'nin "özel veri kategorileri" başlıklı 6. maddesinde, *"İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı şey ceza mahkûmiyetiyle ilgili veriler için de geçerlidir*" şeklinde düzenlenmiştir.[9]

Görüldüğü üzere Sözleşme açısından hassas veriler; kişinin ırksal kökeni, siyasi düşüncesi, inancı, sağlık verileri, cinsel hayat verileri, ceza hükümleri ile bağlantılı verilerdir.

Yönerge'nin "Verilerin Özel İşleme Kategorileri" başlığı altındaki 8. maddesi; "*Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır."* şeklinde düzenlenerek hassas veriler örtülü olarak sıralanmıştır.[10]

### 1.4.Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesinin ne anlama geldiği hususunda uluslararası düzenlemeler yol gösterici olmuştur.

İşleme, "*silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan*

[8]C. KAYA (2011) . A*vrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve İşlenmesi*. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası. 69 (1-2) , 317-334, 318.
[9]Sözleşme metni için bkz. 17 Mart 2016 Tarihli ve 29656 Sayılı Resmî Gazete
[10]https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML(Erişim Tarihi:16.03.2019);Türkçe Çevirisi için bkz. https://kisiselveri.com/9546ec-turkce (Erişim Tarihi:16.03.2019)

*araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisi*" olarak tanımlanmıştır.[11]

Bir verinin işlenmesinin otomatik ve otomatik olmayan işleme olmak üzere iki yolu vardır. Sözleşme'de sadece otomatik olarak kişisel verilerin işlenmesi tanımlanmış olup, Sözleşme'nin 2. maddesinde otomatik işlem, "*tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi ve dağıtılması*" olarak tanımlanmıştır.

Tüzük'te[12] ise Sözleşme'de olduğu gibi bir otomatik işlem veya otomatik olmayan işlem ayrımı yapılmadığı görülmektedir. Buna göre Tüzük'te kişisel verilerin işlenmesi, "*otomatik vasıtalarla olsun veya olmasın, kişisel veriler veya kişisel veri setleri üzerinde elde etme, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, erişme, başvurma, kullanma, yayınlamak, yaymak veya diğer şekilde ulaşılabilir hale getirmek suretiyle ifşa etme, sıralama veya birleştirme, sınırlama, silme veya imha etme gibi faaliyet veya faaliyet setleri*" olarak tanımlanmıştır(M.4).

### 1.5.Kişisel Verilerin Korunması Hukukunun Tarihsel Gelişimi

Öğretide kişisel verilerin korunmasının temeli tarihsel açıdan bazı meslek gruplarının sır saklama yükümlülüğüne dayandırılmaktadır.[13] Sır saklama yükümlülüğünü tarihsel açıdan diğerlerinden önce üstlenen meslek grubu hekimlerdir. Geçerliliğini bugün bile sürdüren hekimin sır saklama yükümlülüğü Hipokrat yemininde konu edinilmiştir.[14] Bu yükümlülüğün hekimlere yüklenilmesinde iki yarar öngörülmüştür. Birincisi hastaların hastalıklarının bilinmesi suretiyle toplumda sosyal açıdan zarar görmemesi, ikincisi ise toplumda hekime olan güvenin sağlanmasıdır.

---

[11]https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML(Erişim Tarihi:16.03.2019);Türkçe Çevirisi için bkz: https://kisiselveri.com/9546ec-turkce (Erişim Tarihi:16.03.2019)

[12]AB Genel Veri Koruma Tüzüğünden kısaca 'Tüzük' olarak bahsedilmiştir.

[13]O. Şimşek(2008). Anayasa Hukukunda Kişisel Verilerin Korunması., İstanbul: Beta Yayınları, 5.

[14]Hipokrat yemininde hekimin sır saklama yükümlülüğü ile ilgili kısım şöyledir:
"Gerek hastanın tedavisi sırasında gerekse tedavi dışında olsun gördüğüm ve duyduğum [ama] dışarıda konuşulmayacak olan insanların tasarrufundaki şeyleri saklayacak ve buna benzer şeyleri konuşmayacağım." İ, Altuner(1990). *Hipokrat Yemini*. Iğdır Üniversitesi Sosyal Bilimler Dergisi. S:7, s.1-7. http://sosbilder.igdir.edu.tr (Erişim Tarihi:07.02.2019)

Din adamı, bankacı, avukat gibi meslekler de hekimlerden sonra sır saklama yükümlülüğünü taşıyagelmişlerdir.[15] Fakat ilerleyen süreçte kamu yararı gibi bazı sebeplerle bu meslek erbaplarının sır saklama yükümlülüklerinde istisnalar öngörülmüştür.

Günümüzdeki anlamıyla kişisel verilerin korunmasının bir gereksinim haline gelmesine teknolojik gelişmeler karşısında bireyin korunması gerektiği düşüncesi sebep olmuştur. Bunun ilk örneği olarak 1960'lı yıllarda gelişmeye başlayan bilgisayar teknolojisi karşısında bireylerin korunması ihtiyacının oluştuğu ABD gösterilebilir. O dönemde ABD'de kişinin banka kredisi alabilmesi, toplumda saygınlık belirtisi sayılmaktaydı. Fakat kredi alabileceklerin bilgisayar tarafından seçilmesi ve bilgisayarın yaptığı seçimlerde hataların olduğunun belirlenmesi karşısında kamuoyunda kişisel verilerin doğru tutulmadığı yönünde endişeler ortaya çıktı. Devamında ülkede bütün yurttaşların bilgilerinin tek bir havuzda toplandığı bir merkezin kurulmasının tartışılması, bireylerin özel hayatın korunması konusundaki endişelerini artırdı. Fakat bu veri bankasının özel yaşamı korumayacağı fikrini savunan toplumsal muhalefet sayesinde bu fikir hayata geçirilemedi. Bu endişeler devam ederken ABD ordusunun siyasi şüpheliler başta olmak üzere gerçek kişiler hakkında veri topladığına dair haberler ortaya çıktı. Toplumda kamusal organların çeşitli vasıtalarla özel yaşama müdahale edebileceği korkusu yayılmaya başladı.[16]

Veri havuzu oluşturulması ile ilgili faaliyetler, çeşitli ülkelerde görülmeye başlamıştır. Örneğin 1960'lı yıllarda İsveç'te nüfus ve vergi sicillerinin toplandığı elektronik veri havuzu kurulmuştur. Bunun dışında Doğu ve Batı Almanya'nın birleşmesinden sonra 1972 yılından beri Doğu Almanya'da halka ait kişisel bilgileri kaydetmek için bir veri sisteminin kurulmuş olduğu dile getirilmiştir. Yine Moskova'da yer alan, halkı kategorik olarak sınıflandıran veri bankalarının varlığından söz edilmiştir.[17]

İsviçre ve Almanya gibi kişisel verilerin kaydedildiği veri bankalarının kurulmasının oluşturduğu tedirginlik, insanların hürriyetlerine sahip çıkma refleksi göstermelerine sebep olmuştur. Devamında yaşanan teknolojik gelişmelerle bu

[15]bkz. 5411 sayılı Bankacılık Kanunu M. 73 ve 1136 sayılı Avukatlık Kanunu M. 36
[16]Şimşek , 2008 , **a.g.k.** , 8.
[17]Şimşek , 2008 , **a.g.k.** , 9.

tedirginlik daha da artış göstermiştir. Dolayısıyla kişiler, kişisel verilerinin kendi talepleriyle korunması gerektiğini kabul etmişlerdir.[18] Netice itibariyle veri bankaları kurulması fikri, özel yaşamına saygı duyulmasını talep eden toplumlar tarafından sert muhalefetle karşılaştığından amaçlanan başarıya ulaşamamıştır.

Fakat 1970li yıllardan sonra teknolojik gelişme bir başka boyuta evirilmiştir. İlk başta devasa, gözle görülebilir olan veri kayıt odaklı büyük bilgisayarların yerini küçük bilgisayar sistemlerinin almasıyla kişisel verilerin kaydedildiğinden toplumun haberdar olmaktan uzaklaşması söz konusu olmaya başlamış, bu durum veri kaydedicilerin işini kolaylaştırmıştır. Bu durumda kişisel verilerin korunmasının teknoloji karşısında bireyi korumaktan ziyade bir vatandaşlık hakkı olduğu tezi öne sürülmüştür. Bu açıdan kişisel verinin korunmasında toplumsal bir tepki yerine bireyin şahsi hak arama mücadelesinin etkili olacağı fikri ortaya çıkmıştır.[19]

Teknolojideki bu dönüşümün kamusal organların bireylerin özel yaşama müdahalesini kolaylaştırmasıyla birlikte toplumda kişisel verilerin korunmasını sağlayan yasal düzenlemelerin getirilmesi talebi yaygınlaşmaya başlamıştır. Bu taleplerin karşılanması yolunda ilk adımlar 1970'li yıllarda atılmaya başlanmıştır.[20]

Fakat teknolojinin geliştiği 1970'li yıllardan önce, 1948 tarihli İnsan Hakları Evrensel Bildirgesi'nin "*Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır*." şeklinde düzenlenen maddesinin, Avrupa İnsan Hakları Sözleşmesi'*(*AİHS*)* nin "*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir*" şeklinde düzenlenen maddesinin[21] ve mahremiyet hakkının koruma altına alındığı 1966 tarihli Kişisel ve Siyasi Haklar Uluslararası Sözleşmesi'nin 17. maddesinin[22] 1970li yıllarda başlayan kişisel verilerin korunmasına yönelik yasalaşma sürecinden önce çıkmış ilk yazılı düzenlemeler olduğu söylenebilir.

---

[18]Y. Çelik. (2017). *Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı*. Türkiye Adalet Akademisi Dergisi. (32) , 391-410, 397.
[19]Şimşek, 2008 , **a.g.k. ,** 9, 10**.**
[20]D. Kılınç (2012) . *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*. Ankara: Ankara Üniversitesi Hukuk Fakültesi Dergisi; C. 61, S. 3, 1089-1170, s.1103; Şimşek, 2008 , **a.g.k**. , 10.
[21]https://www.echr.coe.int/Documents/Convention_TUR.pdf (Erişim Tarihi:23.02.2019); Sözleşmenin Türkçe çevirisi için bkz.19 Mart 1954 tarihli ve 8662 sayılı Resmi Gazete
[22]https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708(Erişim Tarihi:26.02.2019) Sözleşmenin Türkçe çevirisi için bkz. 21 Temmuz 2003 Tarihli ve 25175 Sayılı Resmi Gazete

1970 yılında ABD'de yürürlüğe giren dürüst kredi raporlama kanunu, kişisel verilerin korunmasının yasal güvence altına alınma sürecinin ilk adımıdır. Fakat genel anlamda verilerin korunmasına yönelik ilk kanunun 1970 yılında Hessen eyaletinde[23] yürürlüğe girdiği görülmektedir. Devam eden süreçte İsveç'te, 1973 tarihli Veri Koruma Kanunu'nun, ABD'de 1974 tarihli Özel Alanın Korunması Kanunu'nun, Kanada'da 1977 tarihli İnsan Hakları Kanunu'nun ve Fransa'da 1978 tarihli Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına İlişkin Kanunu'nun yürürlüğe sokulması, veri korumanın yasalaşması sürecinde atılan diğer adımlar olarak gösterilebilir.[24]

Ülkesel bazda veri koruma ihtiyacını gidermeye yönelik yasalaşma süreçlerinin Avrupa'da başlaması, uluslararası alandaki yasalaşma sürecinin temelinin Avrupa kıtasında atılmasının da temelini oluşturmuştur. Bu anlamda Avrupa'da, uluslararası alanda veri korumanın yasalaşması 1980li yıllarda başlamıştır.

1980'de Ekonomik İşbirliği ve Kalkınma Örgütü tarafından(OECD), bağlayıcı olmasa da ileride uluslararası veri koruma mevzuatına temel olacak olan Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler kabul edilmiştir.[25]

1981'de kabul edilen Sözleşme, veri korumasına yönelik uluslararası yasalaşma sürecinin ilk adımı olduğu gibi birçok ülkenin kişisel verilerin korunmasına yönelik oluşturacağı mevzuatın da kılavuzluğunu üstlenmiştir. En başında Sözleşme tarafı ülkeler, sözleşmeyi imzalamakla iç hukuklarında kişisel verilerin korunmasına yönelik mevzuat oluşturmayı taahhüt etmişlerdir.[26]

Sözleşme'den sonra veri koruma hukukunun yasalaşma süreci yeni bir yol izlemeye başlamıştır. Mevcut kanunlar Sözleşme'den sonra güncellenmeye, yeni kanunlar Sözleşme'ye göre düzenlenmeye başlamıştır.

Devamında ortaya konulan uluslararası düzenlemeler şöyle sıralanabilir:

[23]Hessen, Almanya'da bir eyalettir.
[24]Şimşek, 2008, **a.g.k.** , 10.
[25]http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim Tarihi:26.02.2019)
[26]"*Her taraf, kendi iç hukukunda, işbu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır*" şeklinde düzenlenmiştir. (M. 4)

- 1990 yılında Birleşmiş Milletler 45/95 sayılı Bilgisayar Vasıtasıyla İşlenen Veri Dosyalarıyla İlgili Rehber İlkeler kabul edilmiştir.[27]
- 1995 tarihinde Avrupa Birliğince çıkarılan 95/46 sayılı Avrupa Konseyi ve Avrupa Parlamentosu Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Yönergesi'nden sonra Avrupa Birliği üyesi ülkeler, veri koruma mevzuatlarını bu yönerge ile uyumlu hale getirme çabasına girmiştir.[28]
- 1997 yılında, Avrupa Konseyi ve Avrupa Parlamentosu, Yönerge'nin tamamlayıcısı niteliğini taşıyan 97/66 sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi'ni yürürlüğe koymuştur.[29]
- 1998 yılında OECD, Küresel Ağlarda Mahremiyetin Korunması Konusunda Bakanlık Bildirgesi'ni kabul etmiştir.[30]
- 1999 yılında Avrupa Konseyi Bakanlar Komitesi tarafından İnternet Ortamında Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı çıkarılmıştır.[31]
- 2001 yılında, kişisel verilerin korunması hakkı Avrupa Birliği Temel Haklar Şartı'nda güvenceye alınmıştır.[32]
- 2002 yılında AB, Yönerge'nin elektronik iletişim alanında tamamlayıcısı niteliğinde olan 2002/58 sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi'ni yürürlüğe koymuştur.[33]
- 2013 yılında OECD Gizlilik Rehber İlkeleri ve Kişisel Bilgilerin Sınırlar arası Değiştirilmesine İlişkin Tavsiye Kararı kabul etmiştir. Bu karar ile

[27]https://www.refworld.org/pdfid/3ddcafaac.pdf (Erişim Tarihi:26.02.2019)
[28]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (Erişim Tarihi:26.02.2019)
[29]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN (Erişim Tarihi:26.02.2019)
[30]Declaration On The Protection Of Privacy On Global Networks; http://www.oecd.org/internet/ieconomy/1840065.pdf (Erişim Tarihi:07.05.2019)
[31]https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429 (Erişim Tarihi:26.02.2019)
[32]https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708 (Erişim Tarihi:26.02.2019); N. Başalp(2004). *Kişisel Verilerin Korunması ve Saklanması*. Ankara: Yetkin Yayınları., s.27.
[33]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=DE (Erişim Tarihi:26.02.2019)

OECD'nin 1980 tarihli Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri güncelleştirilmiştir.[34]

- 25 Mayıs 2018'de, Yönerge'nin yerine yürürlüğe sokulan ve Yönerge'den farklı olarak bağlayıcı olması için üye devletlerce iç hukuka aktarılması gerekmeyen 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü yürürlüğe girmiştir.[35]

### 1.6.Kişisel Verilerin Korunması Hakkına İlişkin Görüşler

Kişisel verilerin korunmasının öncelikle çözülmesi gereken bir sorun olarak kabul edilmesinden sonra bir hak olarak kabul edilmesi aşamasına gelinmiştir. Fakat bu hakkın kendine özgü bir hak olup olmadığı veya hangi hakkın kapsamı içinde yer aldığı yönünde görüş ayrılıkları yaşanmıştır. Bu konuda genel kabul edilen görüşe bakıldığında bir kişinin kişisel verilerini korumakla kişinin özel hayatının gizliliğinin sağlanmış olduğunun hakim görüş olduğu görülmektedir.[36] Fakat kişisel verilerin korunması hakkına ilişkin diğer görüşlerin varlığı da göz ardı edilmemelidir.

#### 1.6.1.Ekonomik hak görüşü

Ekonomik hak görüşü, kişisel verilerin korunmasını bir insan hakkı olarak görmekten ziyade bireylerin mülkiyet hakkı mahiyetinde olduğunu benimseyen görüştür.[37] Bu fikir doğrultusunda mülkiyet hakkı ve fikri mülkiyet hakkı fikrinden teşekkül etmiş iki yaklaşım ortaya çıkmıştır.

Kişisel verilerin korunmasının hukuktaki karşılığının belirlenmesi yolunda ortaya çıkan görüşlerden ilk ortaya çıkan[38], en fazla eleştirilen[39] ve eleştirilmeyi de hak eden görüşün mülkiyet hakkı görüşü olduğu söylenmelidir.

---

[34]İ. Gül ve İ. Alagöz(2016). *Yeni Bir Güvenlik Sorunu: Kişisel Verilerin Korunmasına Yönelik İhlaller ve Uluslararası Düzenlemeler*. Ankara: Yargı Yayınevi , 45.

[35]H. M. Develioğlu(2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayıncılık. 12,13.
O. Selek (2019). *Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması*. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi , 21(2), 911-951, 911.

[36]S. G. Uyarer(2019). *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Ankara: Seçkin Yayınları, 23.

[37]Uyarer, 2019, **a.g.k.** , 23.

[38]Ş. Sert(2019). *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*. Ankara:Seçkin Yayınları., 50.

[39] Uyarer, 2019 , **a.g.k.** , 24.

Kişisel verilerin kapsamlı olarak korunmasının ekonomiyi menfi olarak etkileyebileceği endişesinin, ekonomik görüşün ortaya çıkmasındaki saiklerden biri olduğu görülmektedir.[40] Zaten bu görüşün argümanları incelendiğinde bir insan hakkı olması gereken kişisel verilerin korunması hakkının kapitalizmin hüküm sürdüğü ekonomik güç merkezlerince yeniden yorumlanmaya çalışıldığı görülmektedir.

Mülkiyet hakkı teorisine göre kişisel veriler kişinin mülkiyetinde olduğuna göre bireyler kişisel verileri üzerinde serbestçe tasarrufta bulunulabilir, kişisel verilerini satabilir, kiralayabilir.[41]

Görüldüğü üzere insan hakkı teorisinden uzak olan bu görüşün çeşitli yönlerden eleştirilmesi kaçınılmazdır.

Mülkiyet hakkı görüşüne göre satılan bir kişisel veri, verilerin yeni sahibi tarafından üçüncü kişiye devredildiğinde eski veri sahibinin kişisel veriler üzerinde söz sahibi olamaması söz konusu olacaktır ve bu durum kişisel verilerin niteliği ile bağdaşmadığı için kişisel verilerin mülkiyet hakkı kapsamında ele alınması mümkün değildir.[42] Eski veri sahibine kişisel veriler üzerinde tüm haklar sağlanmış olsa bile bu durumda şirketler açısından her defasında veri sahibinden izin alınmaya çalışılmasının ortaya çıkaracağı maliyet ekonomik olmayan bir sonuç doğuracaktır.[43]

Diğer eleştiriye göre kişisel veriler, mülkiyet hakkı teorisi kapsamında ele alındığında kişisel verilerin korunması sorumluluğu, kurumların yerine bireylerin üzerine yüklenmektedir ve bu durumun istenmeyen sonuçlar doğurması olasıdır.[44] Devlet ve birey arasındaki güç dengesizliğinin söz konusu olduğu durumda bireylerin bazı tavizler vermesi mümkündür. Örneğin bir devlet kurumunda iş sahibi olmak isteyen bireyin verileri üzerindeki haklarından gönüllü vazgeçmesi söz konusu

[40]M. V. Dülger(2018). *İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması*. İstanbul: İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C.5(1), 71-143,76.
[41]İ. Korkmaz(2019). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*. Ankara: Seçkin Yayınları., 86.
[42]M. Çokmutlu(2014). *Türk Ceza Hukukunda Kişisel Verilerin Korunması* Yayımlanmamış Doktora Tezi. Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü. 50.
[43]Korkmaz(2019). **a.g.k.** , 86, 87.
[44]H. C. Aksoy(2008) *Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü., 80.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

olabilir.[45] Aynı durumun özel sektörde de söz konusu olduğu durumda örneğin bireyler zarar görebilecekken şirketler yarar sağlayacaktır.[46] Mülkiyet hakkı teorisi güçlü ve varlıklı otorite karşısında zayıf ve daha az varlıklı bireyi korumadığından verilerin korunması açısından etkili bir sistem ortaya koyduğu söylenemez.[47]

Diğer bir görüş olan fikri mülkiyet hakkı teorisini benimseyen yazarların bakış açısı irdelendiğinde bu tezlerinin arkasında veri korumasının fikri mülkiyet hakkı olarak değerlendirilmesi gerektiği fikriyatı olduğu görülmektedir.[48] Fikri mülkiyet hakkı ile mülkiyet hakkının korunmasındaki esas amaç bilginin muhafazasını ve dağılımının kontrolünü sağlamaktır.[49]

Fikri mülkiyet hakkının ve kişisel verilerin korunması hakkının her ikisine de konu olan bireyin denetimi altında olduğu verilerdir. Fikri mülkiyet hakkındaki veri telif hakkı olan bir çalışmayken kişisel verilerin korunmasında veri bireye ait her türlü bilgidir.[50] Fikri mülkiyet hakkı sahibinin eseri üzerindeki hakları ile veri sahibinin verileri üzerindeki haklarının benzer olduğu görülmektedir.[51]

Fikri mülkiyet hakkı görüşüne göre veri öznesinin verileri üzerinde fikri mülkiyet sahibinin eser üzerindeki manevi haklarına benzer hakları vardır.[52] Diğer yandan fikri mülkiyet hakkı sahibinin eseri üzerinde tasarruf yetkisi olduğu gibi veri sahibinin de verileri üzerinde tasarruf yetkisi vardır. Örneğin eser sahibi eserini kamuoyunun kullanımına açabilir, telif hakkını devredebilir. Bunun gibi veri sahibi de verilerinin başkalarıyla paylaşabileceği gibi verilerin kullanımını da başkalarına devredebilir. Bu tür benzerliklerin fikri mülkiyet teorisinin dayanağı olduğu görülmektedir.[53]

Mülkiyet hakkı teorisine getirilen eleştiriler ile fikri mülkiyet hakkı teorisine getirilen eleştirilerin ortak noktada buluştuğu yerler vardır. Fikri mülkiyet hakkı teorisi

---

[45]Arthur R. MILLER, s. 213-214'den aktaran E. Küzeci(2010). *Kişisel Verilerin Korunması*. Doktora Tezi, Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, 70.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[46]Korkmaz, 2019, **a.g.k**. , 87.
[47]Uyarer, 2019, **a.g.k.** , 27; Korkmaz, 2019, **a.g.k**. , 87.
[48]Korkmaz, 2019, **a.g.k**. , 79.
[49]Aksoy, 2008, **a.g.k.** , 83.
[50]Korkmaz, 2019, **a.g.k**. , 79.
[51]Aksoy, 2008, **a.g.k.** , 84.
[52]F. N. Yıldırım(2019). *Avrupa Birliği Ve Türk Hukukunda Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, 14.
[53]Aksoy, 2008, **a.g.k. ,** s.85.

de kişisel verilerin insan hakkı teorisinden uzaklaşıp bireyin birçok hakkının korumasız kalmasına sebebiyet verecektir.[54]

Kişisel verilerin fikri mülkiyet hakkı kapsamında ele alınmasına getirilen eleştirilerin dayanaklarından biri de her iki hakkın korunmamasının doğuracağı sonuçların farklı olacağı tezidir. Bu teze göre fikri mülkiyet hakkı ihlal edilen bir kişinin ekseriyetle eserinden kaynaklı maddi kaybı söz konusu olabilecekken kişisel verileri korumasız kalan bireyin mesleğini kaybetmek, sosyal statüsünü kaybetmek ve ayrımcılığa maruz kalmak gibi olumsuz neticelerle karşılaşması muhtemeldir.[55]

Netice itibariyle gerek mülkiyet hakkı görüşünün gerekse fikri mülkiyet hakkı görüşünün kişisel verilerin korunması açısından etkili bir bakış açısı olduğunu söylenemez. Zira bu görüşlerin, sadece ortaya çıktığı ABD hukuk sisteminde[56] kısmen de olsa etkili olabilecek, ekonomik güç çevrelerinin ortaya attığı ve kişisel veriler gibi bireyin hayatını doğrudan etkileyen bir hususu koruma amacı gütmekten ziyade belirli çevrelere ekonomik açıdan katkı sunacak bir kişisel veri piyasası oluşturmaya yönelik ortaya atılan görüşler olduğu görülmektedir.

Kişisel verilerin korunmasını mülkiyet hakkı teorisi ile açıklayan görüşler irdelendiğinde, bu görüşlerin kişisel verilere yeni bir para birimi gözüyle baktığı ve ABD'de bu yükselen yeni değerden kar edilmeye çalışıldığı görülmektedir. Zaten AB Adalet Divanı da ABD'yi kişisel verilerin etkili korunmadığı ülkeler kapsamında görmektedir.[57]

ABD hukuk sisteminde veri korumasının münhasır bir hak olarak görülmediği[58] gibi sair haklar kapsamında da koruma altına alınmadığı, kişisel verilerin korunmasının kaderinin ekonomik otoritelerinin elinde olduğu ve sektörel yaklaşımlarla[59] veri güvenliğinin sağlanmaya çalışıldığı ortaya konmaktadır. Bu açıdan mülkiyet hakkı ve

---

[54]S. E. Aydın(2014). *Aihm İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu*. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, 17.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[55]Korkmaz, 2019 , **a.g.k**. , 88.
[56]H. N. Avcıoğlu(2018). *Türk Hukukunda Kişisel Verilerin Korunması Hakkı.* Yüksek Lisans Tezi. Konya: KTO Karatay Üniversitesi, Sosyal Bilimler Enstitüsü, 16.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:08.04.2020)
[57]Uyarer, 2019, **a.g.k.** , 25.
[58]Dülger, 2018, **a.g.k.** , 76.
[59]Atul Singh, Protecting Personal Data as a Property Right, ILI Law Review, Winter Issue 2016, s.123-129, s.126'dan aktaran Uyarer, 2019, **a.g.k.** , 25.

fikri mülkiyet hakkı görüşünün Kıta Avrupası sisteminin aradığı veri koruma seviyesine ulaşma amacını yerine getirmesinin mümkün olmadığı açıktır.

### 1.6.2.İnsan hakkı görüşü

Tarihsel sürecine bakıldığında kişisel verilerin sorun olarak ortaya çıkmasında esas kaygının insan onurunu korumak olduğu görülmektedir. Devamında bu sorunun çözümüne yönelik yapılan çalışmalarda da nihai amacın insan onurunu korumak ve insan onuruna hak ettiği değeri vermek olduğu anlaşılmaktadır. Kişisel bilgilerin koruma zırhına alınmasının sair hak veya hürriyetlerle olan münasebeti de insan onuru ile ilişkisi ile başlamıştır. Zira temel hak ve özgürlüklerin korunmasının asıl amacı en nihayetinde insan onurunun yüceltilmesidir. İnsan onuru kavramının üzerinde uzlaşılmış bir tanımı yoktur. Eğer insan onuru kavramına bir tanım getirilmek gerekirse insanın biyolojik varlığını sürdürmesinin ötesinde onu diğer canlılardan ayıran manevi kimliği olarak tanımlanabilir. Bu manevi kimlik, bireye yaşadığı ortamda ayırt edilmesini ve ona saygı duyulmasını sağlar. Diğer insan hakları, insan onurunun korunmasına hizmet eden birer araçtır.

Kişisel verilerin korunmamasının insan onuruna verdiği tahribatın geçmişten günümüze bize gösterdiği örnekler de göz önüne alındığında kişisel verilerin korunmasının da doğal olarak insan onurunun korunmasını sağlayacağı gerçeği ortadadır. Bu açıdan kişisel verilerin korunması ya kendine özgü bir insan hakkı olarak ele alınmalı ya da diğer insan haklarının muhtevasına dahil edilmelidir. Her ne şekilde olursa olsun kişisel verilerin, korunması gereken bir müessese olduğu göz ardı edilmemelidir.

Kişisel verilerin korunmasının uluslararası ve ulusal düzenlemelerin bazılarında ayrı bir insan hakkı olarak koruma altına alındığı görülmekteyken bazılarında ise ayrıca bir kişisel verilerin korunması hakkının düzenlenmediği görülmektedir.

Bağlayıcılığı olan düzenlemeler incelendiğinde AİHS'de kişisel verilerin korunması hakkına ilişkin doğrudan bir düzenleme yer almasa da Avrupa İnsan Hakları Mahkemesi(AİHM) içtihatları incelendiğinde AİHM'in kişisel verilerin korunmasını AİHS'in 8. maddesinde koruma altına alınan özel hayata ve aile hayatına saygı hakkı

kapsamında ele aldığı görülmektedir.[60] Fakat Sözleşme'nin ve Tüzük'ün kişisel verilerin korunmasını ayrı bir hak olarak koruma altına aldığı görülmektedir.

Kişisel verilerin korunması hakkı-mahremiyet (özel hayata saygı hakkı) ilişkisinin varlığının kabul görmesinde ana etken AİHM'in bu konudaki içtihatları olmuştur. AİHS'de kişisel verilerin korunması hakkı açıkça düzenlenmediğinden AİHM'in kişisel verilerin korunmasını AİHS m.8'de düzenlenen özel hayata saygı hakkı açısından değerlendirdiği görülmektedir.[61] Mahkeme'nin bu konudaki ilk kararı da Klass ve diğerleri v. Almanya kararıdır.[62]

AİHM'in özel hayatın kapsamı noktasında genişletici bir yorum belirlediği görülmektedir. Örneğin Von Hannover ve Almanya kararında bireyin diğer insanlarla ilişkileri veya kamusal alandaki ilişkilerinin de özel hayat olarak yorumlanabileceğini değerlendirmiştir.[63] Bunun dışında Rotaru ve Romanya kararında otoritelerce sistematik bir şekilde toplanan ve depolanan kamuya mal olmuş bir bilginin özel hayat kapsamında sayılabileceğini belirtmiştir.[64]

AİHM'in de kabul ettiği üzere her bireyin kişisel verilerinin akibetini belirleme hakkı vardır.[65] Herkes, verilerinin nasıl, ne zaman ve nerede açıklanabileceğini belirleyebilmelidir. Fakat burada ifade özgürlüğü ile kişinin kişisel verilerinin kaderini belirleme hakkının çatışması olasıdır. Bu açıdan her iki hakkın arasında dengenin sağlanması önemlidir.

Örneğin M.L ve W.W. v. Almanya kararında AİHM, internet arama motorlarının bilginin kamuoyunca ulaşılmasını kolaylaştırdığını, başvuruculların geçmişte almış oldukları mahkûmiyetlerine ilişkin bilginin silinmesi taleplerinin federal mahkeme tarafından kamunun bu tür olayları bilme hakkı olması sebebiyle haklı olmadığına ve basın organlarının geçmişe dönük haberleri arşivde bulundurmak suretiyle demokrasiye katkıda bulunma görevinin olduğuna karar verdiğini ve bu kararın haklı olduğunu,

[60]E. Solmaz(2019) *Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı*. İdare Hukuku ve İlimleri Dergisi. 18(1): 61-78, 62.
[61]Uyarer, 2019, **a.g.k.** , 30.
[62]Solmaz, 2019, **a.g.k**. , 64.
15473/89 başvuru numaralı ve 21/05/1992 tarihli Klass ve diğerleri v. Almanya kararı için bkz: http://hudoc.echr.coe.int/tur?i=001-45549 (Erişim Tarihi:22.01.2020)
[63]59320/00 Başvuru numaralı ve 24.06.2004 tarihli Von Hannover ve Almanya kararının Türkçe çevirisi için bkz: http://hudoc.echr.coe.int/tur?i=001-112080 (Erişim Tarihi:22.01.2020)
[64]Uyarer, 2019 , **a.g.k.** , 31.
[65]Uyarer, 2019, **a.g.k.** , 31.

arşivden bilgi çıkarılması yönündeki talepleri haklı çıkaracak bir kararın ifade ve basın özgürlüğüne engel olacağını, başvuruculaların arşivdeki bilgilerin anonimleştirilmesi talebinin de AİHS'in 10. maddesinde düzenlenen ifade özgürlüğü hakkının yayınlanacak bilgilerde takdir yetkisini gazetecilere ve onun etik kurallarına bıraktığı için reddedilmesi gerektiğini, netice itibariyle başvurucular açısından AİHS'in 8. maddesinin ihlal edilmediğini değerlendirmiştir.[66]

Unutulma hakkı, bireyin kendisi hakkında doğru olan; fakat güncelliğini yitirmiş bir bilginin ortadan kaldırılmasını talep etme hakkı olarak tanımlanabilir. Unutulma hakkının ortaya çıkışında İsviçre Federal Mahkemesince verilmiş kararların etkisinin büyük olduğu görülmektedir.[67] Örneğin mahkeme vermiş olduğu bir kararda; kamuoyunca bilinmeyen bir kişi tarafından on yıl önce işlenmiş, cezası infaz edilmiş ve adli sicilden silinmiş bir suç kaydına ilişkin yazılmış bir yazının hukuka uygun olmayacağına karar vermiştir.[68]

Unutulma hakkı ile ilgili verilmiş ve ilke niteliğinde olan karar ise AB Adalet Divanı(ABAD)'nın 2014 tarihli Google-İspanya kararı'dır.[69] Çalışmanın ilerleyen bölümlerinde AB Genel Veri Koruma Tüzüğü başlığı altında tekrar değinilecek olan bu kararda ABAD, başvurucunun Google arama motorunda yer alan, kendisi ile ilgili güncelliğini yitirmiş bilginin silinmesi talebini kabul etmiştir. Bu kararda AB Adalet Divanı, Google arama motorunun bir veri sorumlusu olduğunu(33.paragraf) ve başvurucunun unutulma hakkının tanınması gerektiğini(99.paragraf) belirtmiştir.

AB Adalet Divanı'nın bu ilke kararından sonra Avrupa Birliğinin Tüzük'te unutulma hakkını ayrıca koruma altına aldığı görülmüştür. Bu açıdan Google-İspanya kararının uluslararası veri koruma mevzuatına yol gösteren bir nitelik taşıdığı da söylenebilir.

---

[66]Uyarer, 2019, **a.g.k.** , 34.
[67]N. Başalp (2015). *Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri*. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi. 21(1), 77-106, 95-96.
[68]Başalp, 2015, **a.g.k**. , *Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri*. s. 96.
[69]Google-İspanya Kararı için bkz.
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131_SUM&qid=1579769680599&from=EN (Erişim Tarihi:23.01.2020)
Google-İspanya Kararı'nın Türkçe Çevirisi için bkz.
http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_13.pdf(Erişim Tarihi:23.02.2020)

AİHM bilgi edinme hakkını, devletin bireyin bilgi edinme hakkını kısıtlamasının yasaklanması olarak tanımlamış ve bunu devlet açısından pozitif bir yükümlülük olarak görülmemesi gerektiğini değerlendirmiştir.[70]

Çalışmamızın ileride yer alan bölümlerinde görüleceği üzere uluslararası hukukta veri koruma mevzuatı, veri sahiplerine bir takım haklar sağlamaktadır. Örneğin verilerin düzeltilmesini, silinmesini talep etme hakkı bunlar arasında sayılabilir. Veri sahibinin, veri koruma mevzuatının tanımış olduğu hakları kullanabilmesi için kendisi ile ilgili bilgiye erişebilmesi gerekir. Kendisi ile ilgili bilginin yanlış veya eksik olup olmadığı hususunda bilgi sahibi olmayan veri sahibinden düzeltme ve silinme hakkını kullanması mümkün değildir. Bu açından kişisel verilerin korunması hukukunda bilgi edinme hakkının işlevsel açıdan önemi göz ardı edilemez.

[70]Hermann Josef Blanke- Ricardo Perlingeiro, The Right of Access to Public Information- An International Comparative Legal Survey, Springer, 2018, s.147'den aktaran Uyarer, 2019, **a.g.k.** , 40.

# İKİNCİ BÖLÜM

## 2.KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN ULUSLARARASI KAYNAKLARI

### 2.1.Genel Olarak

Kişisel verilerin korunmasının uluslararası mevzuatının oluşması sürecine bakıldığında devletlerin kişisel verilerin korunmasını bir sorun olarak görmesinin başlangıcının ikinci dünya savaşı olduğu söylenebilir. İkinci dünya savaşı sonrası devletlerin insan onuruna vermiş olduğu önemin artması ve insan haklarının yasal bir güvenceye alınmaya çalışılması çalışmaları neticesinde temel hak ve hürriyetlerin koruma altına alındığı uluslararası kaynaklar ortaya çıkmıştır. Ortaya konulan ilk uluslararası düzenlemelerde kişisel verilerin korunması hakkının doğrudan koruma altına alınmadığı görülmektedir. Bunun yerine yaşam hakkı, özel hayatın gizliliği, işkence yasağı gibi temel haklar güvence altına alınmaya çalışılmıştır. Zira ikinci dünya savaşının insanlık üzerinde oluşturduğu tahribatın neticesinde öncelikle bu tahribatın sebeplerini ortadan kaldırma çabası içine girişilmiştir. Bu açıdan savaş sonrası oluşturulmaya çalışılan düzende devletlerin ve toplumun kişisel verilerin korunması gibi teferruat olarak görülen bir hususu düzenlemelerini beklemek haksızlık olabilir. Toplumda kişisel verilerin korunmadığı yönünde bir kaygı ve buna ilişkin ortak bir bilinç oluşmadıkça devletlerin buna ilişkin bir çalışma içine girmedikleri tarih boyunca görülen bir gerçektir. Yaşam hakkı gibi en temel insan hakkını bile milyonlarca insanın öldüğü ikinci dünya savaşından sonra yasal güvenceye alan dünya devletlerinden, gerekli koşullar oluşmadan kişisel verileri koruma çabasına girmesini beklemek bir yanılsama olacaktır.

Nitekim bilgisayar teknolojisinin gelişmesiyle toplumda oluşan kişisel verilerinin yeterli şekilde korunmadığı kaygısı oluşmaya başladıkça özellikle Kıta Avrupası devletlerinde bu yönde bir yasalaştırma çabasına girişilmiştir ve zamanla kişisel verilerin korunmasına ilişkin önceleri bağlayıcı olmayan; fakat zamanla bağlayıcılık niteliği taşımaya başlayan uluslararası düzenlemeler yürürlüğe girmeye başlamıştır.

Çalışmamızın ilerleyen bölümünde kişisel verilerin korunmasında bugüne gelinen noktaya kadar geçen süreçte ortaya konan çalışmalara yer verilmiştir. Kişisel verilerin

korunması hukukunda mevcut duruma gelinme sürecinin anlaşılması açısından tarihsel sıralamaya dikkat edilmesine önem verilmiştir.

### 2.2.İnsan Hakları Evrensel Bildirgesi

Kişisel verilerin korunması gereken bir hak olduğunun gündeme gelmesinin dünyada bilgisayar teknolojisinin gelişimi ile başlayan süreç olduğu göz önüne alındığında 1948 tarihli İnsan Hakları Evrensel Bildirgesi'nde doğrudan kişisel verilerin korunmasının düzenlenmesi beklenmemelidir. Fakat bu beyannamede uluslararası hukukta kişisel verilerin korunmasının temelinin atıldığı söylenebilir.

Yukarıda da belirttiğimiz üzere insanlık tarihinde insan haklarının korunması kaygısının ve bilincinin ortaya çıkması ikinci dünya savaşı sonrasıdır. Bu savaşın doğurduğu tahribatın ve bu savaş sürecindeki insan hakları ihlallerinin bir daha yaşanmaması adına devletler, bir araya gelerek, 10 Aralık 1948 tarihinde BM Genel Kurulunda İnsan Hakları Evrensel Bildirgesi'ni kabul etmişlerdir.

Bildirge'nin 12. maddesinde hiçbir bireyin mahremiyetine, ailesine, ikametgahına yahut muhaberesine keyfi olarak müdahalede bulunulamayacağı; onur ve şöhretine saldırılamayacağı ve herkesin bu müdahale ve saldırılara karşı yasalar ile muhafaza etme hakkının varlığı düzenlenmiştir.[71]

Bildirge'nin en önemli özelliği, evrensel bir insan hakları koruma mekanizması oluşturması ve insan haklarına bir çerçeve belirleyerek kendinden sonraki uluslararası sözleşmelere önayak olmasıdır.[72]

Görüldüğü üzere kişisel verilerin korunmasının tartışılmadığı 1948 yılında kişisel verilerin korunması adı altında olmasa da kişisel verilerin korunmasının temeli olan özel ve aile hayatının gizliliği, insan hakkı olarak görülmeye ve korunmaya başlanmıştır. Fakat AİHM tarafından kişisel verilerin korunmasının özel hayata saygı hakkı açısından koruma altına alındığı mevcut durum göz önüne alındığında insan hakları evrensel

[71]https://www.un.org/en/universal-declaration-human-rights/ (Erişim Tarihi:23.01.2020)
http://www.unicef.org.tr/files/bilgimerkezi/doc/insan%20haklari%20evrensel%20beyannemesi.pdf (Erişim Tarihi:02.11.2019)
https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf (Erişim Tarihi:02.11.2019)
http://www.un.org.tr/humanrights/images/pdf/1-insan-haklari-evrensel-beyannamesi.pdf (Erişim Tarihi:02.11.2019)

[72]H Kalabalık(2005). *İnsan Hakları Hukukuna Giriş*. Ankara: Seçkin Yayınları, 120.

bildirgesinin özel hayata saygı hakkını korumanın temeli atmasıyla kişisel verilerin korunmasının da temelini attığı gerçeği dikkatlerden kaçmamalıdır.

### 2.3. Avrupa İnsan Hakları Sözleşmesi

AİHS, Avrupa Konseyince 4 Kasım 1950'de kabul edilen, temel hak ve hürriyetlerin muhafaza edilmesi için ortaya konulan en önemli çalışmadır.[73]

AİHS'deki temel hak ve hürriyetlerin korunup korunmadığını denetleyen yargı organı ise AİHM'dir. AİHM'in kişisel verilerin korunması hususundaki önemi, bunu sözleşmede yer almasa bile AİHS'in 8. maddesi kapsamında görmek suretiyle koruma altına almasıdır.

AİHS'in hazırlandığı dönemde kişisel verilerin korunması bir mesele olarak görülmediğinden bu sözleşmeye bu konuda bir madde konulması da gündeme gelmemiştir. Fakat zaman içinde gelişen teknoloji ve kişisel verilerin korunmasının bir insan hakkı haline gelmesinin de etkisiyle kişisel verilerin korunması noktasında sözleşmedeki bu eksiklikten doğan boşluğu doldurma görevini AİHM üstlenmiştir ve mahkeme kişisel verilerinin korunması hakkını AİHS'in 8.maddesi kapsamında değerlendirmeye başlanmıştır.[74]

AİHS'in 8. maddesi "özel ve aile hayatına saygı hakkı" başlığı altında şöyle düzenlenmiştir:

"*1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

*2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*"

---

[73]S. G. Uyarer (2019). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Galatasaray Üniversitesi, Sosyal Bilimler Enstitüsü, 29.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[74]Aydın, 2014, **a.g.k.** , 31 .

İnsan Hakları Evrensel Bildirgesi başlığı altında da bahsettiğimiz gibi henüz 1970li yıllara gelinmediği, kişisel verilerin korunmasının, hak ve sorun olarak görülmediği 1950 yılında da AİHS, özel hayatın mahremiyetini koruma altına alarak günümüzde korunmaya çalışılan kişisel verilerin korunması kurumunun temelini atmaya devam etmiştir.

Yukarıda bahsettiğimiz üzere AİHM içtihatlarında kişisel verilerin korunmasının AİHS'in 8. maddesi kapsamında değerlendirildiği görülmektedir. Bu açıdan 1950 tarihli AİHS'in kişisel verilerin korunmasının en önemli güvencelerinden olduğu söylenebilir. Çünkü bağlayıcılık açısından doğrudan kişisel verilerin korunmasını düzenleyen AB bünyesindeki uluslararası düzenlemelerin aksine daha evrensel düzeyde bağlayıcılığı olan bir sözleşme olduğu söylenebilir.

### 2.4. Uluslararası Medeni ve Siyasi Haklar Sözleşmesi

16 Aralık 1966 tarihli BM Genel Kurulunca kabul edilen Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nde de, İnsan Hakları Evrensel Bildirgesi'nde ve AİHS'de olduğu gibi kişisel verilerin korunması doğrudan düzenlenmeyip mahremiyet hakkı koruma altına alınarak kişisel verilerin korunmasının uluslararası boyutta güvence altına alınmasının temeli atılmaya devam edilmiştir.

Sözleşme'de İnsan Hakları Evrensel Bildirgesi'nde yer almayan yeni haklara yer verildiği gibi[75] bildirgede yer alan haklar bir sözleşme formatına dönüştürülerek[76] bu haklara bağlayıcılık kazandırılmıştır.[77]

Sözleşme'nin "mahremiyet hakkı" başlıklı 17. maddesi:

"*1. Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.*

*2. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir.*"

[75]ÇALIK, T . "Birleşmiş Milletler İnsan Hakları Sözleşmeleri Kapsamında İnsan Haklarının Korunması". Selçuk Üniversitesi Hukuk Fakültesi Dergisi 24 (2016 ): 69-120; s.84.
[76]BOZKURT Enver, İnsan Haklarının Korunmasında Uluslararası Hukukun Rolü, Ankara 2003, s.62 ; H. Kalabalık(2017). *İnsan Hakları Hukuku* Ankara: Seçkin Yayınları. 95. vd.
[77]Kalabalık , 2017, **a.g.k**. , 95 vd.

şeklinde düzenlenmiştir.[78]

### 2.5. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Özel Yaşamın Korunması Ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri

23 Eylül 1980 tarihinde yürürlüğe giren ve tavsiye kararı niteliğinde olduğu için bağlayıcı olmayan OECD Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri[79]; OECD'nin diğer ilkelerinde olduğu gibi, her ne kadar bağlayıcı olmasa da OECD üyelerinin uymalarının beklenildiği, üye ülkelerin kişisel verilerin korunması yönündeki ulusal politikalarını belirlemesinde yol gösterici olan, kişisel verilerin korunmasına yönelik uluslararası mevzuatın oluşması sürecinde taslak olarak kullanılan ilkelerdir.[80]

Bu rehber ilkeleri, kişisel verilerin korunması hakkının doğrudan ele alındığı ve kişisel verilerin korunması ile ilgili uluslararası ölçütler belirleyen ilk çalışmadır.[81] Bu bakımdan OECD'nin kişisel verilerin korunması hususunu uluslararası alanda ele alan ilk uluslararası örgüt olduğu söylenebilir.[82]

OECD'nin kuruluş amacı, üyelerinin ekonomik gelişimini desteklemek olduğu için örgüt, kişisel verileri korumaya insan hakları penceresinden bakmak yerine ulusal veya uluslararası çapta ticaret konusu olabilecek değerli bir metaa olarak bakmıştır.[83]

OECD, bu ilkelerle ulusal düzeydeki veri koruma yasalarının birbiriyle uyumunun sağlanmasını amaçlamaktadır.[84] Esasında OECD, bu rehber ilkeleri yayınlamak suretiyle kişisel verilerin korunmasının ekonomik açından önemini de ortaya

---

[78]http://www.unicankara.org.tr/doc_pdf/metin133.pdf (E.T:16.03.2019)
[79]http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim Tarihi:16.03.2019)
[80]İ. Gül ve İ. Alagöz(2016). *Yeni Bir Güvenlik Sorunu: Kişisel Verilerin Korunmasına Yönelik İhlaller ve Uluslararası Düzenlemeler*. Ankara: Yargı Yayınevi , 43.
[81]R. Karabulut (2014). *Kişisel Verilerin Korunması ve Kolluk hizmetleri*. Yayımlanmamış Yüksek Lisans Tezi. Diyarbakır: Dicle Üniversitesi, Sosyal Bilimler Enstitüsü , 12.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
U. Ersoy(2009). *Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması"*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi, Sosyal Bilimler Enstitüsü. , 52.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[82]S. Uncular(2018). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. Ankara: Seçkin Yayınları. 49.
[83]İ. Gür(2009). *Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar Ve Çözüm Yolları*. Yüksek Lisans Tezi. Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü. 109.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[84]Aksoy, Hüseyin Can; Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması ; Çakmak Yayınevi , 2010 , Ankara, s.4 ; Uncular , 2018, **a.g.k.** , 69.

koymuştur.[85] Zira OECD, serbest piyasa ekonomisinin gelişimini amaçlayan bir ticaret örgütü olarak bu amacın gerçekleşmesinde sınır ötesi veri akışının engellenmesinin engel teşkil edeceğini düşünmekte ve bu ilkelerle buna bir önlem almaya çalışmaktadır. Zaten metnin önsözünde bu duruma değinilmiştir. Metin önsözünde ulusal düzeydeki veri koruma mevzuatlarının sınır ötesi veri akışını engelleme tehlikesi olduğu, bu veri akışlarında teknolojik gelişmelerin de katkısıyla artış gözlemlendiği, bu veri akışlarındaki kısıtlamaların bankacılık ve sigorta gibi ekonominin ehemmiyetli alanlarında ciddi bozulma neticesini doğurabileceği, bu kısıtlamaların engellenmesi için ulusal kişisel veri koruma mevzuatlarını uyumlaştırmak gerektiği ve bu uyumun sağlanması için OECD tarafından tavsiye niteliğinde bazı ilkeler kabul edildiği öngörülmüştür.

OECD, bu rehber ilkelerle OECD üyesi ülkelere bu ilkeleri dikkate almak suretiyle iç hukuklarını oluşturmalarını, sınır aşan veri trafiğini engellememelerini, mevcut engelleri kaldırmalarını ve bu rehber ilkelerin hayata geçirilmesinde işbirliği yapılmasını tavsiye etmektedir.[86]

Netice itibariyle OECD rehber ilkelerinin öncelikli amacı serbest piyasanın güçlenmesi için kişisel verilerin serbest dolaşımıyken ikinci amacı kişisel verilerin korunmasıdır.[87] Fakat bu amaçların birbirine karşı bir üstünlüğü olmayıp eşitler arasında birincilik-ikincilik durumunun söz konusu olduğu söylenebilir.

OECD'nin öngördüğü bu ilkeler; toplamayı sınırlama ilkesi, veri kalitesi ilkesi, amaç belirleme ilkesi, kullanımı sınırlama ilkesi, güvenlik tedbirleri ilkesi, açıklık ilkesi, bireysel katılım ilkesi, hesap verilebilirlik ilkesidir.

Toplamayı sınırlama ilkesine göre; kişisel verilerin toplanması ile ilgili sınırlamalar olmalı ve veriler, hukuk uygun vasıtalarla toplanmalıdır. Ayrıca veri sahibi toplama faaliyeti hakkında bilgilendirilmeli ve veri sahibinin muvafakati ile veri toplaması yapılmalıdır(M.7).

---

[85]Uncular, 2018, **a.g.k.** , 49.
[86]E. Küzeci (2018) *Kişisel Verilerin Korunması*. Ankara: Turhan Kitabevi. , 120.
[87]S. Karınçu(2019). *Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü. 23.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

Veri kalitesi ilkesi uyarınca; veriler, kullanım maksadı ile ilgili olmalıdır. Ayrıca bu ilke verilerin, kullanım maksadı için gerekli olduğu kadar doğru, eksiksiz ve güncel olmasını gerektirir(M.8).

Amacın belirliliği ilkesine göre kişisel veriler toplanmadan önce toplanma amacı belirlenmiş olmalı, veriler toplandıktan sonra bu toplanma amacı ile sınırlı olarak kullanılmalıdır.

Amaca uygun kullanım ilkesine göre veri öznesinin rızasının olduğu yahut yasanın yetkilendirdiği durumlar haricinde veriler; elde edildiği ve işlendiği maksat haricinde kullanılmamalıdır, elde edilebilir duruma getirilmemelidir ve açıklanmamalıdır.

Kullanımı sınırlama ilkesine göre kişisel veriler, veri öznesinin izni ve kanunların yetkisi olmadıkça rehber ilkelerde öngörülen amaçlar dışında bir amaç için açıklanmamalı, erişilebilir olmamalı veya başka türlü kullanılmamalıdır(M.10).

Güvenlik önlemleri ilkesine göre kişisel veriler; kaybetme, yetkisiz erişim, yok etme, kullanım, değişiklik ya da verilerin ifşası gibi tehlikelere karşı elverişli güvenlik tedbirleriyle muhafaza edilmelidir(M.11).

Açıklık ilkesine göre kişisel verilere ilişkin gelişmeler, uygulamalar ve politikalarla ilgili genel bir açıklık politikası bulunmalıdır. Kişisel verinin varlığını, doğasını, bunların kullanımının temel amaçlarını, veri denetleyicisinin kimliğini ve normal ikametini tespit etmenin yolları hazır olmalıdır(M.12).

Bireysel katılım ilkesine göre birey şu haklara sahip olmalıdır(M.13):

a-Bir veri kontrol cihazından kişisel verilerine erişmek ve kişisel verinin kendisine ait olup olmadığını teyit etmek,

b-Makul süre içinde, eğer ücret öngörülmüşse makul bir ücret karşılığında, kolay anlaşılabilir biçimde kişisel verilere erişmek,

c-(a) ve (b) bentlerindeki taleplerin reddedilmesi durumunda bunun gerekçelerini öğrenebilmek ve bu reddedilmeye karşı itiraz edebilmek,

d-Kişisel verilerinin silinmesi, düzeltilmesi, değiştirilmesini istemek.

Hesap verebilirlik ilkesine göre veri denetleyici, yukarıda belirtilen prensipleri etkileyen önlemlere uyup uymamaktan sorumlu tutulmalıdır.

Rehber ilkelere göre veri denetleyicisi, verilerin içeriği ve kullanımı hakkında karar vermeye yetkilidir. Veri denetleyicisi gerçek veya tüzel kişi olabilir.

Rehber ilkelerin sınır ötesi veri akışına ilişkin koyduğu bazı temel ölçütler vardır:

1.Veriyi alıcı ülkenin veri koruma mevzuatının gönderici ülke ile eşdeğer koruma sağlamaması durumunda gönderici ülke veriyi göndermekten imtina edebilir.

2.Diğer üye ülkelerin bu rehber ilkeleri yeterince gözetmediği ve gönderici ülkenin iç hukukunun müsaade etmediği durumlar haricinde üye ülkeler diğer üye ülkelere veri akışını kesmemelidir.

3.Üye ülkeler, diğer yerel üye ülke işlemlerinin ve kişisel verilerin yeniden ihraç edilmesinin etkilerini göz önünde bulundurmalıdır.

4.Üye ülkeler, bir üye ülke üzerinden yapılan geçişler de dahil olmak üzere alıcıların kişisel veri akışlarının kesintisiz ve güvenli olmasını sağlamak için tüm makul ve uygun adımları atmalıdır.

5.Bir üye ülke, kendisi ve bir başka üye ülke arasındaki sınırsız kişisel veri akışını kısıtlamaktan kaçınmalıdır. Fakat bu ülke, bazı kişisel veri kategorileri için eşdeğer koruma düzeyinin yasal olarak sağlanmadığı ülkelere veri akışını sınırlayabilir.

6.Üye ülkeler, mahremiyetin kişisel hakların korunması amacını aşacak nitelikte veri akışını engeller nitelikte yasalar, politikalar ve uygulamalar geliştirmekten kaçınmalıdır.

2013 yılında temel ilkeler korunmak suretiyle OECD rehber ilkelerinde değişiklikler yapılmıştır.[88]

### 2.6.108 Sayılı Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Kişisel Verilerin korunmasın konusunda, uluslararası alanda ilk bağlayıcı çalışmaları yapan kurumun Avrupa Konseyi olduğu görülmektedir. OECD'nin ise

[88](http-77).

kişisel verileri konusundaki çalışmalarının ilk uluslararası çalışmalar olduğu fakat bu çalışmaların bağlayıcılık niteliğinin olmadığı görülmektedir. Ayrıca OECD, kuruluş amacının da etkisiyle daha çok ekonomik kaygılarla kişisel verilerin korunmasını ele almışken Avrupa Konseyi, insan haklarını merkeze alan bir çalışma içine girmiştir.

Avrupa Konseyinin kişisel verilerin korunması konusunda ilk çalışma yapan kurum olma özelliğini kazandıran ise Sözleşme'yi yürürlüğe sokmasıdır.[89] Sözleşme, kişisel verilerin korunması konusunda uluslararası alanda ilk bağlayıcılığı olan düzenleme olma vasfını sürdürmeye devam etmektedir.[90]

Avrupa Konseyi her alanda olduğu gibi kişisel verilerin korunması konusunda da insan haklarını koruma bağlamında hassas bir tutum sergilemiştir. Hiçbir Avrupa Konseyi ülkesinin kişisel verilerin korunmasını gündemine almadığı dönemde Avrupa konseyi bunu üyelerinin gündemine getirmiştir. Aynı zamanda üyelerinden kişisel verilerin korunması konusunda insan haklarını koruyan nitelikte iç hukuk mevzuatı oluşturmalarını beklemiştir. Bununla ilgili çalışmalarından en önemlisi, birçok Avrupa konseyi ülkesinin iç hukukunun bir parçası haline gelen 108 sayılı Sözleşme'dir.

Sözleşme ile Avrupa Konseyi, uluslararası alanda bağlayıcılığı olan AİHS'de kişisel verilerin korunması hakkının ayrı bir başlık altında koruma altına alınmamasının doğurduğu güvenlik açığını bağlayıcılığı bulunan bir sözleşme ile kapatmak istemiş[91] ve bunun üzerine Sözleşme'yi yürürlüğe sokmuştur.

Avrupa Konseyi'nin Sözleşme'yi kabul etme amaçlarından biri geleneksel çözüm yöntemleriyle kişisel verilerin korunmayacağını düşünmesidir.[92]

Sözleşme'nin diğer amaçlarından biri de otomatik veri dosyalama sistemleri ile kısa sürede daha çok veri işlenmesi, teknolojinin gelişmesiyle bunda bir artış yaşanma

[89]Sözleşme'nin metni için bkz: https://rm.coe.int/1680078b37 (Erişim Tarihi:24.01.2020)
Sözleşme'nin Türkçe Çevirisi için bkz. 17 Mart 2016 Tarihli ve 29656 Sayılı Resmî Gazete
[90]Y. Avcı(2019). *Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü. 22.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[91]Uncular , 2018, **a.g.k.** , 52.
[92]B. Öztunay(2019). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşverenin Yönetim Hakkının Sınırları*. Yayımlanmamış Yüksek Lisans Tezi. İzmir: İzmir Ekonomi Üniversitesi, Sosyal Bilimler Enstitüsü. 39.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

ihtimali ve artan bilgisayar kullanımı neticesinde ortaya çıkabilecek hak ihlallerine karşı asgari düzeyde de olsa koruma getirmektir.[93]

Özel hayatın gizliliği, insan hakları ile ilgili uluslararası belgelerde koruma altına alınan haklardan biridir. Özel hayat kavramının kapsamın içinde örnek olarak bireylerin fiziksel özellikleri, düşünce ve inançları, sağlık bilgileri, eğitim ve meslek durumu ile ilgili bilgiler, aile bireyleri ve başkaları ile yaptığı haberleşmeler yer almaktadır. Bunlar bireylerin kişisel verileridir.

Kişisel verilerin korunmasına ilişkin önlemlerin alınması konusu ülkeleri oldukça meşgul etmiştir. Bu düzenlemelerin başlatıcısı olan Batı Avrupa, dünya üzerinde kişisel veri korumasının merkezi kabul edilmektedir. Zira kişisel verilerin korunmasının bir ihtiyaç olduğunun ilk farkına varan ülkeler, Avrupa ülkeleridir. Avrupa ülkeleri bu konuda iç hukukunda gerekli düzenlemelerini yapsa da Avrupa Birliği bünyesinde kişisel verilerin korunması konusunda uygulama birliğinin sağlanması için AB bünyesinde uluslararası düzenlemelere ihtiyaç duyulmuştur. Bunlardan biri de Sözleşme'dir.

Bu Sözleşme, ilk uluslararası çok taraflı veri koruma sözleşmesi ve kişisel verilerin işlenmesi ve toplanmasının yol açabileceği kötü kullanımlara karşı bireyleri koruyan bağlayıcı ilk uluslararası belgedir.[94] Özel hayata saygı değerlerinin ve kişiler arası sınırsız bilgi akışının yeniden yapılandırılması amacıyla yapılan bu Sözleşme, kişisel verilerle ilgili belli başlı konuları içermekte ve kişisel verilerin otomatik işleme tabi tutulmasını düzenlemektedir.

Kronolojik olarak Sözleşme'nin ve 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokol'ün uluslararası hukukta yürürlüğe girme süreci şöyledir:

[93]M. Uygun (2010). *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi ışığında kişisel verilerin korunması*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi, Sosyal Bilimler Enstitüsü. 13. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[94]E. Dinç(2006). *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye'nin Durumu*. Yayımlanmamış Yüksek Lisans Tezi. Diyarbakır: Dicle Üniversitesi Sosyal Bilimler Enstitüsü. 41. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

26 maddeden oluşan Sözleşme, 28 Ocak 1981'de imzaya açılmış, 108 sayılı kararla kabul edilmiş ve 1 Ekim 1985 tarihinde uluslararası hukukta yürürlüğe girmiştir.[95]

108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokol, 08.11.2001 tarihinde imzaya açılmış, 181 sayılı karar ile kabul edilmiş ve 01.07.2004 tarihinde uluslararası hukukta yürürlüğe girmiştir.[96]

Sözleşme'nin giriş kısmında çıkartılabilecek sonuçlar şunlardır: Avrupa Konseyi, amaç olarak özellikle hukukun üstünlüğü, insan hakları ve temel özgürlüklere saygılı olmak ve üyeler arası işbirliğinin artması olarak görmektedir.

Girişten, böyle bir sözleşmenin hazırlanmasındaki saik de ortaya çıkmaktadır. Buna göre otomatik işlenen verilerin hudut aşırı akışının artması, hak ve hürriyetlerin muhafazası gereksinimini doğurmuştur. Bunun haricinde Sözleşme, ülke hudutları dikkate alınmaksızın devletlerin haberleşme hürriyetiyle ilgili sorumluluklarını da hatırlatmaktadır. Sözleşme, özel yaşama saygı hakkı ile Avrupa Konseyi'ne üye devlet halkları arasındaki serbest bilgi akışının uyumlu olmasının esas olduğuna vurgu yapmaktadır.

Sözleşme'nin konu ve amacı, şöyle düzenlenmiştir:

> MADDE 1-İşbu Sözleşmenin amacı, her bir Tarafın ülkesinde, uyruğu veya ikamet yeri ne olursa olsun her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır.

Sözleşme'de kişisel verilerin otomatik işlenmesi, özel yaşama bir müdahale olarak görülmektedir ve Sözleşme'nin amacının diğer temel haklar saklı kalmak kaydıyla özellikle özel yaşama saygı hakkını korumak olduğu vurgulanmıştır

Sözleşme'nin tanımlar kısmı şu şekilde yer almıştır:

> MADDE 2- Bu Sözleşmenin amaçları bakımından:

---

[95]M. Kağıtcıoğlu.(2016). *Kişisel Verileri Koruma Kurumu'na İdare Hukuku Çerçevesinden Bir Bakış*. Aurum Journal of Social Sciences, 1 (2) , 77-99, 78. ;Dinç,2006, **a.g.k.**, 43.

[96]Dinç, 2006 **, a.g.k.** , 43.

Protokolün metni için bkz.
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
(Erişim Tarihi:02.03.2020)

Protokol metni için bkz. 24 Mayıs 2016 Tarihli ve 29721 Sayılı Resmî Gazete

a“Kişisel veriler”: Kimliği belirli veya belirlenebilir bir gerçek kişi(“ilgili kişi”) hakkındaki tüm bilgileri ifade eder

b.“Otomatik veri dosyası”; otomatik işleme konu alan bilgilerin tümünü ifade eder;

c.“Otomatik işlem”den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır.

d.“Dosya Yöneticisi”, otomatik veri dosyasının amacının ne olacağı, hangi kişisel veri kategorilerinin kaydedilmesi gerektiği ve bunlara hangi işlemlerin uygulanacağı hakkında karar verebilecek olan gerçek ve tüzel kişileri, kamu kurumunu, birimi veya ulusal kanunlara göre yetkili olan diğer kuruluşları ifade eder.

*Sözleşme*’nin kapsamına ilişkin hususlar şu şekilde yer almaktadır:

MADDE 3-1.Taraflar, işbu Sözleşmeyi kamu sektöründe ve özel sektörde, otomatik kişisel veri dosyalarına ve kişisel verilerin otomatik işleme tabi tutulması konusunda uygulamayı taahhüt ederler.

2.Her devlet, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerinin tevdi edilmesi sırasında veya daha sonra herhangi bir zamanda Avrupa Konseyi Genel Sekreterine muhatap bir beyanla:

a.İşbu Sözleşmeyi, listesi tevdi edilecek olan belli otomatik kişisel veri dosyası kategorilerine uygulamayacağını bildirebilir. Ancak, devlet bu listeye, kendi iç hukukunun otomatik verilerin korunmasına ilişkin hükümlerine tabi olan otomatik dosya kategorilerini dahil edemez. Bu nedenle, ilave otomatik kişisel veri dosyası kategorilerinin kendi iç hukukunun verilerin korunmasına ilişkin hükümlerine tabi kılınması halinde, yapacağı yeni bir beyanla söz konusu listeyi tadil eder;

b. İşbu Sözleşmeyi, topluluklar, dernekler, vakıflar, şirketler, kurumlar ve tüzel kişiliğe sahip olsun veya olmasın, doğrudan veya dolaylı olarak gerçek kişilerin bir araya gelmesiyle oluşmuş her çeşit diğer kuruluş hakkında da uygulayacağını bildirebilir;

c.İşbu Sözleşmeyi, otomatik bilgi işleme konu olmayan kişisel veri dosyaları hakkında da uygulayacağını bildirebilir.

3.Yukarıdaki 2. Fıkranın b veya c bendinde tanımlanan beyanlardan biriyle işbu Sözleşmenin uygulama alanını genişleten her devlet, söz konusu beyanda, genişletmenin ancak tevdi edeceği bir listede gösterilen bazı kişisel dosya kategorilerine uygulanacağını belirtebilir.

4.Yukarıdaki 2. fıkranın a bendinde öngörülen beyanla belli otomatik kişisel veri dosyası kategorilerini Sözleşmenin uygulama alanı dışında tutan Taraf, bunları uygulama alanı dışında tutmayan bir Taraftan işbu Sözleşmenin söz konusu kategoriler hakkında uygulanmasını isteyemez.

5.Keza, işbu maddenin 2.b ve 2.c bentlerinde öngörülen kapsam genişletmelerinden herhangi birini yapmayan Taraf, bu genişletmeleri yapan herhangi bir Tarafın bu hususlarda Sözleşmeyi uygulaması gerektiğini öne süremez.

6.İşbu maddenin yukarıdaki 2. Fıkrasında öngörülen beyanlar, bunları yapmış olan Devlet bakımından, bu beyanların imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerinin tevdi edilmesi sırasında yapılması halinde, sözleşmenin yürürlüğe girdiği tarihte; eğer beyanlar daha sonra yapılmışsa bunların Avrupa Konseyi Genel Sekreteri tarafından alınmasından üç ay sonra hüküm ifade eder.Bu beyanlar Avrupa Konseyi Genel Sekreterine muhatap bir bildirim ile kısmen veya tamamen geri alınabilir. Beyanların geri alınması, bildirimin alındığı tarihten üç ay sonra hüküm ifade eder.

Verilerin korunmasına ilişkin taraf devletin yükümlülüğü şu şekilde yer almıştır:

MADDE 4- 1.Her Taraf, kendi iç hukukunda, işbu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır.

2.Bu önlemlerin Tarafça, en geç, Sözleşmenin kendisi bakımından yürürlüğe girdiği tarihte alınması zorunludur.

Sözleşme'nin "Verilerin niteliği" başlıklı maddesi şöyledir:

MADDE 5-Otomatik işleme konu olan kişisel veriler:

a.Adil biçimde ve yasal yoldan elde edilir ve işlenir;

b.Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılamaz;

c.Kaydedilme amaçlarına uygun ve yerinde olur ve aşırı olmaz;

d.Doğru bilgileri yansıtır ve gerektiğinde güncellenir;

e.Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.

Bu maddede Sözleşme, otomatik işleme konu olan kişisel verilere ilişkin temel ilkeler ve ölçütleri sıralamıştır. Fakat madde, yöntemlere ilişkin ayrıntılardan bahsetmek yerine genel ilkeleri düzenlemiştir. Bize göre Sözleşme, bu maddeyi ayrıntılarıyla düzenlemeli, bu hususları taraf devletlerin iç hukuk inisiyatifine bırakmamalıydı. Zira bu sözleşmenin ortaya çıkışındaki sebeplerden biri, devletler arasında kişisel verilerin korunması konusundaki güvenlik farkıdır. Ayrıca özellikle Avrupa ülkeleri arasında yeterli koruma farklılığı, bunu ortadan kaldıracak ortak ve bağlayıcı bir uluslararası metine ihtiyaç hissedilmesine sebep olmuştur. Dolayısıyla Sözleşme'nin amacına uygun düzenlenmiş, teknik altyapısı olan bir madde olabilirdi.

Sözleşme, bazı özel veri kategorilerine ilişkin ilave güvenlik önlemi öngörmüştür. Bu özel veri kategorileri arasında, ırk, siyasi düşünce, inanç, sağlık ve cinsel hayata

ilişkin ve ceza mahkûmiyetine ilişkin veriler sayılmıştır. Sözleşme'nin, bu konunun düzenlendiği 6. maddesine göre bu tür özel veriler, otomatik işleme tabi olamayacaktır.

Veri güvenliğine ilişkin diğer maddeler de Sözleşme'de yer almıştır. Burada Sözleşme, alınacak önlemlerin ne olduğu konusuna açıklık getirmemekle beraber, taraf devletleri, gerekli önlemi almak konusunda yükümlü kılmıştır. Veri güvenliğine ilişkin 7. maddeye göre "*otomatik dosyalara kaydedilen kişisel verileri korumak için, bunların kaza sonucu veya izinsiz olarak imhasına veya kaza sonucu kaybolmasına veya bunların izinsiz elde edilmesine, değiştirilmesine veya dağıtılmasına karşı uygun güvenlik önlemleri alınır*". Her ne kadar maddede, doğrudan devlete bir yükümlendirme olmasa da 7. maddede öngörülen önlemleri alacak olan, Sözleşme'ye taraf devletlerdir.

Sözleşme'nin veri güvenliği ile ilgili, kişilere sağladığı haklar, şöyle düzenlenmiştir:

> MADDE 8-Herkes;
>
> a-Otomatik kişisel veri dosyasının varlığını, ana amaçlarını, dosya yöneticisinin kimliğini ve mutat ikamet yerini veya başlıca işyerini öğrenmek,
>
> b-Makul aralıklarla ve aşırı gecikmeye veya masrafa maruz kalmadan kendisi ile ilgili kişisel verilerin otomatik dosyada bulunup bulunmadığının teyidini almak ve bu bilgilerin kendisine anlaşılır bir biçimde biçim altında iletilmesini sağlamak,
>
> c-Gerektiği durumlarda, bu verileri tashih ettirmek veya bunların, işbu sözleşmenin 5. ve 6.maddelerinde atıfta bulunulan temel ilkelere işlevsellik sağlayan iç hukuk hükümlerinin ihlali suretiyle işlenmiş olması halinde, söz konusu verileri sildirtmek,
>
> d-İşbu maddenin b ve c fıkralarında düzenlenen teyit talebinin veya duruma göre bildirme, tashih veya silme talebinin yerine getirilmemesi halinde bir başvuru yolundan yararlanmak hakkına sahiptir.

Sözleşme'nin 9. maddesine göre bazı hususların gerçekleşmesi için kanunlarında öngörmüş olmak ve gerekli önlemleri almak koşuluyla taraf devletler, 5., 6. ve 8. maddelerine istisna getirilebilecek önlemler alabilecektir. Bu hususlar; devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatlerinin sağlanması, suçların önlenmesi, ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması olarak belirlenmiştir.

İlgili kişilerin özel yaşamlarına tecavüz tehlikesi bulunmadığının açık olduğu durumlarda, 8. maddenin b, c ve d fıkralarında düzenlenen haklar istatistiki veya

bilimsel amaçlar için kullanılan kişisel veri dosyaları bakımından kanunla kısıtlanabilir.(M.9/3)

Veri kalitesinin sağlanması amacıyla, belirli ölçütler getiren Sözleşme, ayrıca veri sahibinin haklarını da ortaya koymaktadır. Buna göre, her gerçek kişinin, kendisine ait verileri içeren bir dosyanın varlığından ve tutulma amacından haberdar edilme, bu içeriğe ilişkin bilgi talep etme, bu verilerin düzeltilmesini veya silinmesini isteyebilme ve nihayet bu taleplerinin karşılanmaması veya söz konusu kişisel verilerle ilgili açıklama yapılmaması halinde dava açma hakkına sahip olduğu ifade edilmektedir

Sözleşme, taraf devletler arasında veri akışının sağlanmasını desteklemektedir. Nitekim Sözleşme'nin 12. maddesi, taraf devletlerin, sınır ötesi veri akışını engellemelerini kural olarak yasaklamıştır. Ancak istisnaen, belirli veri türleri bakımından özel düzenleme getirmiş olan devletlerin, söz konusu veriler bakımından eş düzey koruma getirmeyen ülkelere veri akışını yasaklayabilmeleri imkân dahilindedir.

Netice itibariyle Sözleşme'nin amacı, tüm dünyada kişisel verilerin korunması bilinci oluşturmak suretiyle hem Avrupa Konseyi üyelerini hem de üye olmayan devletleri kişisel verilerin korunması çabasına ortak etmektir.[97]

### 2.7. 45/95 sayılı Birleşmiş Milletler Bilgisayarla İşlenen Veri Dosyalarıyla İlgili Rehber İlkeler

14 Aralık 1990 tarihinde BM Genel Kurulu tarafından 45/95 sayılı BM Bilgisayarla İşlenen Kişisel Veri Dosyalarıyla İlgili Rehber İlkeler[98] kabul edilmiştir. Bu ilkeler ile bilgisayar ile yapılan kişisel veri işlemelerinde ulusal mevzuatlarda sağlanması gereken asgari ölçütlere ilişkin BM üyesi ülkelere yol gösterilmesi amaçlanmıştır.[99] BM nezdinde çıkarılan rehber ilkeleri tavsiye niteliğinde olup BM üyesi devletler için de bağlayıcı nitelikte değildir. BM'nin 45/95 sayılı tavsiye

[97]Yıldırım , 2019, **a.g.k. ,** 44.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[98]https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ddcafaac(Erişim Tarihi:20.03.2019)
https://www.refworld.org/pdfid/3ddcafaac.pdf(Erişim Tarihi:05.03.2020)
[99]Başalp , 2004, **a.g.k.** , 25.

niteliğindeki rehber ilkeleri, kişisel verilerin korunmasında bağımsız kişisel veri koruma organları oluşturulmasına dikkat çeken ilk uluslararası hukuk belgesidir.[100]

45/95 sayılı Rehber İlkeler'de bahsedilen temel ilkeler şöyle sıralanabilir:

- Dürüstlük ve yasalara uygunluk ilkesi uyarınca kişisel veriler, haksız veya yasadışı yollardan toplanmamalı veya işlenmemeli, Birleşmiş Milletler Tüzüğü'nün amaç ve ilkelerine aykırı amaçlar için kullanılmamalıdır. (1.ilke)
- Doğruluk ilkesi uyarınca kişisel verileri toplamak ve saklamaktan sorumlu kişiler, verinin doğruluğunu ve güncelliğini ve dosyada tutulan bilginin kullanılmasını sağlamalıdır.(2.ilke)
- Amacın belirliliği ilkesi uyarınca kişisel veri dosyasını hazırlama amacı meşru olmalıdır. Kişisel veri dosyası, hazırlanma amacı doğrultusunda ve amaca ulaşana kadar kullanılmalıdır. Kişisel veri dosyası kamuya açık olmalıdır.(3. ilke)
- İlgili kişinin erişimi ilkesi uyarınca kimliğini belgeleyen herkes, kendisiyle ilgili bilgilerin işlenip işlenmediğini bilme ve bu bilgileri gereğinden fazla gecikme veya harcama olmadan anlaşılır bir şekilde elde etme ve bu durumda yapılması gereken düzeltmeleri veya silmeleri yapma hakkına sahiptir.(4.ilke)
- Eşitlik ilkesi uyarınca yasadışı veya keyfi ayrımcılığa neden olabilecek veriler toplanmamalıdır ve işlenmemelidir.(5.ilke)
- Güvenlik ilkesi uyarınca dosyaları kazayla kaybolma veya imha gibi doğal tehlikelere ve yetkisiz erişim, dolandırıcılık amaçlı kötüye kullanma veya bilgisayar virüsleri ile kirlenme gibi insan tehlikelerine karşı korumak için uygun önlemler alınmalıdır(7.ilke).

45/95 sayılı Rehber İlkeler'e göre dürüstlük ve yasalara uygunluk ilkesi, doğruluk ilkesi, amacın belirliliği ilkesi ve ilgili kişinin erişimi ilkeleri'nden sapılması yalnızca milli güvenlik, toplum nizamı, halk sıhhati yahut ahlakının gerektirdiği durumların yanı sıra başkalarının özellikle de zulüm gören kişilerin hak ve özgürlüklerini korumak için gerekli olmaları durumunda mümkündür. Ayrıca bu tür sapmaların, sınırlarını açıkça

[100]C. Başar (2019). *Türk İdare Hukuku ve Avrupa Birliği Hukuku ışığında kişisel verilerin korunması*. Yayımlanmış Doktora Tezi,. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü. 136. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp(Erişim Tarihi:25.02.2020)

belirten ve uygun önlemleri ortaya koyan iç hukuk sistemine uygun olarak ilan edilen bir yasada veya eşdeğer bir düzenlemede açıkça belirtilmesi gerekmektedir.(6.ilke)

45/95 sayılı Rehber İlkeler'e göre her ülkenin mevzuatı, yerel hukuk sistemine göre yukarıda belirtilen ilkelere uyulmasının denetlenmesinden sorumlu olacak olan otoriteyi belirler. Bu otorite tarafsızlık, şahıslara karşı bağımsızlık ve teknik yeterlilik garantisi sunacaktır. Yukarıda belirtilen ilkeleri uygulayan ulusal yasa hükümlerinin ihlali durumunda uygun bireysel çözümlerin yanı sıra cezalar da öngörülmelidir.(8.ilke)

45/95 sayılı Rehber İlkeler'e göre iki ya da daha fazla ülkenin mevzuatı mahremiyetin korunmasına yönelik eşit korumalar sunduğunda, sınır ötesi veri akışı sağlanmalıdır.(9.ilke)

45/95 sayılı Rehber İlkeler, kamusal alandaki ve özel kullanıma tahsis edilmiş bilgisayarlarda hazırlanan veri dosyalarında kıstas alınabileceği gibi fiziken hazırlanan dosyalarda da uygulanabilir olmalıdır. Ayrıca bu rehber ilkeler, isteğe bağlı olarak tüzel kişilere ait verilerin dosyalanmasında da rehber kabul edilebilir.(10.ilke)

## 2.8. 95/46 Sayılı Avrupa Parlamentosu ve Avrupa Konseyi Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Yönergesi (Avrupa Topluluğu Veri Koruma Yönergesi)

### 2.8.1.Veri koruma yönergesinin amacı

Yönerge[101], kişisel verilerin korunması hukuku açısından AB bünyesinde yapılan en temel düzenlemedir.[102] Aynı zamanda bu Yönerge, kişisel verilerin korunması alanında AB bünyesinde oluşturulmuş ilk yasal düzenlemedir.[103] Yönerge bağlayıcı değildir fakat AB üyesi ülkelerin bu yönergelere uygun bir ulusal mevzuat oluşturmaları beklenmektedir. Bu açıdan yönerge ile tüzük'ün farkı şöyle açıklanabilir: Tüzük, doğrudan uygulanabilir bir mevzuat türüdür. Yönerge ise doğrudan uygulanmaz fakat

[101]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (Erişim Tarihi:20.03.2019) ; Türkçe Çevirisi için https://kisiselveri.com/9546ec-turkce (Erişim Tarihi:20.03.2019)
[102]Çalışmanın bu başlığı altında 95/46 EC sayılı Yönerge'den kısaca "Yönerge" olarak bahsedilecektir.
[103]Z. U. Gözüm(2019). *Kişisel Verilerin Korunmasının İş İlişkisi Açısından Değerlendirilmesi*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü. 31. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

AB üyesi ülkelerden bu Yönerge'ye uygun bir iç hukuk mevzuatı oluşturmaları beklenir.[104]

Kişisel verilerin serbest akışı sağlanmadığı müddetçe mal ve hizmet dolaşımının sağlanması da mümkün değildir.[105] Hal böyleyken üye ülkeler arasındaki iç hukuk farklılıklarının serbest dolaşım hakkına engel olacağı da bir gerçektir.[106] Bu gerçeğin farkına varan Avrupa Konseyi, Yönerge'nin hazırlanması sürecini başlatmıştır.

Her ne kadar 108 sayılı Sözleşme AB üyesi ülkelerce onaylanmış olsa da bu ülkeler, kendi iç hukuklarında farklı veri koruma mevzuatı oluşturma eğilimi göstermişlerdir.[107] Bunun yanında kişisel verilerin ticaretin konusu haline gelmesinin yaygınlaşmasıyla üye devletler arasında uygulama farklılığı da görülmeye başlamıştır.[108] Bu da üye ülkeler arasında eşdeğer koruma düzeyinin oluşmasını engellemiştir. Üye ülkeler arasında eşdeğer veri koruma düzeyinin olmaması da ülkeler arasındaki serbest ticaretin sağlanması ve dolayısıyla ortak pazarın kurulması gerekli olan sınır ötesi veri akışını engellemiştir.[109]

İşte bu engelin ortadan kalkması amacıyla düzenlenen Yönerge'nin amacı, Avrupa topluluğunun üye ülkeleri arasındaki ortak pazarın geliştirilmesi için gerekli olan kişisel verilerin sınır aşan veri trafiğinin sağlanması sırasında gerçek kişilerin kişilik haklarının ve özel hayatlarının korunması için üye ülkelerin eş değer koruma sağlayan ulusal mevzuat oluşturmalarında yol gösterici olan ve üye devletler tarafından uyulması beklenen ilkeler belirlemektir.[110] Dolayısıyla tüm üye devletlerde eş değer koruma düzeyinin sağlanması ile sınır ötesi veri akışlarında insan hakları referanslı itirazların önü kesilmek istenmiştir. Ancak ulaşılmak istenen nihai amaç sınır ötesi veri akış trafiğinde bireyi güvenceye almak suretiyle AB bünyesindeki ortak pazarın gelişimini sağlamaktır. En azından Avrupa Birliği Adalet Divanı'nın kişisel verilerin korunmasına ilişkin kararlarında AB'nin kuruluşundaki ekonomik amacını üstün tutan

---

[104]U. Dal (2019). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti*. Kişisel Verileri Koruma Dergisi. 1 (1) , 21-33, 23.
[105]S. Hatipoğlu(2019). *Kişisel Verilerin Korunması Ve İdarenin Sorumluluğu*. Yayımlanmamış Yüksek Lisans Tezi. Edirne: Trakya Üniversitesi. Sosyal Bilimler Enstitüsü. 56.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[106]Hatipoğlu, 2019, **a.g.k.**, 56.
[107]Uygun, 2010, **a.g.k.**, 33.
[108]A. N. Akıncı(2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*. T.C. Kalkınma Bakanlığı. Yayın No: 2968, 6.
[109]Başalp , 2004 , **a.g.k. ,** 30 , 31.
[110]Başalp , 2004, **a.g.k.** , 30.

bir yaklaşım sergilediğini söylemek mümkündür.[111] Fakat bu anlayıştan zamanla uzaklaşıldığı ve Tüzük'ün hazırlanış sürecinde bu değişen anlayışın yol gösterici olduğu görülmektedir.[112]

Yönerge, mevcut veri koruma hukukunu güçlendirmenin yanında bazı yeni haklar getirmek suretiyle ortak bir çerçeve ortaya koymuştur.[113]

Yönerge, gerek mahremiyeti en üst düzeyde koruyan düzenlemeleriyle gerekse verilerin serbest akışına izin vermesiyle kişisel verilerin korunması hususunda AB tarafından atılmış önemli bir adım olarak görülebilir.[114]

Ayözger'e göre Yönerge'nin bazı dikkat çekici özellikleri vardır[115]:

- Kamu ve özel sektörü ayrımı olmadan uygulanması
- Veri koruma hukukunu geniş olarak düzenlemesi
- Veri koruma hukukuna ilişkin fiilleri gönüllü olarak yapacaklara pozitif sorumluluklar yüklemesi
- Sektörel sınırlamalar getirmesi

### 2.8.2.Temel kavramlar

Yönerge, kişisel veriyi, "*fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgi*" olarak tanımlamıştır (M.2-a).

Bu tanıma göre; bireyin kimlik numarası, ismi, taşıt plakası, pasaport numarası, resmi, sesi, parmak izi gibi bireye ulaşılmasını temin eden veriler kişisel verilerdir.

---

[111]O. D. Yörük, (2019). *AB 2016/679 sayılı Avrupa Birliği genel veri koruma tüzüğü doğrultusunda kişisel verilerin korunması*; Yayımlanmış Yüksek Lisans Tezi. İzmir: İzmir Ekonomi Üniversitesi, Sosyal Bilimler Enstitüsü. 41.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[112]Yörük, 2019, **a.g.k**. , 41.
[113]Buğçehan Arıklı(2019). *KKTC hukukunda kişisel verilerin korunması*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi, Lisansüstü Programlar Enstitüsü. 22.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[114]Kılınç , 2012, **a.g.k.** , 1120.
[115]A. Ç. Ayözger(2016) *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*. Yayımlanmamış Doktora Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü. 82.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

Kişisel verilerin işlenmesi, "*silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisi*" olarak tanımlanmıştır( M.2-b).

Otomatik yol ile kişisel verilerin işlenmesinden anlaşılması gereken, bilgisayar ve benzeri otomasyon sistemleri kullanmak suretiyle verilerin işlenmesidir.[116] Bunun dışında bir otomasyon sistemlerinden yararlanılmayan veri işlemesi ise otomatik olmayan(elle) veri işlemesidir.[117]

Yönerge'nin kişisel veri işlemeyi tanımlamaktan ziyade örnekler vererek kişisel veriyi açıkladığı ve bu örnekleri sınırlamadığı görülmektedir. Bu açıdan Yönerge'nin kişisel veri işleme faaliyetinin kapsamını açık bıraktığı anlaşılmaktadır.

Otomatik olmayan veri işleme, geleneksel veri işleme yöntemi olup, bilgisayar teknolojisinin gelişmediği dönemde de uygulanan bir veri işleme yöntemidir.

Otomatik veri işlemesi, bilgisayar gibi otomasyon sistemlerinin ortaya çıkışı ile kullanılmaya başlanan veri işleme yöntemidir.

Yönerge'de yer alan diğer tanımların ise şöyle olduğu görülmektedir:

- Alıcı, "*bir üçüncü şahıs olsun ya da olmasın, verilerin açıklandığı bir gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya başka bir kurul*"dur. Ancak, özel bir soruşturma çerçevesinde verileri alan makamlar alıcı olarak kabul edilmezler(M.2-g).
- Üçüncü şahıs; "*veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici, veri öznesi dışındaki herhangi bir gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya başka bir kuruluş*" tur(M.2-f).
- İşleyici, "*denetleyici adına kişisel verileri işleyen bir gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya diğer bir kuruluş*"tur(M.2-e).

[116]F. G. Taştan(2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. İstanbul: On iki Levha Yayınları. 46.
[117]Taştan , 2017, **a.g.k. ,** 47.

- Kişisel veri dosyalama sistemi, "*ister merkezi ister merkezi olmayan ya da bir işlevsel veya coğrafi tabana dağıtılmış özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisi*"dir(M.2-c).
- Denetleyici, "*kişisel verilerin işlenme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya başka bir kuruluş*"tur(M.2-d).
- Veri öznesinin rızası, "*kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rıza*"dır(M.2-h).

### 2.8.3.Veri koruma yönergesinin uygulama alanı ve ilkeleri

Yönerge'nin uygulama alanı, yönergenin 3. maddesinde şöyle düzenlenmiştir:

> MADDE 3- 1.Bu Direktif, bir dosyalama sisteminin parçasını oluşturması istenen veya bir dosyalama sisteminin parçasını oluşturan kişisel verilerin otomatik araçlar dışında işlenmesine ve kısmen veya tamamen otomatik araçlarla kişisel verilerin işlenmesine uygulanacaktır.
>
> 2.Bu Direktif, kişisel verilerin işlenmesine uygulanmayacaktır:
>
> a.ceza hukuku alanındaki Devlet faaliyetleri ve (işleme faaliyeti Devlet güvenlik konularını ilgilendirdiğinde, Devletin ekonomik refahı dahil olmak üzere) Devlet güvenliği, savunma, kamu güvenliğine ilişkin verilerin işlenmesi için herhangi bir durumda ve Avrupa Birliği Anlaşmasının V ve VI. başlıklarıyla belirtilenler gibi Topluluk hukuku kaspamının dışına düşen bir faaliyet esnasında,
>
> b.bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında.

Yönerge, veri işleyicinin kamu veya özel sektör olması açısından bir ayrım gözetmemektedir.

Tüzel kişiler hakkında tutulan veriler kural olarak Yönerge kapsamında değildir.[118] Fakat bir tüzel kişiye ait veriden bir gerçek kişiye ulaşmak mümkünse bu tüzel kişiye ait verinin işlenme süreci Yönerge kapsamındadır.[119]Örneğin bir dernek tüzel kişisinin üye kayıt defterinden bir gerçek kişiye ulaşmak mümkün olduğundan dernek üye kayıt defterinin oluşturulma süreci Yönerge kapsamındadır.

[118]A. Akgül(2013). *Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi*. Yayımlanmış Doktora Tezi. Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü. 150. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[119]Başalp , 2004, **a.g.k.** , 35.

Yönerge'nin temeli, mahremiyetin korunması ve bireyin özel yaşamına müdahaleleri engelleme amacıyla Yönerge'de düzenlenen veri koruma ilkelerinden oluşmaktadır.[120] Yönerge'nin ortaya koyduğu bu ilkelerle veri sorumlusunun veri işlerken takip etmesi gereken sorumluluklar tespit edilmekte, veri işleme esnasında veri sorumluları ve özneleri arasında meydana gelen menfaat çatışmasında denge kurulmaya çalışılmaktadır.[121]

Yönerge, verilerin hukuka ve objektif iyiniyet kurallarına münasip şekilde işlenmesinin belirli koşullara ve ilkelere uymakla gerçekleşeceğini öngörmüş olup aşağıda bunlar hakkında bilgi verilmiştir.

Dürüstlük kuralı olarak da adlandırılan objektif iyiniyet, "*kişilerin haklarını kullanırken ve borçlarını ifa ederken dürüst, namuslu, ahlaklı ve iyiniyetli bir insandan beklenecek şekilde davranma zorunluluğu*" olarak tanımlanmıştır.[122]

Amaca bağlılık ilkesi uyarınca veri işlemenin belirli ve açık bir amacı olmalıdır. Amacın belirli olmasından kasıt verinin amaca uygun olarak işlenip işlenmediğinin denetiminin kolay olması için amacın yazılı olarak belirlenmesidir. Amacın açık olmasından kasıt kişisel verilerin sadece bariz bir şekilde tespit edilmiş bir gaye ile işlenebileceğidir(M.6-1/b).

Yönerge'ye göre Avrupa topluluğuna üye devletlerin yeterli korumayı sağlamaları şartıyla tarihsel, istatistiksel veya bilimsel amaçlar için veri işlenmesinde amaca bağlılığın varlığı karine olarak sayılmıştır(M.6-1/b).

Gereklilik ilkesine göre ulaşılmak istenen amaç için gerekli olan kişisel veriler işlenmelidir(M.6/f.1/b.c). Örneğin bir işveren, işçilerine karşı iş hukukunun kendisine yüklediği sorumlulukları yerine getirmesini sağlamaya yeterli kişisel verileri işlemelidir. Gereklilik ilkesinin uzantısı olan depolama yasağı ilkesine göre ise gelecekteki olası bir amacın gerçekleştirilmesi için veri işlenmesi yasaktır.[123]

---

[120]B. Yılmaz(2019). *Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. Yayımlanmış Doktora Tezi. Ankara: Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü. 155.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[121]Yılmaz , 2019, **a.g.k.** , 155.
[122]S. Helvacı ve F. Erlüle(2011). *Medeni Hukuk*. İstanbul : Legal Kitabevi. 91.
[123] Başalp , 2004 , **a.g.k.** , 38.

Bunun dışında işçisinin üye olduğu dernek, sendika, parti veya mahkum olduğu cezalar gibi verileri işçisine ait dosyaya işlememelidir. Zira bu verilerin işçi-işveren hukuki ilişkisinde belirleyici bir rolü ve gereği yoktur.

Maddi gerçeklik ilkesi, toplanan ve işlenen verinin doğru, maddi gerçeğe uygun olmasını gerektirir. Bu doğruluk ve gerçekliğin sağlanması açısından verinin sürekli güncellenmesi gereklidir. Gerçekliği ortadan kalkmış, gerçek olmadığı tespit edilen ve işleme amacı ortadan kalkmış kişisel veriler silinmelidir. Yanlış işlendiği tespit edilen veriler düzeltilmelidir.(M.6/f.1/b,d)

Bir verinin saklanması, işleme amacının gerçekleştiği ana kadar hukuka uygundur. Amaç gerçekleştikten sonra veri silinmeli veya anonimleştirilmelidir. Anonimleştirilmeden kasıt verinin veri sahibiyle bağlantısının ortadan kaldırılmasıdır. Bir bakıma o veriden veri sahibine ulaşılamaz hale getirilmesidir. Bu açıdan örneğin bir işveren işçisiyle iş ilişkisi sona erdikten sonra işçisine ait verileri imha etmeli veya anonimleştirmelidir(M.6/f.1/b,e).

### 2.8.4. Hukuka uygunluk sebepleri

İlke olarak veri işlemesi hukuka aykırı bir eylemdir. Diğer bir anlatımla kişisel verilerin işlenmemesi esastır. Fakat belirli şartların bulunması durumunda veri işleme hukuka uyarlık vasfını kazanmaktadır. Yönerge uyarınca Avrupa Topluluğu üyeleri, bu hukuka uygunluk sebepleri gerçekleşmeden kişisel verilerin işlenmesine müsaade etmemelidir(M.7).

Hukuka uygunluk sebepleri şöyle açıklanabilir:

Veri sahibinin rızası, kişisel verinin işlenmesini hukuka uygun hale getiren irade açıklamasıdır. Yönerge'de veri öznesinin(sahibinin) rızası, "*kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rıza beyanı*" olarak tanımlanmıştır(M.2-h). Rıza beyanı baskıya maruz kalmadan ve tereddüde yer vermeyecek şekilde yapılan her türlü irade açıklamasıdır. Beyanın tereddüde yer vermemesinden kasıt veri öznesinin rızası olduğundan şüphe edilmemesidir. Yönerge, rıza beyanını şekle bağlı kılmamıştır. Dolayısıyla tereddüde yer vermedikçe her şekilde rıza beyanında bulunmak mümkündür (M.7/a).

Rızanın veri işlemeden önce verilmesi gerekmektedir; işlemeden sonra verilen rıza işlemenin hukuka aykırılığını ortadan kaldırmaz.[124]

Eğer kişisel verilerin işlenmesi, yasal yükümlülük gereği ise bu veri işlemesi hukuka uygundur.[125] Örneğin işveren tarafından işçi özlük dosyası hazırlanması iş kanunu tarafından işverene yüklenen bir yükümlülük olduğundan işverenin işçi özlük dosyası hazırlaması hukuka uygundur.[126]

İşçiye ücretinin yatırılması için banka hesap numarasının işlenmesinin yasal yükümlülük olduğu için hukuka uyarlık taşıdığı söylenebilir.[127]

Sözleşme öncesi hazırlık işlemlerinin icrası ve sözleşmenin ifası amacıyla kişisel verilerin işlenmesi hukuka uygundur.[128] Sözleşme öncesi hazırlık işlemleri, sözleşmenin kurulması için uygun koşulların oluşturulması için yapılan işlemler olarak tanımlanabilir. Örneğin, bir araç satış şirketinden araç satın alınmak istenmesi durumunda şirket yetkilileri henüz satışa hazır araç olmadığını söyleyerek araç satın almak isteyen kişiye ulaşmak üzere kimlik, telefon ve adres bilgilerini kaydetse kira sözleşmesi öncesi hazırlık işlemini icra etmek için olduğundan bu veri işlemesi hukuka uygundur. Daha sonra aracın mülkiyetini alıcıya devretmek için gerekli bilgileri kayıt altına alırsa bu veri işlemesi sözleşmenin ifası için gerekli olduğundan hukuka uygundur(M.7/b).

Diğer bir hukuka uygunluk sebebi, İlgili kişinin hayati menfaatinin korunmasıdır. Örneğin bir hastanede tedavi altına alınan lösemi hastasının kan grubunun hastane tarafından kayıt altına alınmasında hastanın üstün özel yararı olduğu için bu kayıt hukuka uygundur(M.7/d).

Yaşamsal çıkarlarının mevcudiyetine rağmen ilgili kişinin rızasını almak imkan dahilinde değilse kişisel veriler, kamu menfaati gereği işlenebilir ve bu veri işlemesi hukuka uygundur. Örneğin hastanede tedavi altına alınan ve bilinci kapalı olan bir hastanın kan grubu, hastanın rızasını almak mümkün olmadığı için ilgilinin hayati

[124]N. Yücedağ(2017). *Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.75 (2), 765-790, 775.
[125]Başalp , 2004, **a.g.k.** , 41.
[126]Uncular , 2014 , **a.g.k.** , 57.
[127]Yücedağ , 2017 , **a.g.k. ,** 779.
[128]Korkmaz , 2019 , **a.g.k.** , 216.

menfaati gereği hastane yetkilileri tarafından kayıt altına alınabilir; zira hastaya kan takviyesi gerekmesi durumunda kan grubunun bilinmesi gerekir.

Kamu menfaati ve kamu düzeni gereği görev ifası da hukuka uygunluk sebebidir. Bomba yüklü bir aracın köprüden geçeceği ihbarını alan güvenlik görevlilerinin köprüden geçen araçların plakalarını kayıt altına alması kamu düzenini korumanın gereği olduğundan hukuka uygun bir veri işlemesidir(M.7/e).

Diğer bir hukuka uygunluk sebebi olan haklı çıkarların korunmasına göre verinin işlenmesinden beklenen menfaat ile veri öznesinin temel hak ve özgürlüklerinin korunmasından beklediği menfaat arasındaki denge korunduğu müddetçe veri işlemesi hukuka uygundur.[129] Buna bir bankanın güvenlik kamerası kayıt sistemi kurması örnek verilebilir. Fakat bu kamera sisteminin kurulması sadece bankanın güvenliğini sağlama amacını gerçekleştirdiği ölçüde meşrudur.

### 2.8.5. Hassas verilerin işlenmesi

Yönerge, hassas verinin tanımı açıkça belirtilmese de hassas verilerin neler olduğu sayılmıştır. Belirli istisnalar dışında hassas verilerin işlenmesi yasaktır.

Yönerge'nin 8/1 maddesine göre üye devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır.

Her ne kadar Yönerge'nin 8. maddesinde hassas veriler sınırlı sayı ilkesi gereği sıralamış olsa da amacın hassas verileri korumak olduğu dikkate alındığında hassas verilere ulaştıran her verinin de hassas veri sayılıp korunması gerektiği yönünde görüşler de mevcuttur.[130] Örneğin bir sendikanın aylık olarak çıkarmış olduğu dergiye abone olan memurların listesinden bu sendikaya üye olan kişilere ulaşmak mümkün olduğu için bu derginin abonelerini listelemek de hassas verileri işleme yasağı kapsamında sayılmalıdır. Çünkü böyle bir abone listesini oluşturmaktan bir yarar beklenmesinden ziyade ayrımcılığa zemin hazırlanmasını beklemek daha olasıdır.

*Yönerge*'yi dikkate alarak iç hukuklarında gerekli veri koruma mevzuatlarını hazırlamaları tavsiye edilen AB üyesi ülkelerin ekseriyetinin hassas verilerin kapsamı

[129]Başalp , 2004 , **a.g.k.** , 41.
[130]Uygun , 2010 , **a.g.k.** , 59.

hususunda *Yönerge*'nin 8. maddesini dikkate alsa da bazı ülkelerin başka verileri de hassas veri olarak sayan düzenlemeler getirdiği görülmektedir.[131]

Bunun dışında hassas verilerin kapsamını genişleten yargı kararları da mevcuttur. Örneğin Avrupa Topluluğu Adalet Divanı'nın Lindqvist kararında[132] ayağını inciten kişinin fotoğrafının internette yayınlanmasını hassas veri yasağının ihlali sayması, "*istisnalar dar yorumlanır*" kuralına aykırı olarak Yönerge'nin 8. maddesini geniş yorumladığı gerekçesiyle eleştirilmiştir.[133]

Bu verilerin hassas veri olarak belirlenmesinin temel sebebi, bu veriler sebebiyle kişilerin ayrımcılık yasağına uğrama tehlikesidir.[134] Örneğin kişi cinsel tercihleri, siyasi görüşleri, dini-felsefi inancı, ırk ve etnik kökeni sebebiyle ayrımcılığa maruz kalabilir. Bu sebeple bu veriler hassas verilerdir ve kural olarak işlenmesi yasaktır. Fakat bu verilerin işlenmesinin hukuka uygun olduğu haller de mevcuttur ve bu hukuka uygunluk hallerine Yönerge'nin 8. maddesinde yer verilmiştir. Dolayısıyla mutlak bir hassas işleme yasağından söz etmek mümkün değildir.

Hassas verilerde işlem yasağının bazı istisnaları vardır ve bu istisnaların gerçekleşmesi halinde hassas verilerin işlenmesi hukuka uygun hale gelmektedir:

Veri öznesinin açık rıza beyanı hassas verilerin işlenmesini hukuka uygun hale getirir( M.8). Yönerge'nin 8. maddesinde aranan rıza açık rıza beyanı iken Yönerge'nin 7. maddesinde aranan rıza beyanı tereddüde vermeyecek surette bir rıza beyanıdır. Açık rızanın tereddüde yer vermeyecek rızadan farkı şudur: Bir zımni rıza beyanından rızanın varlığı tereddüde yer vermeyecek şekilde anlaşılıyorsa tereddüde yer vermeyecek rızanın varlığından söz edilebilir. Böyle bir rıza ile hassas olmayan verilerin işlenmesi hukuka uygun olur. Fakat hassas verilerin işlenmesinin hukuka uygun olması için tereddüde yer vermeyen zımni rıza dahi yeterli değildir. Rıza açık olmalıdır.

---

[131]Uygun , 2010 , **a.g.k.** , 60.
[132]ABAD , C-101/01, Bodil Lindqvist , 6 Kasım 2003;
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62001CJ0101&from=EN (Erişim Tarihi:09.03.2020)
Kararın Türkçe Çevisiri için bkz. http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_8.pdf (Erişim Tarihi:09.03.2020)
[133]Uygun , 2010 , **a.g.k.** , 60.
[134]F. Dinkci(2014). *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye Örneği*. Yayımlanmamış Yüksek Lisans Tezi. Samsun: Ondokuz Mayıs Üniversitesi, Sosyal Bilimler Enstisüsü. 55.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp(Erişim Tarihi:25.02.2020)

Bununla birlikte hassas verinin işlenmesine açık rıza gösterilmiş olsa da eğer üye ülkenin iç hukuku bu hassas verinin işlenmesini yasaklamışsa açık rızanın varlığının hassas verinin işlenmesini hukuka uygun hale getirmeyeceği yine Yönerge'nin 8. maddesinden çıkarılacak bir sonuçtur.

İş hukuku kuralları gereği veri sorumlularınca veri işlenmesi hukuka uygundur. Örneğin işverenin kanun gereği tutmak zorunda olduğu işçi özlük dosyası hukuka uygun bir veri işlemesidir.

Bir bankanın kredi sözleşmesi akdetmesi nedeniyle müşterisinin kimlik bilgilerini, ikamet bilgilerini ve gelir bilgilerini kayıt altına alması fiilleri sözleşmenin ifası için gerekli veri işleme faaliyetleri olup hukuka uygundur.[135]

Veri sahibinin açık rızasının alınması hukuken ve fiziken mümkün değilse hassas verinin işlenmesi hukuka uygundur(M.8/f.2-b).[136] Örneğin veri sahibi hakkında gaiplik kararı varsa bu kişiye fiziken ulaşmak mümkün olmadığından bu kişiye ait hassas verinin işlenmesi açık rızası olmasa da hukuka uygundur. Veya kişi hakkında akıl sağlığı yerinde olmadığı için vasi tayin edilmişse bu kişiden açık rıza almak hukuken mümkün olmadığından bu kişiye ait hassas verinin işlenmesi açık rızası olmasa da hukuka uygundur.

Yönerge uyarınca hassas verilerin işlenmesi ilke olarak yasaktır. Fakat verilerin kamuya açıklanması durumunda hassas verinin işlenmesi hukuka uygun olacaktır(M.8/f.2-e). Fakat veri sahibince kamuya açıklansa bile hassas verilerin işlenmesi halinde veri sahibinin hususi alanı yahut hak ve hürriyetleri ihlal edilecekse verinin işlenmesi hukuka aykırı olmaya devam edecektir.[137]Zira veri sahibinin kamuya açıklamasıyla hassas verinin kesin işlenmesi yasağı ortadan kalksa da bu yasağın kalkması Yönerge'nin 6. ve 7. maddelerindeki veri işleme kriterlerinin sağlanmasına gerek kalmadığı anlamına gelmez.

Hassas verinin yargılama kapsamında işlenmesi hukuka aykırılığını ortadan kaldıracaktır. Örneğin bir mahkeme, kişinin üye olduğu sendikaya ilişkin bilgi vermesi için İçişleri bakanlığına müzekkere gönderse ve bu müzekkere üzerine İçişleri bakanlığı, mahkemenin kararını yerine getirmek için kişinin üye olduğu sendikaya

[135]Çokmutlu , 2014 , **a.g.k.** , 104.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)
[136]K. Kılıç(2016) *Kişisel Verilerin Korunması ve 6698 Sayılı Kanun*. Yayımlanmamış Yüksek Lisans Tezi. Erzurum: Atatürk Üniversitesi Sosyal Bilimler Enstitüsü. , 21.
[137]Başalp , 2004 , **a.g.k.** , 45.

ilişkin verileri toplasa ve mahkemeye göndereceği resmi yazıya aktarsa bu veri işlemesi hukuka uygun hassas veri işlemesi olacaktır. Veya mahkemenin isteği üzerine bir sağlık kurumunun kişiye ait sağlık verilerini işleyerek göndermesi hukuka uygun bir hassas veri işlemesidir.

Sır saklama yükümlülerince tıbbi teşhis, yardım, bakım hizmetlerinin ve sağlık hizmetlerinin idari olarak yürütülmesi sürecinde kişiye ait sağlık durumu verilerinin işlenmesi, her ne kadar sağlık durumuna ilişkin veriler hassas veri olsa da hukuka uygundur. Örneğin bir hastaneden başka bir hastaneye nakledilen hastaya ait sağlık verilerinin hastayı kabul eden hastane yetkilileri tarafından işlenmesi hukuka uygundur.(M.8/f.3)

Avrupa Topluluğu üyeleri, önemli kamu menfaatlerinin gerektirmesi durumunda kişisel verilerin korunmasında yeterli garantilerin sağlanmış olması şartıyla kişisel verilerin korunması için görevli denetleme biriminin kararı veya bir yasa ile hassas verileri işleme yasağını daraltabilir.(M.8/f.4)

Örneğin polisin bir toplantı ve gösteri yürüyüşünü kamera kaydına alarak veri toplama faaliyeti neticesinde kayda alınan kişilerin kendileri hakkındaki siyasi görüşün, üye oldukları sendikanın veya cinsel eğilimlerinin ortaya çıkma ve bu sebeple ayrımcılığa uğrama tehlikesi vardır. Örneğin bir siyasi partinin yaptığı mitingi izleyen kalabalığın kayıt altına alınması, bir sendikanın yaptığı yürüyüşün kayıt altına alınması veya LGBTİ bireylerin yapmış olduğu yürüyüşün kayıt altına alınması hassas verinin toplanması faaliyetidir ve kural olarak yasaktır. Burada polisin dahi bu faaliyetleri kamera kaydına alması, bu faaliyetlere katılan bireylerin kimlik bilgilerini kaydetmesi kural olarak yasaktır. Fakat eğer bir terör eyleminin yapılacağı veya bir provokasyon yapılacağı yönünde alınan istihbarat gereği gerekli güvenlik önlemlerinin alınması kamu menfaatinin gereği olduğundan polisin bu faaliyetleri, ölçülülük ilkesini gözetilmek koşuluyla hukuka uygun bir hassas veri işleme faaliyeti olarak sayılabilir. Fakat Yönerge'de de belirtildiği üzere kamu menfaati gerekçesiyle toplanan hassas verilerin korunmasında yeterli garantiler sağlanmadıkça ve polisin bu faaliyetlerinin yasal dayanağı olmadıkça veya görevli denetleme biriminin bu faaliyetlere izin veren bir kararı olmadıkça bu veri toplama faaliyetlerinin hukuka uygunluğundan bahsedilemez.

Ceza hukuku ve idare hukuku kapsamında kişiler hakkında hükmedilen mahkumiyet veya güvenlik tedbirleri kararları idari gözetim altında işlendiği takdirde bu veri işlemesi hukuka uygun olacaktır.(M.8/f.5)

Örneğin kişinin almış olduğu idari para cezalarının bir sicilde tutulması veya mahkumiyetlerinin adli sicilde tutulması hukuka uygundur.

Fakat burada tartışılması gereken mesele, bir kişi hakkında hükmedilen yaptırımın veya mahkeme kararının hassas veri sayılıp sayılmayacağıdır. Zira açıkça Yönerge'nin 8. maddesinde sınırlı olarak sayılan hassas veriler arasında mahkeme kararları ve yaptırımlar yer almamaktadır. Yukarıda bahsettiğimiz "*hassas verilere ulaştıran veriler de hassas veri sayılır*" görüşünü dikkate aldığımızda bir mahkeme kararının muhtevasında kişiye ilişkin hassas veriler bulunuyorsa bu mahkeme kararının kendisinin de hassas veri sayılacağı söylenebilir. Örneğin konusu cinsiyet değiştirme olan mahkeme kararında kişinin cinsel yaşamına veya sağlık durumuna ilişkin veriler gibi hassas verilerin bulunması olası olduğundan bu mahkeme kararının da ilgili kişinin hassas verisi olduğu söylenebilir. Bu açıdan hassas verilerin işlenmesi yasağının esas amacının ayrımcılığa uğrama tehlikesini bertaraf etmek olduğu dikkate alındığında kişiyi ayrımcılığa maruz bırakabilecek bir mahkeme kararı, güvenlik tedbiri veya yaptırım kararının da hassas veri olduğunu söylemek mümkündür.

Vatandaşlık numarası veya kişiye özgü işaretler üye devletlerin bu verileri işleme şartlarını düzenlemeleri şartıyla işlendiği takdirde bu veri işlemesi hukuka uygundur.

Avrupa Topluluğu üyesi ülkeler, Yönerge'nin verdiği yetki gereği hassas veri koruma yasağına ilişkin getirecekleri istisnaları Avrupa Komisyonu'na bildirmekle yükümlüdür(M.8/f.6).

### 2.8.6. İlgilinin haberdar edilmesi ilkesi ve ilgilinin hakları

Yönerge'ye göre eğer veriler, doğrudan veri öznesinden elde ediliyorsa ilgili kişi (veri sahibi) belirli hususlarda bilgilendirilmelidir.

Veri sorumlusu(alıcısı), veri öznesine(sahibine) ait verileri toplarken veri öznesini bilgilendirmelidir ve bu bilgilendirmenin kapsamı asgari olarak aşağıdaki hususları kapsamalıdır:

- Veri sorumlusunun veya vekilinin kimliği

- Veri işlenmesinde güdülen amaç
- Sorulan sorulara yanıt vermenin zorunlu olup olmadığı
- Verilere erişim ve verileri düzeltme hakkının varlığı

Örneğin bir anket şirketinin yaptığı anket çalışması bir tür doğrudan veri toplama ve işleme faaliyetidir. Bu çalışmada kişilere soru soranlar soru sordukları kişilere kimliklerini açıklamalı; bilgi almakta güdülen amaç hususunda, sorulara cevap vermenin zorunlu olup olmadığı hususunda ve verilere erişim ve verileri düzeltme hakkının varlığı hususunda veri öznesine bilgi vermelidir(M.10).

Eğer ilgili yasal mevzuat gereği veri sahibine ait verinin veri sahibine sorulmadan toplanması durumunda veri kaydedilmeye başlanır başlanmaz veri sahibine yukarıda belirtilen asgari bilgileri içeren bilgilendirme yapılmalıdır(M.11).

Eğer veri sahibine sorulmadan toplanan veri üçüncü kişilere aktarılacaksa en geç ilk aktarma anında yukarıdaki asgari bilgileri içeren bilgilendirmede bulunulmalıdır(M.11).

Eğer veri işlemesi, akademik veya istatistiksel amaçlarla yapılıyorsa, yasa gereği veri kaydediliyor veya aktarılıyorsa, veri sorumlusunun ilgiliyi bilgilendirmek için göstereceği zahmet ilgilinin bilgilenmekten beklediği menfaatinden daha fazla ise, ilgilinin haberdar edilmesi imkansız ise veri sorumlusunun haberdar etme yükümlülüğü yoktur(M.11/f.2).

Yönerge'nin ilgili kişilere bir takım haklar verdiği görülmektedir. Bunları şöyle belirtmek mümkündür:

Verileri işlenen kişinin bilgi edinme hakkı Yönerge'nin 12. maddesinde düzenlenmiştir. Bir kişinin hakkındaki veriler hakkında bilgi sahibi olması için öncelikle bu verilere erişebilmesi gerekir. Bu açıdan bilgi edinme hakkının kapsamına erişim hakkı da girer. Buna göre veri sahibi, hakkındaki verilere serbestçe, bir engelle karşılaşmaksızın, makul sürede, aşırı masraf yapmaksızın, uygun aralıklarla, sınırlama olmaksızın erişebilmelidir. Burada bahsedilen makul süre için objektif bir kıstas yoktur. Örneğin elektronik posta yoluyla bilgi edinmek isteyenle yazılı bildirim yoluyla bilgi edinmek isteyen için öngörülen makul sürenin aynı olması beklenemez. Yine bilgi talep

edilen kişiye verilecek bilginin toparlanma süresinin farklılığı da makul sürenin farklılaşmasına sebep olacaktır.

Bilgi edinme hakkının karşılanması için bilgi edinmek isteyen kişinin aşırı masraf yapmaması gerekir. Buradan çıkartılması gereken sonuç bilgi edinmenin ücretsiz olabileceği gibi makul bir ücretin de talep edilebilecek olduğudur.

Bilgi edinme hakkının kapsamında veri sahibinin verinin toplanma, işlenme ve transfer edilme amaçlarını bilme hakkı da vardır.

Bilgi edinme hakkının kapsamında Yönerge'ye aykırı olarak işlenmiş veya yanlış işlenmiş verinin düzeltilmesini, silinmesini isteme hakkı da vardır. Ayrıca aşırı çaba gerektirmeyecekse veya imkansız değilse bu verilerin silinmesinden ve düzeltilmesinden verilerin aktarıldığı üçüncü kişilerin haberdar edilmesini isteme hakkı da bilgi edinme hakkı kapsamındadır.

Eğer veri işlemesi otomatik yöntemlerle yapılıyorsa veri sahibinin bu otomatik işlemenin mantığı konusunda anlaşılır biçimde bilgilendirilmesi de bilgi edinme hakkı kapsamındadır.

Yönerge'de bilgi edinmenin usulü konusunda bir ayrım gözetilmediğinden bilgi verilmenin veya bilgi edinmenin bir şekli olduğu söylenemez.

Şu hususa dikkat edilmelidir: Bilgi vermek, veri işleyicileri veya veri sorumluları açısından bir yükümlülüktür. Verileri işlenenler bakımından bilgi almak ise bir haktır. Bu yükümlülük ve hak birbirinin tamamlayıcısı olup bilgi vermekle yükümlü olanlar yükümlülüğünü yerine getirdiği ölçüde veri sahipleri bilgi alma hakkını kullanabilecektir.

İlgili kişinin itiraz hakkı, Yönerge'nin 14. maddesinde düzenlenmiştir.

İlgili kişinin iki halde kişisel verinin işlenmesine itiraz hakkı vardır ve üye ülkeler bu hakkı iç hukuklarında sağlamalıdır:

Kamu menfaati veya haklı çıkarın korunması gerekçesiyle verileri işlenen ilgililer, -iç hukukta aksi açıkça öngörülmedikçe- verilerini muhafazaya değer gerekçelerle verilerinin işlenmesine itiraz edebilecektir. Eğer itiraz yerinde ise itiraza konu veriler işleme tabi tutulmayacaktır(M.14-a).

Üye devletler, kişisel verilerin üçüncü kişilerce elde edilip pazarlama (doğrudan reklam) amacıyla kullanılması durumunda ilgililerin verileri işleyicilere itiraz hakkını ulusal mevzuatlarında sağlamalıdır. Bunun amacı özellikle telefon, faks, e-posta vb. yollarla kişilik hakkına yapılan rıza dışı müdahalelere karşı kişiyi korumaktır. İlgili kişinin itirazı ile itiraza konu veriler işleme tabi tutulmayacaktır(M.14-b).

İtirazın sonuç doğurması için itiraz hakkı veri işlenmeden önce kullanılmalıdır. Dolayısıyla bu hakkın verinin işlenmesinden sonra kullanılması bu hakkın mantığına aykırıdır. Verilerin işlenmesinden sonra itiraz hakkının yerine verinin düzeltilmesini, silinmesini, işlenmesinin durdurulmasını isteme hakkı söz konusu olur.

İtiraz hakkı bir ücrete bağlı olmamalıdır.

Eğer ilgili kişinin kişisel verisi, doğrudan reklam amacıyla üçüncü kişilere transfer edilecekse ilgili kişi asgari olarak kişisel verilerinin doğrudan reklam amaçlı üçüncü kişiye transfer edildiği ve bu transfere ve kullanıma karşı ilgili kişinin herhangi bir ücret ödemeden itiraz hakkı bulunduğu hususları dahil olmak üzere aydınlatılmalıdır(M.14-b).

Verilerin düzeltilmesi ve işlenmez hale getirilmesi(bloke) de Yönerge'nin 12. maddesinde düzenlenmiştir. Veri sahibine veriye erişme (bilgi edinme) hakkı tanınmasının mantığı, veri sahibinin öğrendiği yanlışlıkları düzeltme, silme ve işlenmez hale getirme hakkını kullanması için gerekli ön koşul olan bilgiyi sağlamaktır. Zira veri sahibinden kendisiyle ilgili veri hakkında bilgi sahibi olmadan bu verileri düzeltmesi, silmesi veya işlenmez hale getirmesi haklarını kullanmasını beklemek mümkün değildir.

Veri sahibinin, Yönerge'ye aykırı olarak işlenmiş veya yanlış işlenmiş verinin düzeltilmesini, silinmesini isteme hakkı da vardır(M.12/b).

Ayrıca aşırı çaba gerektirmeyecekse veya imkansız değilse bu verilerin silinmesinden ve düzeltilmesinden, verilerin aktarıldığı üçüncü kişilerin haberdar edilmesini isteme hakkı da bilgi edinme hakkı kapsamındadır(M.12/c).

Silinme hakkının kökeninde Fransız hukuku kaynaklı geçmiş olayları unutma hakkı anlamına gelen unutulma hakkının olduğu şeklinde değerlendirme mevcuttur.[138] Unutulma hakkına göre ilgili kişi, kendisini utandıran verilerin silinmesini isteyebilir. Burada verinin doğruluğu veya yanlışlığı önemli değildir. Veri doğru olsa bile ilgili kişiyi utandırıyorsa bu bilgilerin silinmesi istenebilir. AB Adalet Divanı'nın Google-İspanya kararında bu görüşü benimsediği görülmektedir.[139]

Yönerge'nin 12. maddesine göre Yönerge, ilgili kişiye Yönerge'de öngörülen kurallara uygun olmayan şekilde işlenen kişisel verilerin silinmesini talep etme hakkı vermiştir. Dikkat edilirse Yönerge sadece eksik ve yanlış kişisel verilerin değil, Yönerge'de öngörülen kurallara aykırı olarak işlenmiş bütün kişisel verilerin silinmesi hakkını tanımıştır.

Avrupa Adalet Divanı, 2015 yılında silinmeyi talep hakkına ilişkin bir karar vermiştir:

> "*Google Spain SL and Google Inc. V Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez kararına*[140] *konu olan olayda, 1998 yılında bir İspanyol gazetesinde Mario Costeja Gonzalez'e ait bir gayrımenkulün, bu kişinin sosyal güvenlik kurumuna olan borçlarının tahsili için açık artırma ile satılacağı ilanı çıkmış, bu ilanlar gazetenin internet sitesinde de yayımlanmıştır.2009 yılı Kasım ayında, Mario Costeja Gonzalez gazeteden artık anlamını yitiren bu ilanların internet sitesinden kaldırılmasını istemiş, ancak talebi ilanların İspanyol İş ve Sosyal Güvenlik Bakanlığı'nın emri ile yayınlandığı gerekçesi ile reddedilmiştir. Bunun üzerine Mario Costeja Gonzalez, Google İspanya'dan ismi ile arama yapıldığında, internet arama sonuçları arasında bu ilanların çıkmamasını talep etmiştir. Google İspanya, bu talebi Kaliforniya'da bulunan Google Inc.'e iletmiştir. Mario Costeja Gonzalez ise İspanyol Veri Koruma Denetim Makamı'na şikayette bulunmuştur. Gazeteye yöneltilen şikayet, ilanın Bakanlık kararına dayanması nedeniyle reddedilmiş ise de, Google İspanya ve Google Inc.'e yöneltilen şikayetler kabul edilmiştir. Google İspanya ve Google Inc. bu kararı, idari yargıda temyiz etmişler, temyiz makamı da konu ile ilgili olarak Avrupa Adalet Divanı'na başvurmuştur. Adalet Divanı, internet arama motoru işletenlerin, veri*

[138]Develioğlu , 2017, **a.g.k.** , 90.
[139]ABAD. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. 13/05/2014, 131/12
[140]ABAD. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. 13/05/2014, 131/12
Google-İspanya kararı için bkz: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131_SUM&qid=1579769680599&from=EN (Erişim Tarihi:23.01.2020)

*sorumlusu niteliğinde olduğuna ve ilgili kişilerin bir internet sitesinde yer alan yer alan kişisel veriler kaldırılmasa dahi, internet arama motorunda bu internet sitesine yönelik arama sonucunun silinmesini isteme haklarının olduğuna karar vermiştir. Mahkeme, ayrıca, bu talepte bulunmak için ilgili kişinin olumsuz sonuçlara maruz kaldığını ispat etmesi gerekmediğini de kabul etmiştir*."[141]

Verinin silinmesi halinde veri, veri sorumlusunun hakimiyeti alanından çıkar. Verinin silinmesi işlemi, elden işlenen verilerde veri evrağının imha edilmesi ile gerçekleşir. Otomatik yolla işlenen verilerin silinmesi işlemi ise veri depolayıcısının(taşıyıcısının) imhası veya bu veri depolayıcısından veri sahibi ile ilgili verilerin silinmesi yoluyla gerçekleşir.[142] Veri depolayıcısına(taşıyıcısına) örnek olarak hard-disk, Dvd, Cd veya disket vs. örnek gösterilebilir.

Verinin işlenmez hale getirilmesi durumunda veri, veri sorumlusunun hakimiyetinden çıkmaz; fakat veri sorumlusu verinin işlenmesine de engel olur.

### 2.8.7. İstisnalar, sınırlamalar ve kişi hakkında otomatik surette verilen kararlar

Avrupa Topluluğu üye devletleri,

- verinin kalitesine ilişkin ilkeler(M.6/f.1),
- verilerin oluşturulmasında bilgilendirme yükümü(M.10,11/f.1),
- bilgi edinme hakkı(M.12),
- işlem aleniyeti(M.21),

ile ilgili hükümlerle sınırlı olmak üzere kişisel verilerin korunmasına ilişkin önlemlerde sınırlama yapabilir. Diğer bir deyişle bu hükümlerin öngördüğü koruma azaltılabilir. Fakat bu korumanın daraltılması için bazı zorunlu hallerin gerçekleşmesi gerekir. Bu zorunlu haller;

- devlet güvenliği ve ülke savunması,
- kamu güvenliği,
- Suçun önlenmesi, soruşturulması, tespiti ve kovuşturulması,
- AB veya AB üyesi devletin önemli ekonomik çıkarlarının korunması

[141]Develioğlu , 2017 , **a.g.k.** , 89.
[142]Başalp, 2004 , **a.g.k.** , 50.

- Kamu güvenliği; suçun önlenmesi, soruşturulması, tespiti ve kovuşturulması; AB veya AB üyesi devletin önemli ekonomik çıkarlarının korunması hallerinden biriyle bağlantılı şekilde geçici veya sürekli olarak kamu gücünün kullanılmasını gerektirecek hallerin varlığı
- İlgilinin ve üçüncü kişinin hak ve özgürlüklerini korunması
- Bilimsel araştırma yapmak ve istatistiksel veri elde etmek

olarak sayılabilir(M.13).

Kural olarak mesleki performans, güvenilirlik, kredibilite gibi hususlardaki otomatik usulle oluşturulmuş kişisel verilerin otomatik surette değerlendirilmesi sonucu insani bir değerlendirme yapılmadan verilen kararlar bağlayıcı değildir. Örneğin bir iş başvurusu veya kredi başvurusu, yapılan psikolojik testin otomatik olarak değerlendirmesi sonucu reddedilirse bu ret kararı bağlayıcı değildir(M. 15/1).[143]

Bu kuralın istisnaları vardır:

- Bir sözleşme ilişkisinden dolayı otomatik surette elde edilen kararlar bağlayıcıdır. Buradaki sözleşme ilişkisi, sözleşmeye hazırlık işlemleri de dahil olmak üzere sözleşme ilişkisinin kurulmasından sona ermesine kadarki süreyi kapsar. Fakat aynı zamanda ya sözleşmenin kurulması veya ifası talep edilmiş olmalı veya ilgilinin haklı çıkarlarının korunması uygun önlemlerle garanti edilmiş olmalıdır(M.15/2).
- Yasa tarafından yetki verilmesi durumunda otomatik surette verilen karar ilgilinin haklı çıkarlarının korunması kaydıyla bağlayıcı değildir(M.15/2).

### 2.8.8. Kişisel verilerin işlenmesinde usule dair ilkeler

*Yönerge*'nin 16. maddesine göre aslolan veri işleme işleminin gizliliğidir.

> MADDE 16-Kişisel verilere erişme hakkı olan işleyicinin kendisi dahil olmak üzere, işleyicinin veya denetleyicinin yetkisi altındaki herhangi bir kişi, bunu yapması kanun tarafından istenmezse denetleyicinin talimatı haricinde verileri işlememelidir.

Kanun tarafından istenmesi haline örnek olarak ceza kovuşturması nedeniyle bilgi verilmesi durumu örnek olarak verilebilir.[144]

[143]Başalp , 2004 , **a.g.k.** , 54.
[144]Uygun , 2010 , **a.g.k.** , 71.

> MADDE 17(1)- Üye Devletler, özellikle işlemenin bir ağ üzerinde verilerin iletilmesini gerektirdiğinde ve işlemenin tüm diğer yasa dışı biçimlerine karşı, yetkisiz açıklama veya erişim, değiştirme, kazara kayıp veya kazara veya yasa dışı tahribe karşı kişisel verileri korumak için gereken uygun teknik ve kurumsal tedbirleri, denetleyicinin uygulamasını sağlayacaklardır. Bu tür tedbirler, uygulamalarının durum ve maliyetini dikkate alarak, korunacak verinin yapısına ve işleme tarafından sunulan risklere uygun seviyede güvenlik sağlayacaktır.

Yönerge'nin 17. maddesinde öngörülen önlemlere örnek olarak veri dosyalarının şifrelenmesi hackerlara karşı güvenlik sisteminin kurulması gösterilebilir.[145] Örneğin bir banka, müşterilerine ait bilgileri koruyucu önlemleri almalı, gerektiğinde teknolojik imkanlardan yararlanmalıdır.

Eğer veri sorumlusu, veri işleme işini bir gerçek veya tüzel kişiye gördürürse iş görme yoluyla verileri işleyen, Yönerge'nin 17. maddesinin öngördüğü güvenlik önlemlerini almalıdır. Bu durumlarda şu hususlara dikkat edilmelidir:

- Veri sorumlusu, iş görme yoluyla verileri işleyecek olan kişiyi bir hukuki işlemle yetkilendirmelidir.
- İş görme yoluyla veri işleyecekler veri sorumlusunun talimatına uymalıdırlar.
- İş görme yoluyla veri işleyecekler, ikamet ettikleri yerlerin mevzuatı çerçevesinde Yönerge'nin 17. maddesinin öngördüğü tedbirleri almalıdır.
- Veri sorumlusu, kendisi adına veri işleyeceklerin işlem güvenliğini sağlayacaklarını bir hukuki antlaşma garanti etmelidir.
- Veri sorumlusu adına veri işleyecekler veri sorumlusunun yükümlülüklerine tabidir.

Yönerge'nin 28. maddesi, AB üyesi devletlerde muadil veri muhafaza seviyesini ve bireylerin kişilik haklarının muhafazasını temin etmek amacıyla Yönerge'de düzenlenen hükümlerin tatbikini takip edecek bağımsız bir denetleyici otoritenin(organın) kurulmasını öngörmüştür. Veri sorumlusu veya temsilcisi, kişisel verilerin işlenmesinden önce Yönerge'nin 28. maddesinin öngördüğü bu kontrol birimine(denetim makamı) bildirimde bulunmalıdır(M.18).

[145]Başalp , 2004 , **a.g.k.** , 56.

Eğer veri işleme kısmen veya tamamen otomatik yolla yapılıyorsa bildirim zorunlu iken otomatik olmayan yolla yapılan veri işlemede bildirim zorunlu değildir.

Kontrol birimine bildirilmesi zorunlu olan bilgiler asgari olarak aşağıdakileri kapsamalıdır:

- Veri sorumlusunun veya temsilcisinin adı ve soyadı
- Verinin işlenme amacı
- Verilerin kategorileri
- Üçüncü ülkelere planlanan veri transferleri
- İşlemlerin güvenliği için alınan tedbirler
- Veri alıcıları ve veri alıcılarının kategorileri

Bilgilerdeki değişiklikler de kontrol birimine bildirilmelidir. Bildirim şekli hususunda takdir yetkisi üye devletlere aittir(M.19).

Bildirim yükümlülüğünden muafiyet sebeplerini şöyle sıralamak mümkündür:

İşlenmesinin ilgili kişinin kişilik hakkına zarar vermeyeceği aleni olan işlemlerin kontrol birimine bildirilmesi zorunlu değildir(M.18). Örneğin elektrik, su gibi tüketim verilerinin işlenmesi, bankaların müşterilerinin hesap bilgilerinin işlemesi buna örnek verilebilir.[146]

Veri sorumlusunun veri koruması görevlisi ataması durumunda bildirim yükümlülüğü ortadan kalkar. Fakat bu yükümlülüğün kalkması için veri koruması görevlisinin veri korumaya yönelik ulusal mevzuatı şirket içinde bağımsız şekilde tatbik edebilmesi gerekir(M.18).

Tapu sicili, gemi sicili, ticaret sicili gibi kamuya açık siciller üzerindeki veri işlemlerinin kontrol birimine bildirilmesine gerek yoktur.

Kar amacı gütmeyen organizasyonların kişisel verinin işlenmesinden kontrol birimini haberdar etme yükümlülüğünden muaf olması için veri işlemenin organizasyonun faaliyet amacı ile aynı kapsamda yürütülmesi gerekir.

[146]Başalp , 2004 , **a.g.k.** , 59.

Nitekim yukarıda da bahsedildiği üzere kamuya yararlı kuruluşların hassas veri işleme yasağına tabi olmaması ile bildirim yükümlülüğüne tabi olmamaları birbiriyle örtüşen durumlardır.

Otomatik olmayan işlemler bildirim yükümlülüğünden muaf tutulabilecektir (M.18/f.5).

### 2.8.9.Ön kontrol(ön denetim) ve işlem aleniyeti

Yönerge'nin ifadesi ile 'spesifik risk taşıyan işlemler' olarak adlandırılan işlemler, üye devletlerce ön denetime tabi tutulmalıdır(M.20). Fakat Yönerge'de spesifik risk taşıyan işlemlerin neler olduğu sayılmamıştır. İç hukuklarında spesifik risk taşıyan işlemleri tanımlama yetkisi üye devletlere verilmiştir. Burada üye devletlerden beklenen, Yönerge'nin öngördüğü hassasiyetlere dikkat etmektir. Örneğin Yönerge'nin 8. maddesinde düzenlediği hassas verilerin işlenmesinin spesifik risk taşıyan işlemler kategorisinde görülmesi gerekir.

Yönerge'ye göre ön kontrol, kontrol birimi veya veri koruması görevlisi tarafından yerine getirilmelidir. Fakat veri koruma görevlisinden beklenen, kontrol birimi ile işbirliği içinde çalışması ve kontrol birimini danışma organı olarak görmesidir.

Kontrol biriminin iki fonksiyonu vardır. Birincisi işleme izin vermek, ikincisi yapılan işlemin spesifik risk taşıyıp taşımadığı hususunda görüş bildirmektir.

Bildirim yükümlülüğüne tabi işlemlerde üye devletler, işlemlerin aleniyet kazanması için gerekli önlemleri almalıdır. Bu önlemlerin alınmasında kontrol birimine Yönerge'nin 18. maddesi gereği bildirim zorunluluğuna tabi işlemlerin sicilini tutma görevi verilmiştir. Kontrol Birimi, Yönerge'nin 19/f.1/b.a-e maddesinde düzenlenen bilgilere sicilinde yer vermelidir. Bu sicil kamuya açık bir sicil olmalıdır(M.21).

Bildirim yükümlülüğüne tabi olmayan işlemlerde bilgi talep eden kişiye en azından Yönerge'nin 19 19/f.1/b.a-e maddesinde öngörülen bilgiler temin edilmelidir. Örneğin tapu sicili üzerindeki işlemler bildirim yükümlülüğüne tabi değildir. Ama bilgi talep eden her ilgiliye bu sicilden istediği bilgiler verilebilir[147](M.21).

[147]TMK MADDE 1020- 1.Tapu sicili herkese açıktır.

### 2.8.10.Yargı yolu, sorumluluk ve yürürlüğe koyma yükümlülüğü

Yönerge'nin esas amacı, kişisel verilerin işlenmesi sırasında kişilik hakkının ihlalinin önlenmesidir. Bu sebeple Yönerge, kişilik hakkı zarar görenlere veri kontrol birimine hak ihlalinin giderilmesi için başvurma hakkı vermiştir. Aynı zamanda kişilik hakkı zarar gören kişi, dava yoluyla da hak ihlalinin giderilmesini talep edebilir. Fakat dava yoluyla hak ihlalinin giderilmesinin ön şartı, ihlal edildiğini iddia ettiği hakkının ilgili ülkenin iç hukukunda garanti altına alınan bir hak olmasıdır(M.22).

Yönerge'nin 23/1 maddesine göre üye devletler, bu Yönerge uyarınca kabul edilen ulusal hükümlerle uyumsuz herhangi bir işlemenin veya yasadışı bir işleme faaliyetinin sonucu olarak zarara uğrayan herhangi bir kişinin uğradığı zarar için denetleyiciden tazminat almaya hak kazanmasını sağlayacaktır. Fakat denetleyici, zarara yol açan olayda sorumlu olmadığını kanıtlarsa kısmen ya da tamamen bu yükümlülükten muaf tutulabilir.

Görüldüğü üzere, ispat yükü hak ihlaline uğrayan kişilerde değil; veri sorumlusundadır. Aynı zamanda Yönerge, üye devletlerin veri sorumlusunu tamamen veya kısmen sorumluluktan kurtaran hükümleri iç hukukunun parçası haline getirmesine izin vermiştir.

Tazminat yükümlülüğünün doğması için gereken şartlar şunlardır:

- Kişisel veri koruması hukukuna aykırı bir veri işlemesi olmalıdır.
- Kişisel verilerin işlenmesinden dolayı zarar ortaya çıkmalıdır.
- Zarar ile hukuka aykırı işlem arasında illiyet bağı olmalıdır.

Yönerge, tazminat yükümlülüğünün doğması için kusur şartını aramamıştır. Buradan çıkartılacak sonuç, Yönerge'nin kusur şartını arayıp aramamakta üye devletleri serbest bıraktığıdır.[148]

Yönerge'nin 24. maddesine göre üye devletler Yönerge'nin iç hukuka uygulanması için gerekli önlemleri almakla yükümlüdür. Özellikle iç hukukta gerekli

---

2.İlgisini inanılır kılan herkes, tapu kütüğündeki ilgili sayfanın ve belgelerin tapu memuru önünde kendisine gösterilmesini veya bunların örneklerinin verilmesini isteyebilir.
3.Kimse tapu sicilindeki bir kaydı bilmediğini ileri süremez.

[148]Başalp , 2004 , **a.g.k.** , 66.

yasal mevzuatın oluşturulması için gereğini yapmakla yükümlüdür. Aynı zamanda Yönerge'ye aykırılığın yaptırımına ilişkin düzenlemeleri de yapmakla yükümlüdür.

### 2.8.11.Üçüncü ülkelere veri transferi ve davranış kuralları

Yönerge'nin 25. maddesine göre AB üyesi ülkelerin AB üyesi olmayan ülkelere kişisel veri transferi yapabilmesinin ön şartı AB'ye üyeliği olmayan ülkenin veri koruma mevzuatının Yönerge'nin aradığı yeterli koruma düzeyine sahip olmasıdır. Diğer bir deyişle AB üyesi olmayan ülkelere veri transferi için bu ülkelerin güvenli ülke olmaları gerekmektedir.[149]

Öyle ki Yönerge'nin yeterli koruma koşullarını sağlamayan ülkelere veri transferini yasaklayan düzenlemesi; Avrupa Birliği dışındaki pek çok ülkeyi benzer muhtevadaki düzenlemeleri kabul etmeye zorlamıştır.[150]

Yönerge'nin yeterlilik için aradığı ön koşul, transfer yapılacak ülkenin kişisel verilerin korunması mevzuatının AB standartlarına uygun olmasına bağlı olmasıdır.[151]

Üçüncü ülkenin veri koruma mevzuatının yeterli koruma mevzuatına sahip olup olmadığını tespit ederken temel hak ve hürriyetlerin korunması ile kişinin özel hayatının korunmasındaki seviye, transfer edilen verinin niteliği, amaca bağlılık, ilgililerin bilgi edinme hakkının olup olmadığı, denetleyici organların varlığı, hukuka aykırı işlemeden sorumluluk ve yaptırımlar gibi hususlar dikkate alınacaktır.[152]

Yeterlilik kavramını açıklamak üzere AB Veri Koruması Grubu, 26 Haziran 1997 tarihinde Üçüncü Ülkelere Kişisel Verilerin Transferinde Temel Prensipler adı altında bir karar yayınlamıştır.[153] Bu prensipler, üye devletlere üçüncü ülkelere veri transferinde yol gösterici olmuştur. Bu karara göre transfer edilecek veriler konularına göre ayrılmalı ve yeterli koruma sağlayan ülkeler beyaz listeye alınmalıdır. Beyaz

---

[149]E. Ağıralan(2015). *Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Mahremiyet Etki Değerlendirmesi*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü. 14. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

[150]Ş. İ. Aşıkoğlu(2018). *Avrupa Birliği Ve Türk Hukukunda Kişisel Verilerin Korunması Ve Büyük Veri*. Yüksek Lisans Tezi. İstanbul : İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü. 56. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

[151]A. Boz(2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü. 66. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

[152]Başalp , 2004 , **a.g.k.** , 68.

[153]https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/1997/wp4_en.pdf (Erişim Tarihi:27.04.2019)

listede yer almayan ülkelere veri transferinde ise yeterli koruma düzeyinin varlığı araştırılmalıdır. Ayrıca bu karara göre Sözleşme'nin tarafı olan ülkeler, yeterli bir koruma mekanizması oluşturmuşlarsa yeterli koruma düzeyini taşıdıkları varsayılmaktadır.

Yönerge'nin üçüncü ülkelere veri transferinde bu kadar hassas olmasının en önemli sebebi bireylere güven vermek istemesidir. Zira bireyler, verilerinin yurtdışına taşınması halinde yabancı ülkelerin bu verileri koruma düzeyi konusunda şüpheye düşerek verileri yurtdışına taşımak istemeyebilirler.[154] Ekonomik gelişimin ve serbest piyasanın gelişimi önündeki en büyük engellerden birinin serbest veri akışını engellemek olduğu dikkate alındığında AB'nin bu konudaki kaygısını anlamak mümkündür. AB, üye devlet vatandaşlarına kişisel verilerinin korunması konusunda gerekli güvenceleri vererek ekonomik gelişmenin AB sınırları içinde kalmasına engel olmak istemiştir.

Yönerge'ye göre üçüncü ülkenin veri koruması düzeyinin uygunluğuna karar verme yetkisi Avrupa Komisyonu'ndadır. Hem Avrupa Komisyonu hem de veri transfer edecek üye devlet uygunluk araştırması yapmakla yükümlüdür. Uygun düzeyin olmadığına kanaat getirilirse Avrupa Komisyonu ve veri transfer edecek üye ülke birbirini bilgilendirmelidir. Komisyon, her somut olayla ilgili olarak kendisine bildirim yapıldığında veya kendiliğinden üçüncü ülkenin veri koruma düzeyinin uygunluğu hakkında karar verebilir. Komisyonun bu kararı bağlayıcıdır(M.25).

Avrupa Komisyonu, vereceği karardan önce veri koruması grubunun görüşünü almalıdır. Veri koruması grubunun görüş bildirme yükümlülüğü vardır. Veri koruma grubu danışma organı niteliği taşıyan bağımsız bir statüye sahiptir(M.29,30).

Avrupa Komisyonu'nun karar verme süreci şöyle işler: Öncelikle Yönerge'nin 31. maddesi uyarınca oluşturulan alt komisyon bir ön karar verir. Avrupa Komisyonu, alt komisyonun bu kararına katılırsa üçüncü ülkenin uygun koruma sağladığına dair bağlayıcı bir karar verir.

[154]G. H. Erdinç(2017). *Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Teknik Üniversitesi, Bilişim Enstitüsü. 33.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:25.02.2020)

Kararları bağlayıcı olan Avrupa Komisyonu'nun olumsuz kararından sonra her üye devletten beklenen, veri koruması açısından uygunsuzluğuna karar verilen üçüncü ülke ile veri transferini sonlandırmasıdır.[155]

Yönerge, aşağıda sayılan hallerde Yönerge'nin 25. maddesinin aradığı uygun muhafaza seviyesine sahip olmayan üçüncü devletlere kişisel veri transferine izin vermiştir(M.26). Şöyle ki;

- Veri öznesi(sahibi), kişisel verisinin transferine tereddüde yer vermeyecek surette şekle tabi olmayan rıza beyanı ile rıza vermişse transfer mümkündür.
- Veri öznesi ile transfer eden veri sorumluları arasında bir sözleşmenin ifası için veri transferi gerekli ise transfer mümkündür.
- Veri öznesinin talebiyle sözleşme öncesi ilişkinin yürütülmesi için veri transferi gerekli ise transfer mümkündür.
- Veri sorumlusu ile üçüncü kişi arasında verileri transfer edilecek kişinin yararına yapılmış sözleşmelerin ifası için gerekliyse transfer mümkündür.
- Transferin kamusal menfaatlerin korunması için gerekli olması durumunda transfer mümkündür. Örneğin uluslararası alanda uyuşturucu ile mücadele edilmesi amacıyla yapılan veri transferinde üçüncü ülkenin yeterli koruma düzeyine sahip olması aranmaz.
- Transferin mahkeme önünde taleplerin dinlenmesi için gerekli olması durumunda transfer mümkündür.
- Transfer yasa gereği zorunlu ise transfer mümkündür. Üye ülke iç hukukunda veri transferini zorunlu hale getirdiyse bu durumda veri transferi mümkündür.
- Transfer hayati önemdeki menfaatlerin korunması için gerekli ise transfer mümkündür. Örneğin ilgilinin rızasının fiilen alınması mümkün olmasa da acil tıbbi müdahale için gerekliyse veri, transfer yasağına tabi olmayacaktır.
- Transferin ilgisini ispat eden herkese açık olan kamu sicillerinden yapılması durumunda veri transferi mümkündür.

[155]Başalp , 2004 , **a.g.k.** , 71.

- Veri sorumlusunun ilgililerin mahremiyeti ve temel hak ve özgürlüklerinin yeterli düzeyde korunacağı hususunda garanti göstermesi ve üye devletin transfere onay vermesi durumunda transfer mümkündür. Üye devlet, transfere onay verdiğini diğer üye devletlere ve Avrupa Komisyonuna bildirmelidir. Bir üye devlet veya Avrupa Komisyonu, transfere itiraz ederse transfere onay veren üye devlet Yönerge'nin 31/1 maddesi uyarınca gerekli tedbirleri almalıdır.

Veri sorumlusu, ilgililerin mahremiyetiyle temel hak ve özgürlüklerinin yeterli düzeyde korunacağı garantisini bir sözleşme ile verebilir(M.26/f.2).

Sözleşmeyle veri transferinde yeterli düzeyde garanti verilmesi durumuna şu örnek verilebilir:

1988 yılında Fiat şirketinin Fransa'daki Fransız alt şirketi, kendi yönetim kadrosunun kişisel verilerini İtalya'da bulunan Fiat'ın merkezine aktarmak için Fransa ulusal veri koruma otoritesinden(CNIL) izin istemiştir. Bu transferin amacı, verileri o dönemde Fiat şirketinin İtalya'da bulunan merkezinde oluşturulan insan kaynakları veri havuzuna (İnternational Human Resources Information System) yönetim kadrosuna ilişkin bilgileri dahil etmekti. Ancak CNIL İtalya'da henüz yeterli bir muhafaza seviyesi oluşturulmadığı için transfere müsaade etmemiştir. Bu nedenle Fiat ile Fransız alt şirket arasında Fransız veri koruması ilkelerini içeren bir sözleşme kurulmuştur, imzalanan sözleşme üzerine CNIL veri transferine izin vermiştir ve verileri transfer edilen kişiler bilgi edinme ve düzeltme haklarından yararlanmışlardır.[156]

Yönerge'nin 27. maddesine göre üye devletler, veri korumasının uygulanabilirliğini artırmak amacıyla meslek birliklerini farklı meslek gruplarına yönelik farklı davranış kurallarını belirleyemeye teşvik etmelidir. Üye devletler, bu davranış kurallarının kontrol birimlerine sunulması için gerekli önlemleri almalıdır.

### 2.8.12.Veri koruması denetim organları ve iç hukuka aktarma

Yönerge'nin 28. maddesi üye devletlere bağımsız kontrol birimleri kurma görevi vermiştir. Yönerge'nin 28. maddesinden anlaşıldığı kadarıyla bu birimlerin oluşturulmasıyla Yönerge, üye devletler arasında eşdeğer bir koruma düzeyi sağlamayı ve kişilik haklarının tam anlamıyla korumayı amaçlamaktadır.

[156]Başalp , 2004 , **a.g.k.** , 74.

Yönerge'nin 28. maddesine göre kontrol birimi;

- Görevinin ifası için gerekli bilgileri toplama,
- Kişisel verilerin işlenmesinden önce verilerin bloke edilmesini, silinmesini ve yok edilmesini isteme,
- Veri koruması mevzuatı ihlallerini şikayet etme ve bu ihlaller sebebiyle dava açma,
- İlgilinin talebi üzerine kişisel verilerin hukuka uygun işlenip işlenmediğini denetleme,

yetkilerine sahiptir.

Üye devletler, kişisel verilerin korunmasına ilişkin mevzuatın oluşturulması sürecinde kontrol biriminin görüşüne başvurulması için gerekli önlemleri almalı, kontrol biriminin danışma organı özelliğine iç hukukta yer vermelidir(M.28/2).

Yönerge'nin 28. maddesine göre kontrol birimi, faaliyetleri hakkında dönemsel olarak rapor hazırlamalı ve bu raporları kamuya açıklamalıdır(M.28/5).

Üye devletlerin içindeki farklı kontrol birimleri kendileri arasında yardımlaşma yükümlülüğü altında olduğu gibi farklı üye ülkelerin kontrol birimleri de kendi aralarında yardımlaşma yükümlülüğü altındadır(M.28/6).

Denetim makamı mensupları, görevleri bitse bile vakıf oldukları bilgilerin gizliliğini sağlamak zorundadır. Üye devletler bu zorunluluğu sağlamalıdır(M.28/7).

Veri koruması grubu, Yönerge'nin 29. maddesi uyarınca kurulmuş, danışma özelliğine haiz, karar ve eylemlerinde bağımsız olan bir kurumdur. Veri koruma grubu kararlarını oy çokluğu ile almaktadır.

Çalışma Grubu, başkanını kendi içinden seçer. Başkan, iki yıllık görev süresini tamamladıktan sonra tekrar seçilebilecektir(M.29).

Veri Koruma Grubunun görevleri şöyle sayılabilir:

- Veri koruma grubunun Yönerge'nin Avrupa Topluluğunda yeknesak uygulanmasını sağlama görevi vardır. Bu görevini yapma kapsamında Yönerge'nin iç hukuka aktarılmasında ortaya çıkan sorunları inceler ve yaptığı

inceleme sonunda Avrupa Komisyonu'na görüş bildirir.[157] Aynı zamanda yine Yönerge'nin yeknesak uygulanması için veri koruması kontrol birimleri ile işbirliği sağlar.

- Veri koruma grubu bir danışma organı olması sebebiyle veri işlemesine ve hususi alanın muhafazasını sağlayabilecek topluluk tedbirlerinde Avrupa Komisyonu'na görüş bildirir(M.30/2).
- Avrupa Topluluğu'ndaki ve üçüncü ülkelerdeki veri koruma düzeyi konusunda Avrupa Komisyonu'na görüş bildirir(M.30/1-b).
- Avrupa Topluluğu seviyesinde hazırlanan davranış kuralları hakkında bilgi verir(M.30/1-d).
- Takdir yetkisi kendisinde olmak üzere kişisel verilerin işlenmesine dair kişilerin korunmasına ilişkin tüm konularda tavsiyelerde bulunabilir(M.30/3).

Veri koruma grubu danışma organı niteliğindedir. Bu sebeple verdiği kararlar üye devletleri ve Avrupa Topluluğu organlarını bağlamaz. Dolayısıyla Veri koruma grubunun görüşlerini Avrupa Topluluğu'nda icra etmeye yetkili organ Avrupa Komisyonudur. Veri koruma grubu, tavsiye ve görüşlerinin Avrupa Komisyonu'na bildirmelidir(M.30/4). Avrupa komisyonu, kendisine bildirilen görüşleri nasıl icra ettiğini veri koruma grubuna bildirmelidir(M.30/5).

Veri koruma grubu, Avrupa Topluluğu'nun veri koruma düzeyi, Yönerge'nin üye devletlerce iç hukuka aktarılması ile üye devletlerde ve üçüncü ülkelerde veri koruma düzeyinin güncel durumu ile ilgili bilgiler içeren yıllık bir faaliyet raporu hazırlamakla görevlidir(M.30/6).[158]

Yönerge'nin 32. maddesine göre Avrupa Topluluğu'na üye devletler, veri koruma yönergesine uyum sağlamak için gerekli düzenlemeleri Yönerge'nin yayımlanmasından itibaren üç yıl içinde yapmalıdır.

### 2.9.97/66 sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi ve 2002/58 Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi

[157]Başalp , 2004 , **a.g.k.** , 82.
[158] M.B. Kaya ve F. G. Taştan (2019). *Kişisel Veri Koruma Hukuku*. İstanbul: Oniki Levha Yayınları., 550. ; https://www.mbkaya.com/hukuk/veri-koruma-hukuku.pdf (Erişim Tarihi:11.04.2020)

1997 tarihli ve 97/66 sayılı Avrupa Konseyi ve Avrupa Parlamentosu Direktifi[159], Veri Koruma Yönergesi'nin ilkelerini iletişim alanında tamamlamak[160]; Yönerge'nin elektronik haberleşme yönündeki noksanlıklarını tamamlamak ve ortaya çıkan boşluğu doldurmak[161] için yürürlüğe sokulmuştur.

Telekomünikasyon alanının kendine özgü mahiyeti Yönerge'yi tamamlayıcı olan Direktif'in hazırlanmasına sebep olmuştur.[162]

Direktif'in iç hukuka aktarılması için üye devletlere tanınan, 24 Ekim 1998'e kadar belirlenen ve daha sonra 24 Ekim 2000'e kadar uzatılan süre dolmuştur. Zaten Direktif, 2002/58 Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi'nin[163] 19. maddesi gereği 30 Ekim 2003 tarihinde yürürlükten kalkmıştır.

2002 yılında, Avrupa Konseyi ve Avrupa Parlamentosu, Veri Koruma Yönergesi'nin elektronik iletişim alanında tamamlayıcısı niteliğinde olan "2002/58 sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi"ni (*EİVKY*) yürürlüğe koymuştur.[164]

*EİVKY*'nin yürürlüğe girmesiyle Direktif yürürlükten kalkmıştır.[165]

*EİVKY*'nin 2. maddesine göre elektronik posta; elektronik iletişim ağı üzerinden iletilen, internet veya bilgisayarda kayıt altına alınabilen yazı, resim, ses, dil gibi iletilerdir.

*EİVKY,* Yönerge'den farklı şekilde münhasıran gerçek kişileri kapsamamaktadır, aynı zaman da tüzel kişileri de kapsamaktadır.[166]

---

[159]Çalışmanın bu başlığı altında 97/66 sayılı Direktif'ten kısaca "Direktif" olarak bahsedilecektir.
[160]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31997L0066&from=EN (Erişim Tarihi:05.05.2019)
TKVKY, 2002/58 sayılı 2002/58 sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi'nin 19. maddesi ile 31.10.2003 tarihi itibariyle yürürlükten kalkmıştır.
**Madde 19-**97/66 sayılı Yönerge, bu Yönerge'nin 17. maddesinde atıf yapılan tarihten itibaren yürürlükten kalkmıştır. Yürürlükten kaldırılan Yönerge'ye yapılan atıflar bu Yönerge'ye yapılmış sayılır.
[161]Uyarer , 2019 , **a.g.k.** , 60.
[162]Küzeci , 2010 , **a.g.k.** , 202.
[163]Çalışmanın bu başlığı altında 2002/58 sayılı Direktif'ten kısaca "*EİVKY*" olarak bahsedilecektir
[164]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=DE (Erişim Tarihi:10.07.2019)
[165]Ayözger , 2016 , **a.g.k.** , 86.

Elektronik posta bir iletişim aracı olduğu gibi bir reklam aracı olarak da kullanılmaktadır. Bireyler, e-posta adreslerini girdikleri her internet sitelerine izlerini bırakmaktadırlar. Bu izler toplandığından giriş yapılan sitelerin bireylerin ilgi ve alışkanlıkları konusunda bir fikir verdiğini söylemek mümkündür. Esasında bunlar da kişisel veri kategorisindedir. Kişi çeşitli sebeplerle girmek istediği bir siteye giriş yapmak için e posta adresini kullandığında reklamcılık sektörünün bu mecburiyetten yararlandığı görülmektedir. Örneğin hukuk kitapları satan bir internet sitesine elektronik posta adresini kullanarak üye olduğumuzda e posta adresimize başka reklamların geldiği sık görülen bir durumdur. Bu bir kişisel verilerin korunması hakkı ihlalidir; çünkü bireyin bu reklam e-postalarıyla rahatsız edilmeme hakkı vardır. Diğer yandan bireyin internette girdiği sitelerin kendisi hakkında bir algı oluşturmasını istememe hakkı da vardır. Aynı zamanda bu e-postaların kötüniyetli kişilerin eline geçme ihtimali tehlikeyi gözler önüne sermektedir.

*EİVKY* uyarınca reklam sahibini izah etmeyen, anlaşılır tarzda ortaya koymayan, mesaj alıcısı olmama isteğini bildirme imkanı sunmayan iletiler gönderilemez.(M.13/f.4)

*EİVKY*'ye göre kural olarak telefon, faks veya elektronik posta gibi yollarla reklam iletisi almak istediğini beyan etmemiş alıcılara reklam iletisi gönderilemez(M.13/f.1).

*EİVKY*'ye göre kural olarak alışverişin gereği olarak müşterilerinin e-postalarını alanlar, müşterilerine bütün ürünleri ile bağlantılı olarak reklam amaçlı iletiler gönderebilir. Fakat bunun için satıcılar, müşterilerini elektronik posta adreslerini alırken reklam gönderecekleri konusunda aydınlatmalı veya müşterilere gönderdiği reklam iletilerinde bir daha reklam iletisi gönderilmesini istememe imkanı sunmalıdır(M.13/f.2).

Bazı internet sitelerine girildiğinde web sayfası sunucuları, kullanıcının bilgisayarının işlemcisine teknik olarak 'cookie' diye tabir edilen küçük veri toplulukları yerleştirerek kullanıcının alışkanlıklarına göre bir web sayfası oluşmasını sağlar. Bu durum kullanıcıya bir konfor sağlasa da kullanıcının alışkanlıklarının kişisel

[166]Şimşek, 2008, **a.g.k**., 58. ; H. Özdemir(2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Ankara: Seçkin Yayıncılık. 37.

veri olarak değerlendirilerek bir kişisel profil oluşmasını sağlaması ihtimali göz ardı edilmemelidir. Ayrıca cookielerin web sayfası sunucularının yardımı ile kullanıcının bilgisayar işlemcisi üzerindeki bir dosyaya erişimleri de söz konusudur.[167]

*EİVKY*'ye göre cookielerin hukuka uygun kullanımından bahsedebilmek için cookielerin bilgisayarının işletim sistemine yerleştirilmeden önce kullanıcının web sayfası sunucuları tarafından kullanım amaçları ile ilgili aydınlatılması gerekmektedir(M.6/f.3). Ayrıca kullanıcı cookilerin erişimini engelleme imkanına sahip olmalıdır.

### 2.10.OECD Küresel Ağlarda Mahremiyetin Korunması Konusunda Bakanlık Bildirgesi

Küresel Ağlarda Mahremiyetin Korunması Bildirgesi[168], 7-9 Ekim 1998 tarihlerinde Ottawa'da düzenlenen OECD Bakanlar Konferansında kabul edilmiştir.

Bu bildirgede OECD üyesi devlet bakanlarının; kişisel verilerin sınır ötesi akışında gereksiz kısıtlamaların kaldırılması gerektiği, küresel ağlarda mahremiyetin korunacağına dair güvenin artırılması gerektiği, küresel ağlarda mahremiyetin korunması sürecinde hükümetler ile iş dünyasının işbirliği içinde olması gerektiği, 1980 tarihli "OECD Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"in kişisel verilerin korunmasında uluslararası bir rehber teşkil etmeye devam edeceği konusunda fikir birliği içinde oldukları görülmektedir.

### 2.11. 99/5 Sayılı Avrupa Konseyi Bakanlar Komitesi İnternet Ortamında Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı

1999 tarihli ve 99/5 sayılı Avrupa Konseyi Bakanlar Komitesi tavsiye kararında[169] kişisel veri alışverişinde önemli yeri olan internet ortamında kişilerin özel hayatının korunması için üye devletlere tavsiyelerde bulunulmuştur. 99/5 sayılı tavsiye kararı önsöz ve tavsiye ekleri olarak ikiye ayrılmaktadır. Tavsiye ekleri kısmı ise; giriş, internet kullanıcılarına tavsiyeler, internet servis sağlayıcılarına tavsiyeler, açıklama ve çözümler olmak üzere dört bölümden oluşmaktadır.

---

[167]Başalp , 2004, **a.g.k.** , 95.
[168]Declaration On The Protection Of Privacy On Global Networks; http://www.oecd.org/internet/ieconomy/1840065.pdf (Erişim Tarihi:07.05.2019)
[169]Of The Committee Of Ministers To Member States For The Protection Of Privacy On The İnternet; https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429 (Erişim Tarihi:07.05.2019)

Önsöz kısmında, teknolojik gelişmelerin bilgi alışverişindeki faydalarının göz ardı edilmemesi gerektiği; fakat bu gelişmelerin kişilerin mahremiyet hakkını ihlal etmesinin de önlenmesi için gerekli çabanın gösterilmesi ve mahremiyet hakkının ihlalinin önlenmesi için gerektiğinde teknik yöntemlerden yararlanılması gerektiği vurgulanmıştır.

Giriş kısmında bu tavsiye kararının muhataplarının internet kullanıcıları ve internet servis sağlayıcıları için bazı ilkeler belirlediği, internet kullanıcılarına internet servis sağlayıcılarının sorumluluklarının farkında olması gerektiği, internetin internet kullanıcılarının mahremiyeti için risk taşıdığı, mahremiyet hakkının her bireyin temel hakkı olduğu belirtilmiştir.

### 2.12.2000/31 Sayılı Elektronik Ticaret Yönergesi

Avrupa Birliği tarafından 2000 yılında yürürlüğe konulan 2000/31 Sayılı Elektronik Ticaret Yönergesi[170] ile ticari iletişimde elektronik postanın kullanımına izin veren üye devletlere bazı yükümlülükler getirilmiştir. Buna göre üye devletler, iç hukukta gönderilen elektronik postanın reklam amaçlı olduğunu muhataplarının anlayabilmesini sağlayıcı tedbirleri almalıdır(2000/31 sayılı yönerge M.7).Yine 2000/31 sayılı yönergeye göre üye devletler, internet servis sağlayıcılarının belirli listelerdeki alıcılara reklam iletisi göndermemeleri yükümlülüğünü getirmelidir. Birden çok listenin varlığı sebebiyle bu konuda bir birliğin sağlanamamış olması yeterli korumanın sağlanamayacağı eleştirisini de beraberinde getirmiştir.[171]

### 2.13.Avrupa Birliği Temel Haklar Bildirgesi

Bildirge'nin[172] 8. maddesi:

> "1. Herkes, kendisiyle ilgili kişisel verilerinin korunmasını isteme hakkına sahiptir.
>
> 2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin onayına veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.
>
> 3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir."

şeklinde düzenlenmiştir.

---

[170]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=DE (Erişim Tarihi:11.07.2019)
[171]Başalp , 2004 , **a.g.k.** , 95.
[172]https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708 (Erişim Tarihi:06.07.2019)

Kişisel bilgilerin korunması hakkı, Avrupa Birliği Temel Haklar Bildirgesi'nin ilk halinde yer almayıp daha sonra temel hak olarak bildirgede yerini alan bir haktır. Kişisel verilerin korunması hakkı temel haklar bildirgesine 2001 yılında girmiştir.[173]

Lehmann'a göre temel haklar bildirgesinde kişisel verilerin korunması hakkına yer verilmesinin amacı kendi kaderini tayin hakkını temel hak düzeyine yükseltmektir.[174]

### 2.14.2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü

2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü[175](GPDR), Yönerge'nin yerine yürürlüğe konulmuş bir düzenlemedir.[176] Tüzük'ün 94/1 maddesi:

> "1.95/46/EC sayılı Yönerge, 25 Mayıs 2018 tarihinden itibaren yürürlükten kaldırılmaktadır.
>
> 2.Yürürlükten kaldırılan Yönerge'ye yapılan atıflar, bu Tüzük'e yapılmış atıflar olarak anlaşılacaktır.95/46/EC sayılı Yönerge ile kurulmuş Kişisel Verilerin İşlenmesine ilişkin olarak Bireylerin Korunmasına dair Çalışma Grubu'na yapılan atıflar, bu Tüzük tarafından kurulmuş Avrupa Veri Koruma Kurulu'na yapılmış atıflar olarak anlaşılacaktır."

şeklinde düzenlenmiştir.

Avrupa Birliği'nin 4 Mayıs 2016 tarihli Resmi Gazetesi'nde yayımlanan[177] Tüzük, yürürlük maddesinde belirtildiği üzere 24 Mayıs 2016 tarihinde yürürlüğe girmiştir.

> Yürürlük ve uygulama

---

[173]Başalp , 2004 , **a.g.k.** , 27.
[174]Lehmann, Festschrift für Adolf Dietz, München 2000, s.119'dan aktaran Başalp, 2004, **a.g.k.**, 27.
[175]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Erişim Tarihi:27.08.2019)
Türkçe çevirisi için bkz: https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf
(Erişim Tarihi:27.08.2019)
Tüzük'ün Türkçe çevirisi için "*H. M. Develioğlu(2017). 6698 sayılı Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku. İstanbul On İki Levha Yayıncılık*" isimli eserden yararlanılmıştır.
[176]Çalışmanın bu bölümünde AB Genel Veri Koruma Tüzüğü'nden kısaca "Tüzük" olarak bahsedilecektir.
[177]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
(Erişim Tarihi:12.04.2020)

MADDE 99-1.Bu Tüzük, Avrupa Birliği Resmi Gazetesi'nde yayınlanmasını takip eden yirminci günde yürürlüğe girer.

2.25 Mayıs 2018'den itibaren uygulanacaktır.

Bu Tüzük, tüm Üye Devletlerde bir bütün olarak bağlayıcı ve doğrudan uygulanabilir olacaktır.

### 2.14.1. Amaç ve kapsam

Tüzük'ün '*konu ve amaçlar*' başlıklı maddesi şöyledir:

MADDE 1-1.Bu Tüzük, gerçek kişilerin kişisel verilerinin işlenmesine dair korunmasına ilişkin kuralları ve kişisel verilerin serbest dolaşımına ilişkin kuralları ortaya koyar.

2.Bu Tüzük, gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin korunması haklarını korur.

3.Birlik dahilinde kişisel verilerin serbest dolaşımı, gerçek kişilerin kişisel verilerinin işlenmesine dair olarak korunması ile bağlantılı nedenlerle kısıtlanamaz veya yasaklanamaz.

Buna göre Tüzük, tüzel kişilere ait kişisel verilerin korunmasında uygulanmaz.[178] Halbuki Tüzük'ün yürürlükten kaldırdığı Yönerge'de, Tüzük'ten farklı şekilde Yönerge'nin tüzel kişilere uygulanabileceği öngörülmüştür.[179]

Tüzük, veri sorumlusu veya veri işleyicinin AB sınırları içindeki bir kuruluşunun faaliyetleri bağlamındaki kişisel verileri işleme faaliyetinde uygulanır(M.3/1). Buradan çıkartılacak sonuç; Tüzük'ün kapsamına girmek için veri işlemenin doğrudan kuruluş tarafından yapılmasının aranmadığı, kuruluşun faaliyeti kapsamında yapılan veri işlemelerinin tüzük kapsamına girdiğidir. Ayrıca tüzük açısından fiziki olarak verinin işlendiği yerin de önemi yoktur. Örneğin Almanya merkezli bir şirket AB sınırları içinde sunduğu hizmeti AB sınırları dışında olan Türkiye'de sunmak istese Türkiye'deki müşterilerin kişisel verilerinin toplanması ve işlenmesi Türkiye'de gerçekleşse bile bu veri işleme ve toplama faaliyeti, AB sınırları içerisinde yer alan bir kuruluşun faaliyetleri kapsamında yürütüldüğünden Tüzük'ün uygulama alanı içerisindedir.

Bununla ilgili olarak Avrupa Birliği Adalet Divanı'nın Google Spain kararından da bahsetmek gerekir.[180] Bu karar, esasında ABAD'ın unutulma hakkına yönelik

[178]Develioğlu , 2017 , **a.g.k.** , 30.
[179]Develioğlu , 2017 , **a.g.k.** , 30.

değerlendirmesiyle bilinse de Avrupa Birliği Adalet Divanı'nın Tüzük'ün yer bakımından nasıl uygulanacağına yönelik değerlendirmesini de yansıtması sebebiyle önem arz etmektedir. Karara konu olay şöyledir: İspanya'da faaliyet gösteren Google Spain, ABD merkezli bir tüzel kişi olan Google Inc.'nin İspanya'daki pazarlama faaliyetlerini gerçekleştiren ve ayrı bir tüzel kişiliği olan alt kuruluştur. ABAD'a göre Google Inc. veri sorumlusudur, Google Spain ise veri işleyicisidir. Çünkü Google Arama Motorunu işleten her ne kadar Google Inc de olsa bu verileri arama motoruna işleyen Google Spain'dir. Arama motoru sadece önceden işlenmiş verileri göstermektedir. Ve veri işleyicisi olan Google Spain, AB hukuku kapsamında sorumluluk taşımaktadır. Bu kararın ortaya çıktığı dönemde Tüzük yürürlükte olmasa bile Yönerge'ye yapılan atıfların Tüzük'e yapılmış sayılacağı kuralı dikkate alındığında ABAD'ın Google Spain kararıyla Tüzük'ün yer bakımından nasıl uygulanacağı yönünde bir yol gösterdiği söylenebilir.

Tüzük, verileri işlenen kişinin AB vatandaşı olup olmaması konusunda bir ayrım yapmadığı için her gerçek kişiye ilişkin veri işleme faaliyetinin Tüzük kapsamında olabileceği söylenebilir. Ayrıca Tüzük'ün 3. maddesinde işleme faaliyetinin AB sınırları dışında gerçekleşip gerçekleşmediği ayrımı yapmadığı özellikle vurgulanmıştır.

> MADDE 3- 2.Bu Tüzük, Birlik dahilindeki ilgili kişilerin kişisel verilerinin Birlik dahilinde işletmesi bulunmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesi halinde, işleme faaliyetlerinin:
>
> (a)ilgili kişiden bir ödeme istenip istenmeyeceğine bakılmaksızın, Birlik dahilinde bulunan ilgili kişilere mal veya hizmet sunulmasına
>
> (b)Birlik dahilinde gerçekleşen davranışlarının gözlemlenmesine ilişkin olması halinde uygulanır.

Tüzük'ün gerekçesi ve Avrupa Veri Koruma Kurulu'nun yorumu dikkate alındığında herhangi bir nedenle geçici olarak AB sınırları içinde bulunan, uyruğu ve ikametgâhı AB dışındaki bir gerçek kişi de Tüzük'ün 3. maddesinin 2. fıkrası kapsamındadır.[181] Örneğin iş gereği veya turistik amaçla geçici süreliğine bir AB

---

[180]ABAD. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. 13/05/2014 , 131/12
http://www.abgm.adalet.gov.tr/abadaletdivani/abadaletdivani.html (Erişim Tarihi:05.12.2019)
http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_13.pdf (Erişim Tarihi:05.12.2019)
[181]Yörük , 2019 , **a.g.k**. , 50.

ülkesinde bulunan bir Rus vatandaşı, Tüzük'ün 3. maddesinin 2. fıkrası kapsamında AB sınırları içerisindeki bir veri öznesidir.

Tüzük'ün 3. maddesinin 3. fıkrasına göre eğer AB sınırları içerisinde bir kuruluşu bulunmayan veri sorumlusu, uluslararası hukukun gereği olarak AB üyesi devletlerin hukukunun uygulandığı bir yerde bulunuyorsa bu veri sorumlusunun kişisel veri işleme faaliyetinde Tüzük uygulanır.

### 2.14.2.Tanımlar

Tüzük'te tanımlara 4. madde'de yer verilmiştir.

Kişisel Veri, "*kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi*" olarak tanımlanmıştır.

Belirlenebilir gerçek kişi, "*bir tanımlayıcıya, örneğin ismine, kimlik numarasına, konum bilgisine, bir çevrimiçi tanımlayıcıya ya da bu kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ilişkin bir veya birden fazla etkene referans yaparak doğrudan ve dolaylı olarak belirlenebilen kişi*" olarak tanımlanmıştır.

İşleme, "*otomatik veya otomatik olmayan araç ve yöntemlerle, kişisel veri veya veriler üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya elde etme, danışma iletim yoluyla açıklama, , yayma, değiştirme, kullanma, kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi*" olarak tanımlanmıştır.

İşleme kısıtlaması, "*saklanan kişisel verilerin gelecekte işlenmelerinin sınırlanması amacı ile işaretlenmesi*" olarak tanımlanmıştır.

Profil çıkarma, "*bir gerçek kişinin çalışma yaşamındaki performansı, bireysel tercihleri, sağlığı, ekonomik hali, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere bu gerçek kişiye ait belirli şahsi özelliklerin değerlendirilmesi amacıyla kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimi*" olarak tanımlanmıştır.

Takma ad kullanımı ise "*kişisel verilerin tanımı yapılmış veya tanımlanması mümkün bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile ek bilgilerin*

*ayrı tutulması ve teknik ve düzenlemeye ilişkin tedbirlere tabi tutulması koşuluyla, kişisel verilerin bu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesi*" olarak tanımlanmıştır.

Dosyalama sistemi, "*işlevsel veya coğrafi bir temelde özellikli ölçütlere göre erişilebilen, yapılandırılmış herhangi bir kişisel veri dizisi*" olarak tanımlanmıştır.

Veri kontrolörü(veri sorumlusu), "*tek başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*" olarak tanımlanmıştır. Görüldüğü üzere, veri sorumlusu, kişisel verileri elinde bulundurması dolayısıyla değil, kişisel verilerin işleme amaçlarını ve vasıtalarını belirlemekle veri sorumlusu sıfatını kazanmaktadır.

Örneğin, müşterilerinin iletişim bilgilerini ihtiva eden listeyi bulunduran firma, bu bilgileri ne şekilde kullanacağına karar verdiği için veri sorumlusudur.[182] Firma, bu listeyi, kendi kontrolünde olmak suretiyle bir firmanın bulut veri tabanına[183] aktarırsa veri sorumlusu olarak kalmaya devam eder. Bulut veri tabanı sahibi firma, kişisel verilerin işlenmesi amaç ve vasıtalarını belirlemediğinden veri sorumlusu sıfatını kazanmaz. Fakat bulut veri tabanı sahibi firma, listedeki bilgileri kullanmaya başlarsa(müşterilere reklam mesajı yollamak gibi) veri sorumlusu kabul edilecektir.

İşleyici, "*veri sorumlusu adına kişisel verileri işleyen bir gerçek kişi veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*" olarak tanımlanmıştır.

Alıcı(aktarılan), "*üçüncü bir kişi olsun veya olmasın, kişisel verilerin açıklandığı bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*" olarak tanımlanmıştır.

Üçüncü kişi, "*veri sahibi, veri sorumlusu, veri işleyici ve veri sorumlusu ya da işleyicinin doğrudan yetkisi altında, kişisel verileri işleme yetkisi bulunan kişiler*

[182]Develioğlu , 2017 , **a.g.k.** , 42.

[183]Bulut Bilişim; "internet üzerinden bir internet tarayıcı kullanarak ek bir yazılıma ihtiyaç duymadan servis sağlayıcıdan saatlik günlük aylık kiralanabilen kaynak havuzunun kullanımıdır." B. Arslan(2018). *Bulut Bilişim'in avantajları ve dezavantajları*. Yayımlanmamış Yüksek Lisans Projesi. İstanbul: Maltepe Üniversitesi Sosyal Bilimler Enstitüsü. 3.
http://openaccess.maltepe.edu.tr/xmlui/handle/20.500.12415/3403#sthash.ktM8Ai2q.diEHLBIN.dpbs(Erişim Tarihi:16.04.2020)

*haricindeki bir gerçek veya tüzel kişi, kamu kurumu, kuruluşu veya organı*" olarak tanımlanmıştır.

Veri sahibinin rızası, "*veri sahibinin bir beyanla ya da açık bir rıza ile kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge*" olarak tanımlanmıştır.

Kişisel veri ihlali, "*iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlali*" olarak tanımlanmıştır.

Genetik veri, "*bir gerçek kişinin sağlığı veya fizyolojik durumu ile ilgili kendine özgü bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtım yoluyla alınan veya kazanılan özelliklerine ilişkin kişisel veri*" olarak tanımlanmıştır.

Biyometrik veri, "*bir gerçek kişinin diğerlerinden ayırt edilebilir surette teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veri*" olarak tanımlanmıştır. Parmak izi, biyometrik veriye örnek olarak verilebilen kişisel verilerdendir.

Sağlıkla ilgili veri, "*sağlık hizmetlerinin sağlanması da dahil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel veri*" şeklinde belirlenmiştir.

Tüzük'de asıl kuruluş kavramının iki tanımı düzenlenmiştir. Birinci tanıma göre asıl kuruluş, "*birden fazla üye devlette işletmesi bulunan bir kontrolör ile ilgili olarak, kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemlere yönelik kararların kontrolörün Birlik içerisindeki başka bir işletmesinde alınmaması ve bu işletmenin söz konusu kararları uygulatma yetkisinin bulunmaması durumunda (ki bunların gerçekleşmesi halinde, söz konusu kararları alan işletme asıl kuruluş olarak kabul edilir), Birlik içerisindeki merkezi idare yeri*" olarak tanımlanmıştır. İkinci tanım ise, "*birden fazla üye devlette işletmesi bulunan bir işleyici ile ilgili olarak, Birlik içerisindeki merkezi idare yeri veya, işleyicinin Birlik içerisinde merkezi bir işletmesinin bulunmaması halinde, işleyicinin bir işletmesinin faaliyetleri bağlamındaki temel işleme*

*faaliyetlerinin işleyicinin bu Tüzük kapsamındaki spesifik yükümlülüklere tabi olduğu ölçüde gerçekleştiği Birlik içerisindeki işletmesi*" şeklinde düzenlenmiştir.

Temsilci, "*Birlik içerisinde kurulu bulunan kontrolör veya işleyici tarafından yazılı olarak belirlenen, bu Tüzük kapsamındaki yükümlülükleri ile ilgili olarak kontrolör veya işleyiciyi temsil eden bir gerçek veya tüzel kişi*" olarak tanımlanmıştır.

İşletme, "*hukuki biçimine bakılmaksızın bir ekonomik faaliyetle uğraşan gerçek veya tüzel kişi*" olarak tanımlanmıştır.

Teşebbüsler grubu, "*bir denetleyici teşebbüs ve denetlenmiş teşebbüs*" olarak tanımlanmıştır.

Bağlayıcı kurumsal kurallar, "*ortak bir ekonomik faaliyetle meşgul olan bir teşebbüsler grubu veya bir işletmeler grubu içerisinde bir veya daha fazla sayıda üçüncü ülkedeki bir kontrolör veya işleyiciye kişisel veri aktarımları veya aktarım dizisiyle ilgili olarak Birliğin üye devletlerinden birinin topraklarında kurulmuş olan bir kontrolör veya işleyici tarafından uyulan kişisel veri koruma politikaları*" olarak tanımlanmıştır.

Denetim Makamı; Tüzük'ün uygulamasının izlenmesinden sorumlu olan, AB üyesi devletlerin kurmak zorunda olduğu bağımsız kamu kuruluşlarıdır.

Bunun dışında Tüzük'te yer bulan tanımlar, 4. madde'de şu şekilde yer almaktadır.

> MADDE 4-(22) 'İlgili denetim makamı':
>
> (a)Veri sahibi veya veri işleyenin işletmesinin, denetim makamının bulunduğu Üye Devlet sınırları içinde bulunduğu;
>
> (b)Denetim makamının bulunduğu Üye Devlette yerleşik ilgili kişilerin işleme nedeniyle önemli ölçüde etkilendiği veya etkilenmeleri muhtemel olduğu;
>
> (c)denetim makamına şikayette bulunulduğu için kişisel verilerin işlenmesi ile ilgilenen denetim makamı anlamına gelir,
>
> (23) 'sınır-ötesi işleme'
>
> (a) veri sorumlusunun veya veri işleyenin birden fazla Üye Devlette işletmesinin bulunduğu hallerde veri sorumlusunun veya veri işleyenin birden fazla Üye Devletteki işletmelerindeki faaliyetleri kapsamında gerçekleşen kişisel veri işlemeleri; veya

(b)veri sorumlusunun veya veri işleyenin Birlik dahilindeki tek işletmesinin faaliyetleri kapsamında gerçekleşen ancak birden fazla Üye Devlette bulunan ilgili kişileri önemli ölçüde etkileyen veya etkilemesi muhtemel olan kişisel verileri işlemeleri anlamına gelir;

(24) 'alakalı ve gerekçeli itiraz' bu Tüzük'ün ihlal edilip edilmediğine veya veri sorumlusuyla ya da veri işleyenle ilgili olarak planlanan faaliyetin bu Tüzük'e uygun olup olmadığına ilişkin bir taslak karara, taslak kararın ilgili kişilerin hak ve özgürlüklerine ve ilgili hallerde, Birlik dahilinde kişisel verilerin serbest dolaşımına teşkil ettiği risklerin önemini açıkça ortaya koyan itiraz anlamına gelir;

(25) 'bilgi toplumu hizmeti' Avrupa Parlamentosu ve Konseyi'nin 2015/1535 sayılı Yönergesi'nin[184] 1(1). maddesinin (b) bendinde tanımlanan hizmet anlamına gelir;

(26) 'uluslararası kuruluş' uluslararası kamu hukukuna tabi bir kuruluş ile ast kuruluşlarını veya iki veya daha fazla ülke arasında bir anlaşma ile veya buna dayanarak kurulmuş diğer kuruluş anlamına gelir.

### 2.14.3.Kişisel verilerin işlenmesine ilişkin ilkeler

Kişisel verilerin işlenmesi, kanuna uygun olsa bile bazı temel ilkelere aykırı ise bu veri işlemesinin hukuka uygun bir veri işlemesi olduğu söylenemez. Bu sebeple Tüzük, 5. maddesinde bazı temel ilkelere yer vermiştir.

Bu ilkelerden birinin hukuka uygunluk, dürüstlük ve şeffaflık ilkesi olduğu söylenebilir.[185]

Kural olarak kişisel verilerin işlenmesi faaliyeti hukuka aykırıdır. Hukuka uygunluğun sağlanması için kişisel verilerin, tüzükte belirtilen hukuka uygunluk hallerinde işlenmesi gerekir.

Şeffaflık ile veri işleyici ve işleme maksadı hususunda her halükarda veri sahibini bilgilendirmek amaçlanmaktadır.[186] Şeffaflık kuralı, Tüzük'ün yürürlükten kaldırdığı Yönerge'de düzenlenmemişken Tüzük'te düzenlenmiştir.

Hukuka uygunluk ve dürüstlük ilkeleri, Tüzük'ten önce, Yönerge'de, OECD rehber ilkelerinde, Sözleşme'de, BM rehber ilkelerinde, APEC Çerçeve Belgesinde, "kişisel verilerin hukuka uygun ve meşru usullerle toplanması ve işlenmesi gerektiği"

[184]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L1535&from=EN (Erişim Tarihi:09.09.2019)
[185]H. Üzeltürk(2018). Avrupa Birliği Genel Veri Koruma Düzenlemesi. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi. C.15, 2018/2, 161-179, 164.
[186]Develioğlu , 2017 , **a.g.k.** , 44 .

ifade edilmek suretiyle yer almaktaydı. Şeffaflık ilkesi ilk defa Tüzük'te yer alan bir ilke olarak karşımıza çıkmaktadır.[187]

Kişisel verileri işlenmesi faaliyetinde dürüstlük ilkesine uyan bir veri sorumlusundan beklenen, veri öznelerine(sahiplerine) karşı adil bir tutum içerisinde olması, veri öznelerinin menfaatlerini ve makul beklentilerini dikkate alması, tarafların menfaatleri arasında bir denge gözetmesidir.[188] Bir açıdan dürüstlük ilkesinin karşılığının 'hakkaniyet' olduğu söylenebilir.

Şeffaflık ilkesine uyan bir veri sorumlusu, Tüzük'ün veri sorumlusunun veri sahibi ile paylaşması gerektiğini öngördüğü ve Tüzük'ün 13. ve 14. maddesinde yer alan bilgiler ile ilgili olarak veri öznesini bilgilendirmelidir.[189] Şeffaflık ilkesine uyulmayan bir kişisel veri işleme faaliyetinde dürüstlük ilkesine uyulması mümkün değildir. Zira veri sorumlusunun veri öznesine ait verileri işlerken ondan bu faaliyete ilişkin bilgileri saklaması, veri sorumlusu ile veri öznesi arasındaki menfaat dengesizliğine sebebiyet vermektedir. Bu menfaat dengesizliği, 'hakkaniyet' anlamına da gelen dürüstlük ilkesiyle bağdaştırmak mümkün değildir.

Amaçla sınırlı olma kuralına göre kişisel veriler; belirli, açık ve meşru amaçların gerçekleşmesi maksadıyla toplanır, işlenir.

Bu kural uyarınca verilerin toplandıktan sonraki işlenme amaçlarının toplanma amacıyla uyumlu olması gerekmektedir. Örneğin, bir internet sitesi, topladığı verileri pazarlama amacıyla kullanmayacağını açıklamış olmasına rağmen internet sitesi kullanıcısına reklam e-postası gönderiyorsa bu veri işlemesinin amaçla sınırlı olma kuralını ihlal ettiği için hukuka aykırı bir veri işlemesi olduğunu söylemek mümkündür.[190]

Tüzük, bir kişisel verinin toplandığı amaç dışında işlenebilmesi için veri sahibinin rızasının varlığını aramıştır(M.6/4).

---

[187]Yörük , 2019 , **a.g.k**. , 53.
[188]S. Oğuz (2018). *Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*. Bilgi Ekonomisi ve Yönetimi Dergisi. 13 (2), 121-138, 132.
[189]Yörük , 2019, **a.g.k**. , 53.
[190]Develioğlu , 2017, **a.g.k.** , 46.

Amacın meşru olması, kişisel verilerin yasal bir dayanağa göre toplanmasını ve bu yasal dayanaklar ile getirilen ilkelere uygun bir amaç doğrultusunda işlenmesini ifade eder.[191]

Amacın belirli ve açık olması, gelecekte ortaya çıkacak bir amaç için veri toplanmamasıdır. Zira gelecekteki bir amaç için veri toplamak kişileri muhtemel suçlu konumuna koymak anlamına gelir[192] ki bu da kişilerin maddi ve manevi varlığını geliştirme hakkına, masumiyet karinesine zarar vermekten başka bir sonuç doğurmaz.

Veri sınırlaması (veri minimizasyonu) ilkesi gereği veri sorumlusu, maksadına erişecek kadar veri toplamalıdır.[193]

Ayrıca Tüzük'ün 25. maddesi ile veri sorumlularına veri minimizasyonu ilkesinin gerçekleştirilmesi için her türlü tedbiri alma yükümlülüğü getirilmiştir.

Bu kapsamda örneğin iş, okul ve benzeri kurumlara başvuru formlarında veya internetteki kayıt sayfalarında amaca ulaşmak için gerekli olandan fazla bilgi talep edilmemeli veya güvenlik kameraları, güvenlik amacını aşacak surette veri toplayacak şekilde yerleştirilmemelidir.[194]

Fransa'da *Commission national de I'informatique et des libertes* (CNIL)[195], bir koleje giriş-çıkışların rahat yapılması için, çalışan ve öğrencilerin parmak izlerinin alınmasını ölçülülük ilkesine aykırı kabul etmiştir.[196]

Veri sınırlaması ile ilgili verilebilecek diğer örnek ise şudur: Evcil köpekler ve sahiplerinin kayıtlı tutulduğu bir sicilde bu köpek sahiplerinin uyuşturucu bağımlısı olup olmadıkları bilgisi yer alması ölçülülük ilkesine aykırıdır; zira bu sicillerin tutulma amacı köpeklerin yetiştirilme koşullarına ve saldırgan davranışlarına önlem almak suretiyle kamu güvenliğini sağlamaktır.[197]

---

[191]Yörük , 2019, **a.g.k**. , 55.
[192]Küzeci, 2010, **a.g.k**. , 215.
[193]Oğuz, 2018, **a.g.k.** , 134.
[194]Küzeci , 2010, **a.g.k**. , 203-204.
[195]Kişisel Verilerin Toplanması, Depolanması ve Kullanımına Veri Gizliliği Yasası'nın uygulanmasını sağlamak üzere Fransa'da kurulmuş, bağımsız bir idari düzenleme organıdır. https://en.wikipedia.org/wiki/Commission_nationale_de_l'informatique_et_des_libert%C3%A9s (Erişim Tarihi:25.03.2020)
[196]Develioğlu , 2017 , **a.g.k.** , 47.
[197]Nouveau Stoffel, Dominique, Vingt ans de protection des donnees, 1993-2013, Revue Fribourgeoise de Jurisprudence, 2013, s. 3 vd.'den aktaran Develioğlu, 2017, **a.g.k.**, 48.

Doğruluk ilkesine göre doğru ve güncel olmayan kişisel veriler için gerekli düzeltmeler yapılmalıdır. Zaten Tüzük de veri sahibine gerekli düzeltmenin yapılmasını isteme hakkı vermiştir. Veri sorumlusu açısından bu düzeltmeyi yapmak aynı zamanda bir yükümlülüktür. Veri öznesinin bu hakkını kullanması veya veri sorumlusunun bu yükümlülüğünü yerine getirmesi doğruluk ilkesine ulaşmaya katkı sağlaması açısından önemlidir.

Kişisel verinin doğru ve güncel olması veri sahibinin temel haklarının korunması için önemlidir. Fakat veri sorumlusu için de verinin güncel ve doğru olması önemlidir. Zira doğru ve güncel olmayan bir veri, veri işleme amacına ulaşmanın önünde bir engel teşkil etmektedir. Zaten Tüzük'ün "*ilgili kişi, veri sorumlusundan, doğru olmayan kişisel verilerin gecikmeksizin düzeltilmesini sağlama hakkına sahiptir. İlgili kişi, işlemenin amaçları dikkate alındığında, ek beyanda bulunmak suretiyle de olmak üzere, eksik kişisel verilerin tamamlanması hakkına sahiptir*" şeklinde düzenlenen 16. maddesinde ilgili kişilere, doğru olmayan veriyi düzeltme hakkı verilmesi, Tüzük'ün doğruluk ilkesine verdiği önemi göstermektedir.

Sınırlı süre saklanma ilkesine göre kişisel veriler, işlendikleri amacın gerektirdiğinden daha uzun süre ilgili kişinin belirlenmesine izin veren halde tutulmayacaktır. Mevzuatta bir süre belirlenmediyse veriler, amacın gerçekleşmesine yetecek makul sürede korunmalı, bu müddetin neticesinde silinmeli yahut anonimleştirilmelidir.[198] Kişisel verilerin "bir gün gerekli olursa" düşüncesiyle tutulmasının bütün bir toplumu olası suçlu pozisyonuna sokabileceği[199] dikkate alındığında; sınırlı süre saklama ilkesi ile amacın belirliliği ilkesinin birbirini tamamladığını söylemek mümkündür.

Örneğin, bir telekom şirketiyle yapılan şikayete ilişkin çağrı merkezi ile yapılan görüşmenin şikayet sonuçlandırıldıktan sonra silinmesi sınırlı süre saklama kuralının gereğidir.[200]

Veya bir anket için toplanan kişisel veriler anket sonuçlandıktan sonra silinmelidir.

---

[198] Develioğlu , 2017 , **a.g.k.** , 49.
[199] Küzeci , 2010 , **a.g.k.** , 215.
[200] Develioğlu , 2017, **a.g.k.** , 49.

Aynı şekilde sınırlı süre saklama prensibine göre bir dergi abonesinin kişisel verileri, kişi aboneliğini iptal ettikten sonra tekrar abone olma ihtimali göz önünde tutularak saklanmamalıdır.[201]

Tüzük'ün 17. maddesinde sınırlı süre saklama prensibinin gerçekleşmesi için kişisel verilerin toplandıkları ve işlendikleri amacın gerçekleşmesi için gerekli olmaması halinde veri sorumlusunun kişisel veriyi silme yükümlülüğü taşıdığı düzenlenmiştir.

Yönerge'de yer almayan; fakat Tüzük'te yer bulan bütünlük ve gizlilik kuralına göre kişisel veriler, uygun ortam sağlanarak, bu kapsamda yetkisiz ve hukuka aykırı şekilde işlenmelerine ve kazaen kaybolmalarına, imha edilmelerine yahut hasara maruz kalmalarına mukabil güvende tutulmaları amacıyla münasip teknik ve organizasyonel önlemler alınmak suretiyle işlenmelidir(Tüzük M.5/1-f).

Hesap verilebilirlik(sorumluluk) kuralına göre veri sorumlusu, yukarıdaki kurallara uygun davranmaktan sorumlu olmalı ve bu kurallara uyduğunu ispatlayabilmelidir(Tüzük M.5/2).

Daha genel anlamıyla hesap verilebilirlik ilkesi; veri sorumlusunun işleme faaliyetlerinde kişisel verilerin korunması kurallarına uyulmasını güvence altına alan tedbirleri alma ve bu önlemlerin alındığını veri sahiplerine, denetim kurumlarına ispatlayan belgeleri bulundurma yükümlülüğü olarak açıklanabilir.[202]

### 2.14.4.Kişisel verilerin işlenmesinin hukuka uygunluk şartları

Tüzük'ün 6. maddesindeki "*İşleme faaliyeti, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve olduğu ölçüde, hukuka uygundur*" ibaresinden de anlaşıldığı üzere Tüzük uyarınca kural olarak kişisel verilerin işlenmesi, hukuka aykırı bir faaliyettir. Fakat belirli şartların gerçekleşmesi durumunda kişisel veri işlemesi hukuka uygun bir faaliyet hale gelir.

Belirli bir veya birden fazla amaç için olmak üzere kişisel veri sahibinin rızası kişisel veri işlemesini hukuka uygun bir faaliyet haline getirir.

[201]Yörük , 2019 , **a.g.k**. , 59.
[202]Yörük , 2019 , **a.g.k**. , 60.

Tüzük'ten farklı olarak Yönerge'de hukuka uygunluk sebebi olarak kabul edilebilecek rızanın niteliği hususunda açık bir kriter olmadığı ve AB üyesi ülkelerin rızanın şeklini kendi iç hukuklarında belirlediği görülmektedir.[203]

Tüzük'te ise rıza, "*bir beyan veya olumlayıcı eylem şeklinde kendisiyle ilgili kişisel verilerin işlenmesine mutabık kaldığını ortaya koyan, ilgili kişinin isteklerinin özgürce verilmiş, konuya özel, bilgilendirilmiş ve belirsizlik içermeyen bir göstergesi*" olarak açıkça tanımlanmıştır(M.4/11).

Tüzük uyarınca veri öznesinin iradesini açıkça ortaya koymadan verdiği beyan geçerli bir rıza olarak değerlendirilemez. Dolayısıyla kişinin sessiz kalarak zımnen rıza verdiği şeklindeki karine geçersizdir.[204]

Emsal olarak kişinin internet tarayıcısından kendisiyle alakalı veri toplanmasını mümkün kılan ayarları değiştirmemesiyle zımni bir rıza verdiği, dolayısıyla bu rızanın veri toplamayı hukuka uygun hale getirdiği söylenemez.[205]

Tüzük'ün, hukuka uygunluk sebebi olarak rıza gösterilmesi noktasında hassas veri-hassas olmayan veri ayrımı yaptığı; bu doğrultuda hassas verilerin işlenmesinde açık rızayı, hassas olmayan verilerin işlenmesinde ise açık olmayan rızayı hukuka uygunluk sebebi olarak aradığı görülmektedir.[206]

Tüzük'ün rızanın şekli konusunda bir ayrım yapmadığı görülmektedir. Bu açıdan özgür iradeyle verilmek şartıyla yazılı, sözlü ve elektronik yollarla verilen açık rızanın da tüzük açısından hukuka uygunluk sebebi sayılan, geçerli bir rıza olduğu söylenebilir. Tüzük'ün giriş kısmında da rızanın nasıl olması ile ilgili örneklere yer verilmiştir.[207] Örneğin bir internet sitesinde yer alan kişisel verilerin işleneceğine dair kutunun tıklanması, internetten bir hizmet satın almak için gerekli teknik ayarların seçilmesi ve benzeri davranışlarda bulunulması Tüzük'ün aradığı rızayı açıkça ortaya koyar. Fakat önceden işaretli kutudaki işaretin kaldırılmaması şeklindeki bir hareketsiz kalma Tüzük'ün hukuka uygunluk sebebi olarak aradığı rıza şekli değildir.

[203]Develioğlu , 2017, **a.g.k.** , 52.
[204] Selek , 2019 , **a.g.k.** , 932.
[205]Develioğlu , 2017 , **a.g.k.** , 52.
[206] Selek , 2019 , **a.g.k.** , 913.
[207]Develioğlu , 2017 , **a.g.k.** , 52-53.

Tüzük ve Yönerge'deki rıza tanımları benzerliğine rağmen Tüzükte geçen "bir beyan veya onaylayıcı eylem" ibarelerinin Yönerge'de olmadığı görülmektedir.[208]

Rıza, genel bir onay şeklinde olmamalı, hangi işleme faaliyetine rıza gösterildiği açıkça anlaşılabilmelidir.[209]Örneğin bir internetten satış sitesinde internet kullanıcısından her türlü işlem için verilerin kullanılacağına dair alınan rıza geçerli değildir. Fakat sadece reklam mesajlarının gönderilmesi için verilerin kullanılması için alınan rıza geçerli bir rızadır.

Tüzük'ün 7. maddesinde, rızanın geçerlilik şartları düzenlenmiştir.

> MADDE 7- 1.İşlemenin rızaya dayalı olduğu hallerde, veri sorumlusu ilgili kişinin kişisel verilerinin işlenmesine rıza gösterdiğini ortaya koyabilmelidir.
>
> 2.İlgili kişinin rızasının başka hususları da kapsayan yazılı bir beyan olarak verildiği hallerde, rıza verilmesi talebi, diğer konulardan açıkça ayırt edilebilecek nitelikte sunulmalı, anlaşılır ve kolayca erişilebilir şekilde olmalı, açık ve basit bir dil kullanılmalıdır. Böyle bir beyanın Tüzük'e aykırılık teşkil eden kısımları bağlayıcı olmayacaktır.
>
> 3.İlgili kişi her zaman rızasını geri alma hakkına sahiptir. Rızanın geri alınması, rıza geri alınana kadar gerçekleştirilen işlemelerin hukuka uygunluğunu etkilemez. İlgili kişi rıza vermeden önce bu konuda bilgilendirilmelidir. Rızanın geri alınması, rızanın verilmesi kadar basit olmalıdır.
>
> 4.Rızanın serbestçe verilip verilmediğinin değerlendirilmesinde, diğer hususların yanında, sözleşmenin ifasının, bir hizmetin sunulması dahil olmak üzere, sözleşmenin ifası için gerekli olmayan bir işlemenin gerçekleştirilmesi şartına bağlanıp bağlanmadığına azami önem verilmelidir.

Yönerge'de, çocuğun rızasına yönelik bir düzenlemenin yer almadığı görülmektedir. Fakat Tüzük'te çocukların rızası üzerine de düzenlemeler mevcuttur. Bilgi toplumu hizmetleri'ne ilişkin yapılacak veri işlemelerinde çocuğun rızası, 8. maddede ayrıca düzenlenmiştir. Fakat öncelikle 'bilgi toplumu hizmeti' kavramını açıklamak gerekmektedir.

Tüzük, 'bilgi toplumu hizmeti' kavramını doğrudan tanımlamamakta; fakat Avrupa Parlamentosu ve Avrupa Konseyi'nin 2015/1535 sayılı Yönergesi'ndeki tanıma

[208]Selek , 2019 , **a.g.k.** , 915
[209]Develioğlu , 2017 , **a.g.k.** , 53.

atıfta bulunmaktadır.2015/1535 sayılı Yönerge'deki[210] tanıma göre bilgi toplumu hizmetleri, uzaktan ve elektronik yollarla ve hizmet alıcısının bireysel talebi neticesinde kural olarak bedel karşılığı sağlanan hizmetlerdir.

Tüzük'ün 8. maddesinde bilgi toplumu hizmetlerine ilişkin olarak çocukların rızasına ilişkin koşullar şöyle belirlenmiştir:

> MADDE 8- 1.6(1). Maddenin (a) bendinin uygulandığı hallerde, doğrudan bir çocuğa bilgi toplumu hizmeti sunulmasıyla ilgili olarak çocuğun kişisel verilerinin işlenmesi, çocuk en az 16 yaşındaysa hukuka uygun olur. Çocuk 16 yaşının altındaysa, böyle bir işleme sadece çocuk üzerinde velayet sorumluluğunu taşıyan tarafından rıza veya yetki verilmesi halinde hukuka uygun olur.
>
> Üye devletler 13 yaşından daha az olmamak üzere, kanun ile daha düşük bir yaş belirleyebilirler.
>
> 2.Veri sorumlusu bu durumlarda çocuk üzerinde velayet sorumluluğunu taşıyan tarafından rızanın verildiğini veya yetkilendirildiğini tahkik etmek için, mevcut teknoloji ışığında makul çaba gösterecektir.
>
> 3.1.fıkra, Üye Devletlerin sözleşmenin geçerliliği, kurulması veya bir çocuğa ilişkin hükmü gibi genel sözleşmeler hukuku kurallarını etkilemez.

Tüzük'ün 6. maddesinde, rıza dışındaki hukuka uygunluk hallerinin;

- İşlemenin bir aktin kurulması ya da ifası için mecburiliği,
- İşlemenin veri sorumlusunun yasal sorumluluğunu ifası için mecburiliği,
- İşlemenin ilgili kişinin veya sair gerçek kişilerin yaşamsal çıkarlarını muhafaza için gerekliliği,
- İşlemenin kamu yararını gerçekleştirmek için yerine getirilen bir görevin ifası için gerekli olması
- İşlemenin veri sorumlusunun resmi yetkisinin kullanılması için gerekli olması,
- İşlemenin meşru menfaatlere ulaşmak amacıyla gerekli olması

olarak sayıldığı görülmektedir.

[210](http-184).

Tüzük'ün 6. maddesine göre kişisel veri işlemesi, bir aktin kurulması yahut ifası için gerekliyse bu kişisel veri işlemesi hukuka uygundur.

Bu hükmün getiriliş amacı, veri sorumlusunu, sözleşme ilişkisinde olduğu veya olabileceği kişi ile ilgili gerekli bilgileri alması halinde doğabilecek risklere karşı korumaktır.[211]

Sözleşmenin kurulması işlemleri, sözleşmeye hazırlık işlemleri olarak da tanımlanmaktadır. Bu işlemler, sözleşmenin kurulması öncesinde sözleşmenin kurulup kurulmayacağı hususunda tarafların karar verdiği, sözleşmenin kurulması için gerekli koşulların oluşturulduğu, sözleşmelerin taraflarının birbiriyle iletişime geçmesini sağlayan işlemlerdir. Örneğin kurulması muhtemel sözleşmenin taraflarından birinin sözleşme şartlarını görüşmek üzerine diğer taraftan adres ve telefon bilgilerini istemesi durumunda bu kişisel verilerin elde edilmesi sözleşme öncesi hazırlık işlemi olduğu için hukuka uygun bir kişisel veri işlemesidir. Örneğin bir şirket ile işçi adayı arasında iş sözleşmesi kurulmadan önce şirketin adaydan özgeçmişini temin etmesi sözleşme öncesi hazırlık işlemi olduğu için hukuka uygun bir kişisel veri işlemesidir.

Eğer sözleşme hazırlık işlemleri neticesinde sözleşme kurulmazsa sözleşmeye hazırlık işlemleri neticesinde elde edilen kişisel veriler amacın ortadan kalkması sebebiyle imha edilmelidir veya veri sahibine iade edilmelidir.[212]

İşlemenin sözleşmenin ifası için gerekli olmasına bir şirketin satış sözleşmenin ifası için müşterisine teslimat yapacağı adresi alması ve şirket kayıtlarına geçirmesi veya satıcı şirketin teslimatı yapacak kargo firmasına bu adresi ve müşterinin ismini vermesi örnek olarak verilebilir.

Diğer bir örnek de şudur: Sözleşmenin ifası için banka yoluyla para havale emri ile muhatap olan banka, havale emri veren kişiden bazı bilgilerinin işlenmesi ve üçüncü kişilere bildirilmesi hususunda rıza almak zorunda değildir. Sözleşmenin ifası için Tüzük'ün 6/1-b maddesindeki hukuka uygunluk sebebinden istifade ederek havale işlemini gerçekleştirebilir.[213]

[211]Develioğlu , 2017 , **a.g.k.** , 60.
[212]Develioğlu , 2017 , **a.g.k.** , 61.
[213]Selek , 2019 , **a.g.k.** , 934.

Kişisel veri işlemesi, veri sorumlusu için yasal bir zorunluluksa bu veri işlemesi hukuka uygundur.

Hukuki yükümlülüğün hukuka uygunluk sebebi olabilmesi için AB hukuku ve AB üyesi devletlerin mevzuatından doğması ve işlemenin bu mevzuatın amacına uygun olması ve veri sahibinin bu hukuki yükümlülüğe uyup uymamakta seçim hakkı olmaması gerekir.[214]

Veri sorumlusunun yasal sorumluluğunu ifa edebilmesi için mecburi olduğu veri işlemesine örnek olarak bir işverenin işçisine ait bilgileri sosyal güvenlik kurumuna bildirmesi gösterilebilir.

Yönerge'de sadece veri öznesinin hayati menfaatlerinin korunması şartıyla hukuka uygunluk sebebi sayılan; fakat hayati menfaatten kastedilenin ne olduğuna dair bir açıklama getirilmeyen bu koşulun Tüzük'te veri öznesi dışındaki ilgililerin hayati menfaatleri söz konusu olması halinde de hukuka uygunluk şartı olarak yer aldığı görülmektedir.

Hayati menfaatin yoruma açık bir kavram olduğu ortada olsa bile Tüzük'ün 29. maddesi uyarınca kurulan çalışma grubu, hayati menfaat kavramının dar yorumlanması gerektiği ve "*ölüm-kalım meseleleri ya da en azından yaralanma veya başka bir şekilde kişinin sağlığına zarar verme riski oluşturan tehdit halleri*" olarak sınırlı olarak tanımlanması gerektiği görüşünü ortaya koymuştur.[215]

Bu hukuka uygunluk sebebine örnek olarak ameliyat olması gereken, bilinci kapalı, kan kaybeden bir hastanın kan grubunun kayıt altına alınması gösterilebilir. Zira bu kişinin rızasının alınması mümkün olmasa bile kan grubunun bilinmesi hayati menfaati için önem teşkil etmektedir.

Sıhhi sebeplerle karantinaya alınmış bir bölgedeki kişilerin kimlik bilgilerinin yetkili makamlarca kayıt altına alınması da bu hukuka uygunluk sebebine örnek gösterilebilir.

Kişisel veri işlemesi, kamu yararı için gerçekleştirilen bir görevin ifası içinse veya veri sorumlusunun resmi yetkisinin kullanılması için gerekli ise hukuka uygundur.

---

[214]Develioğlu , 2017 , **a.g.k.** , 63.
[215]Yörük , 2019 , **a.g.k**. , 66.

Kamu yararı maksadıyla bir görevin yerine getirilmesi hukuki sorumluluğun yerine getirilmesinden daha geniş bir kavramdır. Bir veri sorumlusu, hukuki sorumluluğu olmamasına rağmen kamu yararı için gerçekleştirilen bir görevi ifa edebilir.

Tüzük, 'kamu yararı için gerçekleştirilen bir görevin ifası' hukuka uygunluk sebebinden yararlanma konusunda veri sorumlusunun kamu sektöründe olması şartını açıkça belirtmediğinden özel sektördeki bir veri sorumlusunun kamu menfaatini sağlamak maksadıyla ifa edilen bir vazife için yapacağı veri işlemelerinin de hukuka uygun olacağı söylenebilir.

Veri sorumlusu, kişisel veri işlemesini doğrudan yasanın kendisine verdiği bir yetki gereği yapmış olabileceği gibi resmi yetkisi olan üçüncü kişilerin yetkileri dahilinde de yapabilir. Her iki durumda da veri sorumlusunun veri işleme faaliyeti hukuka uygun olur. Doğrudan veri sorumlusunun yasadan aldığı yetkiyle yapmış olduğu veri işlemesine kamu kurumu niteliğindeki meslek kuruluşlarının, mesleki denetim yetkilerini kullanırken ya da yaptırımlar uygularken üyelerinin kişisel verilerini işlemesi örnek verilebileceği gibi veri sorumlusunun üçüncü kişilerin resmi yetkileri dahilinde veri işlemesine de veri öznelerinin kişisel verilerinin paylaşılmasını talep eden kamu kurumları ile bu bilgileri paylaşması örnek verilebilir.[216]

'Veri sorumlusunun resmi yetkisinin kullanılması için gerekli olması' hukuka uygunluk sebebine örnek olarak ceza soruşturması kapsamında telefonları dinlenen birinin görüştüğü kişilere ait bilgilere soruşturma dosyasında yer vermek veya bir vergi dairesinin, kamu alacağının tahsili amacıyla vergi borçlularının kişisel verilerini işlemesi örnek gösterilebilir.

İşlemenin meşru menfaatlere ulaşmak amacıyla gerekli olması Tüzük'te hukuka uygunluk sebebi olarak yer almıştır. Şöyle ki özellikle ilgili kişinin çocuk olduğu durumlarda ilgili kişinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hak ve özgürlükleri ağır basmadıkça veri sorumlusu veya üçüncü kişi tarafından hedeflenen meşru menfaatlere ulaşmak amacıyla gerekli olması durumunda veri işlemesi hukuka uygundur(M.6).

[216]Yörük , 2019 , **a.g.k**. , 67.

Örneğin bir avukatın müvekkiline ait alacağı tahsil etmesinde meşru bir menfaati vardır. Bu menfaate ulaşmak amacıyla borçlunun kişisel verilerini işlemesi, örneğin takip dosyasına borçluya ait isim ve adres bilgilerini girmesi hukuka uygundur.

Amaç ile menfaat kavramları aynı değildir. Amaç, kişisel veri işlemenin saiki; menfaat, kişisel veri işlemekten beklenen yarardır. Yukarıdaki örnekte kişisel veri işlemenin amacı alacağın tahsilidir. Menfaat ise avukatın avukat sözleşmesi gereği müvekkiline vekalet borcunu ifa etmesidir.

Eğer bu örnekte borçlunun menfaati avukatın menfaatinden üstünse avukatın borçluya ait kişisel verileri işlemesi hukuka uygun değildir. Zira ilgili kişinin baskın menfaatinin olması, veri sorumlusunun ve üçüncü kişinin meşru menfaati gereği yapılsa bile kişisel veri işlemesinin hukuka uygun olmasına engel teşkil eder.

Tüzük'e göre bu hukuka uygunluk sebebi, kamu kurumlarınca gerçekleştirilen işleme faaliyetleri yönünden de geçerli değildir. Yönerge'de ise bu şekilde bir sınırlamanın yapılmadığı görülmektedir.

Bilindiği üzere kişisel verinin elde edildiği amaçtan farklı bir amaçla işlenmesi yasaktır. Fakat tüzükte bu yasağa istisna getirilmiştir. Tüzük'ün 6/4 maddesine göre kural olarak kişisel verinin elde edilme amacından farklı sonraki bir amaçla işlenebilmesi için ilgili kişinin rızası gerekmektedir.

Eğer sonraki amaç, veriyi elde etme amacı ile uyumlu ise ilgili kişinin rızası olmasa bile bu veri işlemesi hukuka uygundur.

#### 2.14.5. Özel nitelikteki kişisel verilerin işlenmesi açısından hukuka uygunluk halleri (hassas verilerin işlenmesi)

Tüzük'ün 9/1 maddesi; "*Irksal veya etnik kökeni, siyasal görüşü, dini veya felsefi inanışları veya ticaret birliklerine üyeliğini ortaya koyan kişisel verilerin işlenmesi ve genetik verilerin, biyometrik verilerin bir gerçek kişiyi ayırdedici şekilde tanımlamak amacıyla ve sağlıkla ilgili verilerin veya bir gerçek kişinin cinsel hayatı veya cinsel tercihine ilişkin verilerin işlenmesi yasaktır*." şeklinde düzenlenmiştir.

Bu veriler, Tüzük tarafından özel nitelikte kişisel veri kategorisi olarak kabul edilmektedir.

Yönerge'nin aksine Tüzük'te genetik ve biyometrik verilerin özel nitelikte kişisel veri olduğu açıkça belirtilmiştir.[217] Fakat Tüzükte her genetik ve biyometrik verinin değil bir gerçek kişinin teşhisi için işlenen biyometrik ve genetik verilerin özel nitelikte olduğu belirtilmiştir.[218]

Tüzük, hassas (özel nitelikteki) verilerin işlenmesine koyduğu yasaklara yine 9. maddesinde istisnalar getirmiştir.[219] Şöyle ki;

a- Veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi durumunda özel nitelikteki kişisel veriler işlenebilir.

b- İş ve sosyal güvenlik hukuku kapsamındaki yükümlülüklerin ifası ve hakların kullanılması için özel nitelikteki kişisel veriler işlenebilir.

c- Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması durumunda hassas veriler işlenebilir. Örneğin komada olduğu için sağlık verilerinin işlenmesine rıza gösteremeyen kişinin hayati menfaatlerini korumak için gerekli olan işleme hukuka uygundur.[220] Bu açıdan Tüzük'ün hassas olmayan verilerin işlenmesinde aradığı[221] rızanın varlığını bile aramaya gerek yoktur.

d- Kar amacı taşımayan kuruluşlar meşru menfaatleri için üyelerine ait hassas verileri işleyebilir.

e- Veri sahibi tarafından alenileştirilen hassas kişisel veriler işleme faaliyetine konu olabilir. Örneğin kişinin cinsel tercihleriyle alakalı veriyi sosyal medyada kamuya açık bir profilden temin eden üçüncü bir kişinin bunu bir başkasına aktarması hukuka uygun bir veri işlemesidir.[222]

---

[217]Develioğlu , 2017, **a.g.k.** , 70.
[218]A. Boydak (2017). *İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış*. Türkiye Adalet Akademisi Dergisi, (30), 321-336, 327.
[219]Üzeltürk , 2018 , **a.g.k. ,** 165.
[220]Selek , 2019 , **a.g.k.** , 935.
[221]B. Orak(2019). *Kişisel Sağlık Verilerinin Korunması*. Yüksek Lisans Tezi. Ankara: Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü. 56.
https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi:13.04.2020)
[222]Selek , 2019 , **a.g.k.** , 936.

f- Yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde işleme faaliyetinin gerekmesi durumunda hassas veriler işlenebilir.

g- Bir hakkın tesisi, kullanılması veya korunması için gerekli ise hassas veriler işlenebilir.

h- Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Avrupa Birliği hukukuna veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına işleme faaliyetinin gerekmesi durumunda hassas veriler işlenebilir.

i- Bireysel ve kamusal sağlık hizmetlerinin sunulması kapsamında kamu yararının gerektirdiği durumlarda hassas veriler işlenebilir.

j- Kamunun yararı adına arşivleme, bilimsel ve tarihsel araştırma ve istatistiksel amaçlar için hassas verilerin işlenmesi hukuka uygundur.

Tüzük'ün 9. maddesine göre AB üyesi devletler; genetik, biyometrik ve sağlıkla ilgili verilerin işlenmesine ilişkin sınırlamalar getirebilir veya başka kurallar koyabilir.

Tüzük'ün 10. maddesine göre 6(1). madde uyarınca cezai hükümler ve suçlar ya da ilgili güvenlik tedbirleriyle alakalı kişisel verilerin işlenmesi ancak resmi makamın denetimi altında ya da ilgili kişinin hak ve özgürlüklerinin korunmasına yönelik uygun güvenceler öngören Birlik veya Üye Devlet hukukunca izin verildiği hallerde gerçekleştirilebilir. Cezai hükümlere ilişkin kapsamlı siciller sadece resmi makamın kontrolü altında tutulabilir.

### 2.14.6.Yurtdışına aktarım halinde hukuka uygunluk halleri

"Yurtdışına aktarım" kavramının, Tüzük'te açıkça tanımı yapılmamıştır. Fakat Tüzük'ün ilgili maddelerinden yurtdışına aktarımdan kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmanın kastedildiği anlaşılmaktadır.

Kişisel verilerin yurtdışına aktarımı için Tüzük'ün bir takım kurallar öngördüğü görülmektedir. Hukuka uygun bir yurtdışına aktarımın ilk şartı, kişisel verinin Tüzük'e uygun olarak elde edilmiş olması ve işleniyor olmasıdır.[223]

[223]Develioğlu , 2017 , **a.g.k.** , 73.

Tüzük'e göre yurtdışına aktarımın hukuka uygun olarak gerçekleşmesi iki şekilde mümkündür:

- Uygunluk Kararı Çerçevesinde Aktarım
- Uygunluk Kararı Bulunmayan Hallerde Aktarım

Uygunluk kararı çerçevesinde aktarımın düzenlendiği Tüzük'ün 45. maddesi uyarınca bir üçüncü ülkeye, üçüncü ülkedeki bir bölgeye ya da bir ya da daha fazla belirli sektöre veya milletlerarası kuruluşa aktarım, Komisyon'un söz konusu ilgili üçüncü ülkenin, üçüncü ülkedeki bir bölgenin ya da bir veya daha fazla belirli sektörün, uluslararası kuruluşun yeterli seviyede koruma sağladığına karar verdiği durumlarda gerçekleşebilir. İlgili aktarım için ayrıca izin aranmayacaktır.

Tüzük'ün yürürlükten kaldırdığı Yönerge'de, uygunluk kararı verme yetkisi hem üye devletlerde hem de AB Komisyonu'ndaydı. Tüzükle AB üyesi devletlerin uygunluk kararı verme yetkisi kaldırılmıştır.

AB komisyonu, uygunluk kararı alırken hukukun üstünlüğünü, temel hak ve özgürlüklerin koruma seviyesini, kişisel verileri koruma mevzuatının uygulanışını, bağımsız denetim organlarının mevcudiyetini ve işleyişini, aktarım yapılacak üçüncü ülke veya uluslararası kuruluşun kişisel verilerin korunması hususunda uluslararası anlaşmalarla ortaya koyduğu taahhütleri dikkate alır.

AB komisyonunun uygunluk veya uygun bulmama kararı güncel duruma göre geri alınabilir, değiştirilebilir, askıya alınabilir ve AB komisyonu, aktarımın yapılacağı üçüncü ülke veya uluslararası kuruluşlarla kişisel verilerin korunmasına dair mevcut durumun düzeltilmesi için görüşmeler yapabilir.

AB komisyonu, vermiş olduğu kararları en geç dört senede bir, tüm gelişmeleri de dikkate alarak gözden geçirmeli ve güncellemelidir.

AB komisyonu, kararlarına ait bir listeyi Avrupa Birliği resmi gazetesinde yayımlamaktadır.

Tüzük'ün 46. maddesine göre AB Komisyonu'nun uygunluk kararı olmadığı durumlarda veri sorumlusu veya veri işleyen, kişisel verileri yurtdışına

- veri sorumlusu veya veri işleyicisinin uygun tedbirler olması

- ilgili kişilerin hakları icra edilebilir nitelikte olması
- ilgili kişiler için etkili hukuksal çarelerin bulunması

şartlarının birlikte gerçekleşmesi şartıyla aktarabilir.

Kamu makamları arasındaki bağlayıcı ve icra edilebilir anlaşmalar, bağlayıcı kurumsal kurallar, standart veri koruması hükümleri, davranış kuralları ve sertifikasyon mekanizması uygun tedbirler olarak kabul edilir ve bunların varlığı halinde AB komisyonu tarafından verilecek bir uygunluk kararı aranmaz.

Tüzük'ün 4. maddesine göre işletmesi, bir üye devletin sınırları dahilinde bulunan bir veri işleyenin yahut veri sorumlusunun ortak bir ekonomik faaliyet içinde bir teşebbüsler birliği veya girişimler kapsamında bir veya daha fazla üçüncü ülkede bulunan bir veri sorumlusu veya veri işleyene kişisel veri aktarımları veya aktarım setleri için uydukları kişisel verilerin korunması politikaları olarak tanımlansa da bağlayıcı kurumsal kurallarla kastedilen, uluslararası grup şirketlerin farklı ülkelerde bulunan birimleri arasında yapılacak kişisel veri aktarımında öngördükleri kişisel verilerin korunması politikalarıdır. Standart veri koruması hükümleri, AB komisyonu tarafından hazırlanan veya bir denetim makamı tarafından hazırlanarak Avrupa Birliği Komisyonu tarafından onaylanan örnek sözleşme metinleri olup AB üye devletleri'nde ve üçüncü ülkelerde bulunan veri sorumluları veya veri işleyenler, yurtdışına veri aktarımlarında Tüzük'te aranan kişisel veri korumasının sağlanacağını bu sözleşmeler ile taahhüt edebilirler.[224]

Bağlayıcı kurumsal kurallar veya standart veri koruması hükümleri, veri sorumlularına Tüzük'ün aradığı veri koruma seviyesini sağlamak için öngördüğü yükümlülüklerini yerine getirmesini sözleşme yoluyla taahhüt etmesini ve veri sorumlularının bulundukları üçüncü ülkelere yönelik AB komisyonu tarafından verilen bir uygunluk kararı olmasa bile kişisel verilerin üçüncü ülkelerde bulunan veri sorumlularına aktarımını mümkün kılan hükümlerdir.[225]

Tüzük'e göre davranış kuralları; Tüzük'ün daha doğru uygulanmasına katkı sağlama amacı güden, farklı kişisel veri işleme sektörlerine özgü kurallar benimsenmesine imkan tanıyan, veri sorumlusu veya veri işleyen kategorilerini temsil

[224]Develioğlu , 2017 , **a.g.k.** , 76.
[225]Develioğlu , 2017 , **a.g.k.** , 77.

eden kuruluşlar tarafından farklı işleme sektörlerinin, mikro işletme ve kobilerin özellikleri dikkate alınarak hazırlanan, Tüzük'ün nasıl uygulanacağını daha belirgin kılan kurallardır(M.40). Davranış kurallarına uyulup uyulmadığının denetimi, Avrupa Veri Koruma Kurulu'nun görüşü alınarak yetkili denetim makamları tarafından akredite edilen uzman bir kuruluş tarafından yapılabilir(M.41).

Davranış kurallarına göre yapılacak yurtdışına veri aktarımlarında üçüncü ülkedeki veri sorumlusu veya veri işleyicisi uygun tedbirleri uygulayacağını taahhüt etmelidir.

Tüzük'ün 42. maddesine göre AB üyesi devletler, denetim makamları, Avrupa Veri Koruma Kurulu, AB Komisyonu; veri sorumlularının ve veri işleyenlerin işleme faaliyetlerinin Tüzük'e uygunluğunu göstermek amacıyla veri koruması sertifikasyon mekanizmalarının tesis edilmesini teşvik etmekle yükümlüdür. Sertifikasyon mekanizmasında sertifikasyon kuruluşları ve yetkili denetim makamları tarafından veri sorumlusu ve veri işleyenlere veri sorumluları ve veri işleyenlerin işleme faaliyetinin Tüzük'e uygun olduğunu göstermek amacıyla sertifikalar verilir. Sertifikalar gönüllülük esasıyla alınmalı ve sertifikasyon mekanizması şeffaf işlemelidir. Sertifikalar, 3 yıl geçerli olmak suretiyle verilir; fakat koşullara uyulması halinde geçerlilik süresi uzatılabilir. Sertifikalar, koşullara uyulmadığını tespit eden sertifika veren kuruluş ve denetim makamı tarafından veri sorumlusu ve veri işleyicisinden geri alınabilir.

Sertifikasyonlara dayanarak yapılan aktarımlarda da tıpkı davranış kurallarına dayanarak yapılan aktarımlarda olduğu gibi veri sorumlusu ve veri işleyen uygun tedbirleri uygulayacağını bağlayıcı ve icra edilebilir şekilde taahhüt etmelidir.

Veri sorumlusu veya veri işleyen ile üçüncü ülke veya uluslararası kuruluştaki veri sorumlusu, veri işleyen veya aktarılan arasındaki sözleşmesel hükümler ve kamu makamları ve kuruluşları arasındaki idari sözleşmelere eklenecek hükümlerin Avrupa Veri Koruma Kurulu'nun görüşünün alınmasının ardından yetkili denetim makamları tarafından onaylanması halinde de yurtdışına kişisel veri aktarımı gerçekleşebilir.

Tüzük'ün 48. maddesine göre bir üçüncü ülkede verilen, veri sorumlusunun ve işleyicisinin verileri aktarmasına ya da ifşa etmesine yönelik herhangi bir mahkeme, kurul veya idari makam kararı; ancak talepte bulunan üçüncü ülke ile AB veya AB

üyesi devlet arasında yürürlükte bulunan adli yardımlaşma anlaşması gibi uluslararası bir anlaşmaya dayanıyorsa tanınabilir veya tenfiz edilebilir.

Tüzük'ün 49. maddesinde düzenlenen yukarıdaki şartların bulunmadığı bazı durumlarda üçüncü bir ülkeye veya uluslararası kuruluşa veri aktarımının yapılabilmesinin mümkün olduğu istisnai haller şunlardır:

- İlgili kişinin AB komisyonu tarafından verilen bir uygunluk kararı veya uygun güvencelerin yokluğu sebebiyle veri aktarımının muhtemel riskleri hakkında bilgilendirildikten sonra veri aktarımına rıza göstermiş olması,
- Veri aktarımının ilgili kişi ve veri sorumlusu arasındaki aktin ifası yahut ilgili kişinin talebiyle akit evvelindeki tedbirlerin uygulanması için gerekli olması,
- Veri aktarımının veri sorumlusu ile diğer gerçek yahut tüzel kişi arasında, ilgili kişi menfaatine akit kurulması yahut ilgili yararına kurulan akitin ifası için gerekli olması,
- Veri aktarımının kamu menfaatiyle ilgili ehemmiyetli sebepler için lüzumlu olması,
- Veri aktarımının kanuni taleplerin tesisi, icrası yahut muhafazası için lüzumlu olması,
- Veri aktarımının fiziksel olarak veya hukuki olarak rıza gösterilmesinin mümkün olmadığı hallerde ilgili kişinin veya diğer kişilerin yaşamsal çıkarlarını muhafaza için lüzumlu olması,
- Veri aktarımının AB hukuku veya AB üyesi devlet hukuku uyarınca kamuya bilgi sağlamak amacı güden ve genel olarak kamunun ya da meşru menfaatleri olduğunu ispat edenlerin incelemesine açık olan bir sicilden ancak AB hukuku ya da AB üyesi devlet hukukunun incelemeye yönelik şartların yerine getirildiğinin ortaya konulduğu ölçüde yapılıyor olması.

### 2.14.7.Kişisel veri sahibinin hakları

Tüzük'ün bilgilendirme hakkının düzenlendiği maddesi şöyledir:

> MADDE 13/1- İlgili kişiye ait kişisel verilerin ilgili kişiden elde edildiği hallerde, veri sorumlusu, kişisel verilerin elde edildiği sırada, ilgili kişiye aşağıdaki bilgileri sağlar:

a.Veri sorumlusunun veya ilgili hallerde veri sorumlusunun temsilcisinin kimliği ve iletişim bilgileri;

b. İlgili hallerde, bilgi güvenliği yetkilisinin iletişim bilgileri;

c. Kişisel verilerin işlenmesinde hedeflenen amaçlar ve işlemenin hukuki dayanağı;

d. işlemenin 6(1). maddenin (f) bendine dayandığı hallerde, veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatler;

e. varsa, kişisel verilerin aktarılanları veya aktarılan kategorileri;

f. ilgili hallerde, veri sorumlusunun kişisel verileri bir üçüncü ülkeye veya uluslararası kuruluşa aktarma niyeti olduğu ve Komisyon'un uygunluk kararı olup olmadığı veya 46, 47 ya da 49(1). maddenin 2. alt fıkrası kapsamındaki aktarımlarda, uygun veya münasip güvencelere ve bunların bir kopyasının ne şekilde elde edilebileceğine veya nerede erişime sunulduğuna dair bilgi.

İlgili kişi, Tüzük'ün 13. maddesinde öngörülen bilgilere sahipse veri sorumlusu tarafından ilgili kişiye tekrar bir bilgi verilmesine gerek yoktur.

Tüzük'ün 14. maddesinde kişisel verilerin ilgili kişiden temin edilememesi durumunda veri sorumlusunun ilgili kişiye sağlaması gereken bilgiler düzenlenmiştir. Bu bilgiler Tüzük'ün 13. maddesi ile örtüşmekte olup sadece Tüzük'ün 14. maddesinde ilgili kişiye sağlanması gereken bilgiler arasında kişisel verilerin aktarıldığı kişi ve kişi kategorilerine yer verilmediği, bunun yerine kişisel veri kategorilerine yer verildiği görülmektedir.

Kişisel verilerin ilgili kişiden doğrudan elde edilemediği durumlarda veri sorumlusu, Tüzük'e göre ilgili kişiyle paylaşması gereken bilgileri verileri elde ettikten sonra bir ayı geçmemek şartıyla makul süre içinde ilgili kişiye verir. Kişisel verilerin ilgiliyle iletişim kurmak için kullanılması halinde iletişimin ilk anında ilgili kişiye bu bilgiler verilmelidir. Kişisel veriler üçüncü bir aktarılana açıklandığı durumlarda ilk açıklama sırasında ilgili kişiye gerekli bilgiler verilir.

Veri sahibi, kişisel verilere erişme hakkına sahiptir. Kişisel veri sahibinin aşağıda bahsedeceğimiz düzeltme, silme(unutulma), işlemi sınırlama, veri taşınabilirliği, itiraz, otomatik münferit karar verme haklarını kullanabilmesi için öncelikle kişisel verilere erişme hakkı tesis edilmelidir. Kişisel verilerine erişemeyen bir kişisel veri sahibinin diğer haklarını kullanması mümkün değildir.

Tüzük'ün 15. maddesi uyarınca ilgili kişi, veri sorumlusundan kişisel verilerinin işlenip işlenmediğine teyitte bulunmasını ve kişisel verileri işleniyorsa söz konusu kişisel verilere ve aşağıdaki bilgilere erişmeyi talep etme hakkına sahiptir:

(a)işlemenin amaçları,

(b)ilgili kişisel veri kategorileri,

(c)kişisel verilerin ifşa edildiği veya edileceği, özellikle bir üçüncü ülke veya uluslararası kuruluşta bulunan aktarılanlar veya aktarılan kategorileri,

(d)mümkün olan hallerde, kişisel verilerin saklanacağı öngörülen süre, bu mümkün değilse, bu sürenin nasıl belirleneceğine ilişkin kriterler,

(e) veri sorumlusundan kişisel verilerin düzeltilmesini veya silinmesini, ilgili kişiyle alakalı işlemenin sınırlandırılmasını talep etme veya işlemeye itiraz etme hakkının varlığı,

(f)denetim makamına şikayette bulunma hakkı,

(g)kişisel verilerin ilgili kişiden elde edilmediği hallerde, verilerin kaynağına ilişkin tüm mevcut bilgiler,

(h)profilleme dahil olmak üzere otomatikleştirilmiş karar vermenin uygulandığı ve bu hallerde asgari olarak uygulamanın mantığına dair anlamlı bilgiler ve işlemenin önemi ve bu işlemenin ilgili kişi bakımından sonuçları.

Tüzük'ün 15/2 maddesine göre AB Komisyonu'nun uygunluk kararı olmadan yurtdışına aktarım halinde ilgili kişi aktarmaya ilişkin alınan uygun tedbirler hakkında bilgi edinme hakkına sahiptir.

Tüzük'ün 15/3 maddesine göre veri sorumlusu, işlenmekte olan kişisel verilerin bir kopyasını sağlamalıdır. Fakat bu kopya elde etme hakkı, başkalarının hak ve özgürlüklerini olumsuz şekilde etkileyemez. Birden fazla kopya talep edilirse veri sorumlusu makul ücret talep edebilir. İlgili kişinin elektronik vasıtalarla talepte bulunduğu hallerde ve ilgili kişi aksini talep etmedikçe bilgi elektronik yolla sağlanır.

Düzeltme hakkı Tüzük'ün 16. maddesinde düzenlenmiştir. Buna göre ilgili, veri sorumlusundan maddi hata barındıran, yanlış olan kişisel verilerin gecikmeksizin

düzeltilmesini isteyebilir. İlgili kişi, işlemenin amaçları dikkate alındığında ek beyanda bulunmak suretiyle de olmak üzere eksik kişisel verinin tamamlanması hakkına sahiptir.

Verinin doğru ve güncel olması olarak açıklanabilecek olan doğruluk ilkesinin sağlanması açısından veri öznesine sağlanan düzeltme hakkının önemi büyüktür. Yukarıda veri sorumlularının yükümlülüklerinden bahsedilirken değinildiği üzere düzeltme, veri öznesi açısından bir hak olduğu gibi veri sorumlusu açısından da bir yükümlülüktür.

Tüzük'ün 19. maddesine göre veri sorumluları, mümkünse veya orantısız bir gayret gerektirmeyecekse kişisel verilerin düzeltildiği hususunda kişisel verileri açıkladığı her alıcıyı bilgilendirmek ve veri sorumlusunu bu alıcılar hakkında bilgilendirmek zorundadır.

Tüzük'te düzenlenen silinmeyi talep hakkının(unutulma hakkı) daha önce Yönerge'de düzenlendiği görülmektedir. 95/46 EC sayılı Yönerge başlığı altında da açıkladığımız üzere silinmeyi talep hakkının kökeninde Fransız hukuku kaynaklı unutulma hakkının olduğu doktrindeki esaslı görüştür. Unutulma hakkı kapsamında ilgili kişi kendisini utandıran bilgileri bu bilgiler doğru olsa bile silmeyi talep edebilir.

Yönerge'de unutulma hakkına ilişkin münferit bir düzenleme bulunmamaktaydı. Veri öznesinin erişim hakkının düzenlendiği 12. maddede özellikle verinin eksik veya doğru olmaması gibi *Yönerge* hükümlerine aykırı hallerde veri öznesinin veri sorumlusundan işlenen verilerin düzeltilmesi, silinmesi veya engellenmesi talebinde bulunabileceği hususu yer almaktaydı. Tüzük öncesi unutulma hakkına ilişkin istekler genellikle bu düzenleme esas alınarak karşılanmaktaydı.[226]

ABAD'ın unutulma hakkı ile ilgili olarak vermiş olduğu *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez* kararında başvurucunun Google arama motorundan silinmesini istediği verilerin silinmesinin gerekliliği değerlendirilmiştir. Üstelik ABAD, silinmesi gereken

[226]T. Soysal (2019). *Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi*. Uyuşmazlık Mahkemesi Dergisi, 0 (13), 339-422, 364.

verinin doğru olup olmadığının veya ilgili kişiyi mağdur edip etmediğinin önemsiz olduğunu belirtmiştir.[227]

Bu kararın ardından Tüzük'te silinmeyi talep hakkı daha detaylı düzenlenmiştir. Dolayısıyla Tüzük'te unutulma hakkının düzenlenmesinde AB Adalet Divanı'nın bu kararının etkili olduğu söylenebilir.

> MADDE 17-1.İlgili kişi, veri sorumlusunun, kendisine ait kişisel verilerin gecikmeden silmesini sağlamak hakkına sahiptir ve veri sorumlusu aşağıdaki hallerden birinin varlığında gecikmeden kişisel verileri silme yükümlülüğü altındadır:
>
> (a)kişisel verilerin elde edildikleri veya başka surette işlendikleri amaçla ilgili olarak artık gerekli olmaması;
>
> (b)işlemenin 6(1). maddenin (a) bendine veya 9(2). maddenin (a) bendine dayandığı hallerde, ilgili kişinin rızasını geri çekmesi ve işleme için başka bir yasal dayanak olmaması;
>
> (c)ilgili kişinin, 21(1). madde uyarınca işlemeye itiraz etmesi ve işleme için baskın çıkan meşru menfaatlerin bulunmaması veya ilgili kişinin 21(2). madde uyarınca işlemeye itiraz etmesi;
>
> (d)kişisel verilerin hukuka aykırı surette işlenmiş olması;
>
> (e)kişisel verilerin Birlik veya veri sorumlusunun tabi olduğu Üye Devlet hukukundan kaynaklanan hukuki bir yükümlülüğe uymak için silinmesi gerekiyorsa,
>
> (f)kişisel veriler 8(1). maddede belirtilen bilgi toplumu hizmetlerinin sunulması ile bağlantılı olarak elde edildiyse.
>
> 2. Veri sorumlusu, kişisel veriyi kamuya açıkladığı ve 1. fıkra uyarınca silmesi gereken hallerde, veri sorumlusu mevcut teknolojiyi ve uygulama masraflarını dikkate alarak, teknik tedbirler dahil olmak üzere, ilgili kişinin kişisel veriyi işleyen veri sorumlularının söz konusu kişisel verilerin bağlantı veya kopya veya nüshalarını silmesini istediği yönünde bu veri sorumlularını bilgilendirmek için tüm makul adımları atar.
>
> 3. 1. ve 2. fıkralar işlemenin şu hallerden biri için gerekli olduğu ölçüde uygulanmaz:

[227]Develioğlu , 2017 , **a.g.k.** , 89-90.
ABAD. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. 13/05/2014, 131/12
https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:62012CJ0131_SUM&qid=1579769680599&from=EN (Erişim Tarihi:25.03.2020)

(a) ifade ve bilgi alma özgürlüklerinin kullanılması;

(b) Birlik veya veri sorumlusunun tabi olduğu Üye Devlet hukuku uyarınca işlemenin gerekli olduğu hukuki bir yükümlülüğe uymak veya kamu yararı için gerçekleştirilen bir görevin ifası veya veri sorumlusunun resmi yetkisinin kullanılması;

(c) 9(2). maddenin (h) ve (i) bentleri ile 9(3). maddeye uygun olarak kamu sağlığı alanında kamu yararı sebebiyle;

(d)1. fıkradaki hakkın kullanılması, bu işlemenin amacına ulaşmasını imkansız kılacak veya ciddi şekilde engelleyecek ise, 89(1). madde uyarınca kamu yararı için arşivleme amacı, bilimsel veya tarihi araştırma veya istatistiksel amaçla,

(e) yasal hakların tesisi, kullanılması veya korunması için.

Veri sorumlusu, silinmesi istenen kişisel verileri kamuya açıklamışsa bu veriyi işleyen diğer veri sorumlularını da ilgili kişinin silinme hakkını kullandığından haberdar etmelidir. Yönerge'deki silinmeyi talep hakkı ile Tüzük'teki unutulma hakkının farkının bu haberdar etme yükümlülüğü olduğu ifade edilmektedir.[228]Çünkü tam anlamıyla unutulma hakkının tesis edilmesi için verinin yayıldığı tüm veri sorumlularının kişisel veriyi silmeleri gerekmektedir.

Tüzük'te işlemenin sınırlandırılmasının tanımı "*depolanan kişisel verilerin, gelecekte işlenmelerinin sınırlandırılması amacıyla işaretlenmesi*" şeklinde yapılmıştır (M.4) Diğer bir deyişle bu hakkın kullanılması neticesinde işaretlenen kişisel veriler bir süre işlenemeyecek, akıbetlerine göre bir hareket sergilenecektir.[229]

MADDE 18-1.İlgili kişi aşağıdaki hallerde veri sorumlusundan işlemenin sınırlandırılmasını sağlama hakkına sahiptir:

(a)ilgili kişi, kişisel verilerinin doğruluğuna itiraz ederse, veri sorumlusunun kişisel verilerin doğruluğunu teyit etmesine elverişli bir süre için,

(b)işleme hukuka aykırı ise ve ilgili kişi verilerin silinmesine itiraz eder ve bunun yerine kullanımlarının sınırlandırılmasını talep ederse,

(c)veri sorumlusu işlemenin amacı bakımından kişisel verilere artık ihtiyaç duymuyorsa, ancak kişisel veriler yasal hakların tesisi, kullanılması veya korunması için ilgili kişi tarafından talep edilirse,

[228]Develioğlu , 2017 , **a.g.k.** , 91.
[229]Develioğlu , 2017 , **a.g.k.** , 93.

(d)ilgili kişinin 21(1). madde uyarınca işlemeye itiraz ettiği hallerde, veri sorumlusunun meşru menfaatlerinin ilgili kişininkinden baskın olup olmadığı tayin edilene kadar.

Yukarıda sayılan işlemenin sınırlandırılacağı hallerde, kişisel verilerin depolanması haricinde, ilgili kişisel veriler, sadece;

- İlgili kişinin rızası ile,
- Yasal hakların tesisi, kullanılması veya korunması için,
- Başka bir gerçek veya tüzel kişinin haklarının korunması için,
- AB'nin veya AB üyesi devletin önemli kamu yararı için

işlenebilir(M.18/2).

Yukarıda sayılan işlemenin sınırlandırılacağı hallerde, kişisel verilerinin işlenmesinin sınırlandırılmasını sağlayan ilgili kişi bu sınırlama kaldırılmadan önce veri sorumlusu tarafından haberdar edilir(M.18/3).

Tüzük'ün 19. maddesi uyarınca veri sorumlusu, her türlü kişisel verilerin silinmesi, düzeltilmesi veya işlemenin sınırlandırılması halini kişisel veriler kendisine ifşa edilmiş olan her bir aktarılana haber vermekle yükümlüdür. İlgili kişinin talebi halinde veri sorumlusu ilgili kişiyi aktarılanlar hakkında bilgilendirir.

Veri taşınabilirliği hakkı, unutulma hakkında olduğu gibi Yönerge'de düzenlenmeyip ilk defa Tüzük'te koruma altına alınan iki haktan biridir.

Tüzük'ün 20. maddesine göre işlemenin

- bir rızaya dayandığı,
- bir aktin kurulması veya ifası için lüzumlu olduğu,
- otomatik usullerle gerçekleştirildiği,

durumlarda ilgili kişinin, veri sorumlusuna temin ettiği kişisel verilerini, biçimlendirilmiş, genel olarak kullanılan ve makine tarafından okunabilen bir formatta talep etme ve bu kişisel verileri sağladığı ilk veri sorumlusunun engellemesi ile karşılaşmadan başka bir veri sorumlusuna aktarma hakkı vardır(M.20/1).

Tüzük'te, veri taşınabilirliği hakkının düzenlenmesindeki amaç, çevrimiçi hizmetlerden yararlanan kişilerin sağladıkları kişisel verileri diğer bir hizmet

sağlayıcına aktarabilmelerini mümkün kılarak ilgili kişiyi kişisel verilerini aktaramadığından dolayı memnun olmadığı bir hizmet sağlayıcısına mahkum etmemektir[230].Örneğin, bir e-posta kutusu sağlayıcısı aracılığıyla e-posta hesabı açan kişi, bu hesaba gelen e-postaların başka bir e-posta sağlayıcısına geçebilmesini sağlayabilmelidir.[231] Böylece kişisel veriler üzerinde ilgili kişinin hakimiyetinin artması sağlanmış olsa da bu hakkın kullanılması veri sorumlusunun daha fazla masraf altına girmesine de sebep olabilir.[232]

Veri taşınabilirliği hakkının kullanılması silinme hakkının (unutulma hakkı) kullanılmasına engel teşkil etmez. Fakat veri taşınabilirliği hakkı, kamu menfaatini sağlamak için yapılan bir vazifenin ifası ya da veri sorumlusuna verilmiş resmi bir yetkinin kullanılması için lüzumlu olan işlemelere uygulanmaz(M.20/3).

Veri taşınabilirliği hakkı, başkalarının hak ve özgürlüklerini olumsuz olarak etkileyemez(M.20/4).

Tüzük'ün 21. maddesine göre;

- Kişisel veri işlemesinin kamu menfaati için ifa edilen görev için lüzumlu olması,
- Kişisel veri işlemesinin veri kontrolörünün resmi yetkisinin icrası için lüzumlu olması,
- Özellikle ilgili kişinin çocuk olduğu durumlarda, ilgilinin kişisel verilerinin muhafazasını icabettiren yararları, temel hakları, özgürlükleri baskın olmadıkça, kişisel veri işlemesinin veri kontrolörü yahut üçüncü kişi tarafından hedeflenen meşru menfaatlere ulaşmakta lüzumlu olması

durumlarında veri sahibi, verilerinin işlenmesine itiraz edebilir. Bu gibi durumlarda;

---

[230]Van Der Auwermeulen, Barbara, How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations, Computer Law & Security Review, 33, 2017, s.74; Hornung, Gerrit, A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft of 25 January 2012, SCRIPTed, 9, 2012, s.74'den aktaran Develioğlu, 2017, **a.g.k.**, 95.
[231]Develioğlu , 2017 , **a.g.k.** , 95 vd.
[232]Safarı, Beata A., Intangible Privacy Rights; How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, Seton Hall Law Review, 47, 2017, s.829-830'dan aktaran Develioğlu , 2017 , **a.g.k.** , 96.

- kişisel veri işlemesinin ilgilinin menfaatlerine, haklarına, özgürlüklerine ağır basan kanuni dayanaklarının mevcudiyetini,
- kişisel veri işlemesinin kanuni hakların kurulması, icrası yahut muhafazası açısından lüzumlu olmasını

ispatlamadıkça veri sorumlusu kişisel verileri işlemeyi sürdüremez.

Doğrudan pazarlama maksadıyla yapılan kişisel veri işlemelerinde her şartta eğer ilgili kişi işlemeye itiraz ederse veri sorumlusu işleme faaliyetini durdurmak zorundadır. Böyle durumlarda veri sorumlusu, kişisel veri işlemesinin ilgilinin menfaatlerine, haklarına, özgürlüklerine ağır basan kanuni dayanaklarının mevcudiyetini, kişisel veri işlemesinin yasal hakların kurulması, kullanılması yahut muhafazası için lüzumlu olduğunu ispatlasa bile ilgili kişi itiraz etmişse veri işlemeye devam edemez.

Kişisel verilerinin işlenmesine itiraz hakkı olduğu en geç ilgili kişi ile gerçekleştirilen ilk haberleşme sırasında açık şekilde ilgili kişinin dikkatine sunulmalıdır.

Tüzük'ün veri sahibinin verilerin işlenmesine itiraz hakkı vermesinin ve itiraz sonucu verilerin işlenmesinin durdurulmasına karar verilmesinin; verilerin işlenmesine itiraz hakkının düzenlendiği 21. maddenin 17.maddede düzenlenen unutulma/silme hakkını kuvvetlendirici, destekleyici bir tesire sebep olacağı göz ardı edilmemelidir.[233]

Münferit hareket etme hakkı, Tüzük'ün 22. maddesinde düzenlenmiştir:

> MADDE 22/1-İlgili kişi, profilleme dahil olmak üzere, sadece otomatik işleme dayanan ve kendisi hakkında hukuki sonuçlar doğuran veya onu benzer surette önemli ölçüde etkileyen bir karara konu olmama hakkına sahiptir.

Fakat bu karar, taraflarını veri sorumlusu ve ilgili kişinin oluşturduğu sözleşmenin kurulması yahut uygulanması için gerekliyse bu kararın alınmasına AB veya veri sorumlusunun tabi olduğu AB üyesi devlet hukukunca izin verilmişse ve ilgili kişinin haklarını, özgürlüklerini, meşru menfaatlerini korumaya uygun tedbirler öngörülmüşse; bu karar ilgili kişinin açık rızasına dayanıyorsa ilgili karara tabi olmama hakkı kullanılamaz.

[233]Soysal , 2019, **a.g.k.** , 367.

Kararın ilgili kişi ve veri sorumlusu arasında bir sözleşme kurulması için gerekli olduğu veya ilgili kişinin açık rızasına dayandığı hallerde veri sorumlusu ilgili kişinin hak ve özgürlüklerini, meşru menfaatlerini korumaya uygun tedbirleri almalı; en azından ilgili kişiye veri sorumlusu nezdinde bir insan tarafından müdahale edilmesini sağlama, kendi görüşünü belirtme ve karara itiraz etme hakkı tanımalıdır.

Bir denetim makamına şikayet hakkı, Tüzük'ün 77. maddesinde düzenleme altına alınmıştır.

> **MADDE 77-**1.Diğer idari ve yasal çarelere halel gelmemek üzere, her ilgili kişi kendisiyle ilgili kişisel verilerin işlenmesinin bu Tüzük'ü ihlal ettiğini düşünüyorsa, olağan yerleşim yeri, işyeri veya ihlalin gerçekleştiği iddia edilen yer denetim makamına şikayette bulunmak hakkına sahiptir.
>
> 2.Şikayetin yapıldığı denetim makamı, şikayette bulunanı şikayetin durumu ve 78. madde uyarınca yasal çarelere başvurma imkanı dahil olmak üzere sonucu konusunda bilgilendirir.

Tüzük, veri öznelerine denetim makamının kendileri hakkındaki bağlayıcı kararlarına karşı veya Tüzük'e aykırı veri işlemesi yapan veri sorumluları ve veri işleyicilerine karşı kanun yoluna başvurma hakkı tanımıştır. Tüzük, denetim makamının bağlayıcı kararlarına karşı başvuru hakkını 78. maddesinde; veri sorumlusu veya veri işleyicilerine karşı kanun yolunu ise 79. maddesinde düzenlemiştir.

Tüzük'ün 78/1 maddesine göre;**"** İdari ve diğer yargı dışı mevcut çarelere halel gelmemek üzere, her gerçek veya tüzel kişi, denetim makamının kendisi hakkındaki hukuken bağlayıcı kararlarına karşı etkin yasal çarelere başvurma hakkına sahiptir."

Bu kanun yolu başvurusu, denetim makamının bağlı olduğu AB üyesi devletin mahkemelerine yapılır.

Tüzük'ün 79. maddesine göre veri özneleri, Tüzük'e aykırı veri işlemesi sebebiyle Tüzük'ün koruma altına aldığı haklarının ihlal edildiğini düşünüyorsa veri sorumlusu ve veri işleyicilere karşı veri işleyici veya veri sorumlusunun bulunduğu AB üyesi devletin mahkemelerine kanun yolu başvurusu yapabilir. Veri sorumlusu veya veri işleyicinin kamu gücünü kullanan AB üyesi bir devlet kurumu olmadığı durumlarda veri öznesi, mutad yerleşim yerinin bulunduğu AB üyesi devlet mahkemelerine de başvuru yapabilir.

### 2.14.8.Veri sorumlularının yükümlülükleri

Veri sorumlularının yükümlülükleri Tüzük'ün 13 ila 22. maddelerinde düzenlenmiştir.

Tüzük'ün 27. maddesine göre, Tüzük'ün 3. maddesinin 2. fıkrasının icra edildiği durumlarda veri sorumlusu yahut veri işleyen yazılı şekilde AB dahilinde bir temsilci atamakla yükümlüdür.

Tüzük'ün 3/2 maddesi şöyle düzenlenmiştir:

> "Bu tüzük, birlik dahilindeki ilgili kişilerin kişisel verilerinin Birlik dahilinde işletmesi bulunmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesi halinde, işleme faaliyetlerinin;
>
> (a)ilgili kişiden bir ödeme istenip istenmediğine bakılmaksızın, Birlik dahilinde bulunan ilgili kişilere mal veya hizmet sunulmasına,
>
> (b)birlik dahilinde gerçekleşen davranışlarının gözlenmesine,
>
> İlişkin olması halinde uygulanır."

Veri sorumlusu ve veri işleyenin temsilci atama yükümlülüğü, işlemenin geçici olduğu ve özel nitelikli kişisel verilerin geniş ölçekli olarak işlenmesinin söz konusu olmadığı hallerde işlemenin niteliği de dikkate alınarak gerçek kişilerin hak ve özgürlüklerinin zarar görmesi muhtemel olmayan işlemelere veya kamu kurum ve kuruluşlarına uygulanmaz.

Temsilcinin işletmesi, mal veya hizmet sunulması veya davranışlarının gözlemlenmesi ile ilgili olarak kişisel verileri işlenen ilgili kişilerin bulunduğu AB üyesi devletlerden birinde bulunmalıdır.

İşlemeyle ilgili her konuda Tüzük'e uygun hareket edilmesinin sağlanması konusunda denetim makamları ve ilgili kişiler karşısında muhatap olmak üzere veri sorumlusu veya veri işleyen tarafından temsilcinin yetkilendirilmiş olması gerekir.

Veri sorumlusu veya veri işleyen tarafından temsilci atanması veri sorumlusunun veya veri işleyenin kendisine karşı yasal yollara başvurulmasını engellemez.

Tüzük'te Yönerge'den farklı olarak veri sorumlusunun tedbir almak yükümlülüğüne ilişkin kurallardan ziyade veri sorumluları ve veri işleyenler için bir uyum programının düzenlendiği belirtilmektedir.[234]

Tüzük'ün 24. maddesine göre veri sorumlusu; işlemenin tabiatı, muhteviyatı, bağlamı ve maksatları ile gerçek kişilerin hakları, özgürlükleri bakımından farklı olasılık ve önemde riskleri dikkate alarak işlemenin bu Tüzük'e uygun şekilde gerçekleştirilmesini sağlamak ve bunu ortaya koyabilmek için uygun teknik ve organizasyonel tedbirleri almakla yükümlüdür. İşleme faaliyetleri ile orantılı olduğu hallerde bu tedbirler, veri sorumlusu tarafından uygun kişisel verilerin korunması politikaları uygulamasını da kapsar. Bu hükmün veri sorumlularının alacakları tedbiri belirlemekte serbest bıraktığı yönünde değerlendirmeler mevcuttur.[235]

Ayrıca Tüzük'e göre onaylanmış davranış kurallarına veya onaylanmış sertifikasyon mekanizmalarına bağlılık, veri sorumlusunun yükümlülüklerine uyduğunu ortaya koymak için bir unsur olarak kullanılabilir.

Tüzük'ün 25. maddesine göre veri sorumlusu; tekniğin vaziyeti, uygulama maliyeti; işlemenin tabiatı, kapsamı, bağlamı, maksatları; gerçek kişilerin hak ve özgürlükleri bakımından farklı olasılık ve önemdeki riskleri dikkate alarak veri sınırlandırılması gibi veri koruma kurallarını uygulamak için tasarlanmış psödeonimleştirme[236] gibi uygun teknik ve organizasyonel tedbirleri hem işleme vasıtalarının belirlenmesi hem de işleme sırasında etkin şekilde tesis etmelidir ve Tüzük'ün şartlarını yerine getirmek ve ilgili kişilerin haklarını korumak için gerekli tedbirleri veri işlemesinin parçası haline getirmelidir.

Yine Tüzük'ün 25. maddesine göre veri sorumlusu, sadece işlemenin belirli amacı için gerekli kişisel verilerin işlenmesinin başlangıçtan itibaren esas olmasını temin etmek için elverişli teknik ve organizasyonel önlemleri almalıdır. Bu mükellefiyet,

---

[234]Imperıalı, Rosario, The Data Protection Compliance Program, Journal of International Commercial Law& Technology, 7, 2012'den aktaran Develioğlu , 2017 , **a.g.k.** , 100.

[235]De Hert, Paul/ Papakonstantınou, Vagelis, Three Scenarios for International Governance of Data Privacy:Towards and International Data Privacy Organization, Preferably a UN Agency, I/S: A Journal of Law and Policy fort he Information Society,9,2013, s.271 vd'den aktaran Develioğlu , 2017 , **a.g.k.** , 101.

[236]Tüzük'ün 'tanımlar' başlıklı 4. maddesinde psödonimleştirme, ek bilgilerin ayrı olarak saklanması ve belirli veya belirlenebilir bir gerçek kişiye atfedilememesini sağlamaya yönelik ve teknik ve organizasyonel tedbirlere tabi olması şartıyla, kişisel verilerin, ek bilgiler olmadan belirli bir kişiye atfedilemeyeceği şekilde işlenmesi olarak tanımlanmıştır.

toplanan verilerin niceliği, işlenme boyutu, saklama müddeti, erişilebilirlikleri açısından da uygulanır. Bu tedbirler, özellikle bireyin müdahalesi olmadan kişisel verilerin belirsiz sayıda gerçek kişiye açık olmamasını temin etmelidir.

Müşterek veri sorumlularının işbölümü anlaşması yapma yükümlülüğü Tüzük'ün 26. maddesinde düzenlenmiştir.

Tüzük'ün 26. maddesine göre iki veya daha fazla veri sorumlusu işleme amaçlarını ve yollarını müşterek olarak belirlerlerse bu veri sorumluları müşterek veri sorumlusu olurlar.

AB veya veri sorumlularının tabi olduğu üye devlet hukuku tarafından belirlenmiş olmadıkça müşterek veri sorumluları, özellikle ilgili kişilerin haklarının kullanılması ve bilgi sağlama yükümlülüklerine ilişkin olarak bu Tüzük'e uygun davranmaları için her birinin yükümlülüklerini şeffaf bir şekilde belirlerler.

Bu anlaşma, ilgili kişiler karşısında her bir müşterek veri sorumlusunun görevlerini ve aralarındaki ilişkiyi tam olarak yansıtmalıdır. Anlaşmanın esası ilgili kişilerin erişimine açık olmalıdır.

Anlaşmanın hükümlerinden bağımsız olarak ilgili kişi, Tüzük'ten kaynaklanan haklarını müşterek veri sorumlularından herhangi birine karşı ileri sürebilir.

Veri sorumlusunun veri işleyenlerin seçimi ile ilgili yükümlülükleri de vardır. Tüzük'ün 28.maddesine göre veri sorumlusu, sadece Tüzük'ün gereklerini karşılayabilecek ve ilgili kişilerin hakkını koruyabilecek tedbirleri uygulama konusunda yeterlilik gösterebilecek veri işleyenleri kullanmalıdır.

Veri sorumlusunun genel veya özel izni olmadıkça veri işleyen başka bir veri işleyen kullanamaz. Fakat veri sorumlusunun genel bir izin vermiş olduğu durumlarda veri işleyen kendi yerine veya kendi yanında bir veri işleyicisi görevlendirme niyetini veri sorumlusuna bildirirse başka bir veri işleyicisi kullanabilir.

Veri işleyen tarafından gerçekleştirilecek veri işlemeleri, AB veya AB üyesi devlet hukukuna tabi olan, veri sorumlusu karşısında veri işleyeni bağlayan ve işlemenin konusu ve süresini, işlemenin tabiatını ve amacını, kişisel verilerin türünü,

ilgili kişilerin kategorilerini ve veri sorumlusunun yükümlülüklerini ve haklarını içeren bir sözleşme veya diğer bir hukuki işleme tabi olmalıdır.

Veri işleyen, yurtdışına aktarım da dahil olmak üzere veri sorumlusunun belgelendirebileceği talimatlarına aykırı bir veri işlemesi yapamaz.

Tüzük'ün 30. maddesine göre veri sorumluları ve temsilcileri, sorumlulukları kapsamındaki işleme faaliyetlerinin ve aldıkları önlemlerin kaydını tutmalıdır.

> MADDE 30-1.Her bir veri sorumlusu ve ilgili hallerde veri sorumlusunun temsilcisi, sorumlu oldukları işleme faaliyetlerinin kaydını tutar. Bu kayıt en azından şu bilgileri içermelidir:
>
> (a)veri sorumlusunun ve ilgili hallerde müteselsil veri sorumlusunun, veri sorumlusunun temsilcisinin ve bilgi güvenliği yetkilisinin kimliği ve iletişim bilgileri;
>
> (b)işlemenin amaçları;
>
> (c) ilgili kişi kategorilerinin ve kişisel veri kategorilerinin açıklaması;
>
> (d)bir üçüncü ülke veya uluslararası kuruluştaki aktarılanlar dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı aktarılan kategorileri;
>
> (e) ilgili hallerde, hangi üçüncü ülke veya uluslararası kuruluş olduğu da belirtilerek, bir üçüncü ülkeye veya uluslararası kuruluşa yapılan aktarımlar ve 49(1). Maddenin ikinci alt fıkrası kapsamındaki aktarımlarda, uygun tedbirlere ilişkin dökümantasyon;
>
> (f)mümkün olan hallerde, farklı veri kategorilerinin silinmesi için öngörülen süre kısıtlamaları;
>
> (g)mümkün olan hallerde, 32(1). maddede belirtilen teknik ve organizasyonel tedbirlerin genel bir açıklaması.
>
> 2.Her bir veri işleyen ve ilgili hallerde veri işleyenin temsilcisi, veri sorumlusu adına gerçekleştirilen tüm işleme faaliyeti kategorilerine ait aşağıdakileri içeren bir kayıt tutar:
>
> (a)veri işleyenin veya veri işleyenlerin ve veri işleyenin adına hareket ettiği her bir veri sorumlusunun ve ilgili hallerde veri sorumlusunun veya veri işleyenin temsilcisinin ve bilgi güvenliği yetkilisinin kimliği ve iletişim bilgileri;
>
> (b)her bir veri sorumlusu adına gerçekleştirilen işleme kategorileri;

(c)ilgili hallerde, hangi üçüncü ülke veya uluslararası kuruluş olduğu da belirtilerek, bir üçüncü ülkeye veya uluslararası kuruluşa yapılan aktarımlar ve 49(1). maddenin ikinci alt fıkrası kapsamındaki aktarımlarda, uygun güvencelere ilişkin dokümantasyon;

(d)mümkün olan hallerde, 32(1). maddede atıf yapılan teknik ve organizasyonel tedbirlerin genel bir açıklaması.

3. 1 ve 2. fıkralarda belirtilen kayıtlar yazılı şekilde tutulmalıdır, elektronik biçim de kullanılabilir.

4. Denetim makamının talebi üzerine veri sorumlusu, veri işleyen ve ilgili hallerde, veri sorumlusunun veya veri işleyenin temsilcisi, bu kayıtları sunmakla yükümlüdür.

5. 1. ve 2. fıkralarda belirtilen yükümlülükler, işlemenin gerçek kişilerin hak ve özgürlükleri açısından risklere yol açmasının muhtemel olması, arizi nitelikte olmaması veya 9(1). maddede belirtilen özel nitelikli kişisel veri kategorilerine veya 10. Maddede belirtilen cezai hükümlere veya suçlara ilişkin olması halleri istisna olmak üzere, 250'den az kişi istihdam eden girişime veya organizasyona uygulanmaz.

Tüzük'ün 31. maddesine göre veri sorumlusu ve veri işleyen ve ilgili hallerde temsilcileri, talep üzerine görevlerinin ifası için denetim makamları ile işbirliği yapmakla yükümlüdür.

Tüzük'ün 'İşlemenin güvenliği' başlıklı 32. maddesine göre veri işleyen veya veri sorumlusu, tekniğin durumu, uygulama maliyeti ve işlemenin tabiatı, kapsamı, bağlamı ve maksatlarına; gerçek kişilerin haklarına, özgürlüklerine yönelik farklı olasılık ve önemde riskleri dikkate alarak riskle orantılı güvenlik düzeyi temin etmek için elverişli teknik ve organizasyonel tedbirleri almalıdır. Tüzük'ün bu düzenleme ile amacı, kişisel verilerin ele geçirilmesinden doğacak riskleri ortadan kaldırmaktır.[237] Bu tedbirler arasında;

- Kişisel verilerin psödonimleştirilmesi ve şifrelenmesi,
- İşleme sistemleri ve hizmetlerinin bütünlüğünü, gizliliğini, dayanıklılığını ve ulaşılabilirliğini sürekli olarak temin etme yetisi,
- Fiziksel yahut teknik kaza olduğunda verilerin kurtarılması ve verilere tekrar erişim sağlama yetisi,

[237]Develioğlu , 2017 , **a.g.k.** , 107.

- İşlemenin güvenliğini temin eden teknik ve organizasyonel tedbirlerin etkinliğini düzenli olarak kontrol etmek, ölçmek ve değerlendirmek için bir prosedür yer almalıdır.

Uygun güvenlik seviyesinin belirlenmesi için aktarılan, depolanan ya da sair surette işlenen verilerin kaza sonucu ya da hukuka aykırı surette bozulması, kaybı, değiştirilmesi, izinsiz ifşa edilmesi ve erişilmesi başta olmak üzere işlemenin teşkil ettiği riskler göz önüne alınır.

Veri sorumlusu, onaylanmış davranış kurallarına veya onaylanmış sertifikasyon mekanizmalarına uymasını veri güvenliğini sağlamak için öngörülen tedbirleri aldığına delil gösterebilir.

Veri sorumlusu veya veri işleyen, AB veya AB üyesi devlet hukuku uyarınca mecbur kılınmadığı sürece kendi otoritesi altındaki kişisel verilere erişimi olan gerçek kişilerin kişisel verileri talimatı dışında işlememesini sağlamak için gerekli önlemleri almalıdır.

Tüzük, veri sorumlusuna kişisel veri güvenliği ihlalini denetim makamına bildirme yükümlülüğü getirmiştir. Her ne kadar işlemenin güvenliğini sağlama yükümlülüğü getirilse de bir şekilde bu güvenliğin sağlanamaması ihtimaline karşı tüzük, veri sorumlusuna güvenlik ihlalini denetim makamına bildirme yükümlülüğü getirmiştir.

Bildirim yükümlülüğü Tüzük'ün 33.maddesine düzenlenmiştir. Buna göre veri sorumlusu, kişisel veri güvenliğinin ihlal edilmesi halinde, ihlalin gerçek kişilerin hak ve özgürlükleri bakımından risklere yol açması ihtimali düşük olmadıkça gecikmeden ve mümkünse ihlali öğrenmesinden itibaren 72 saat içinde yetkili denetim makamına bu ihlali bildirmelidir. Bu bildirim en azından;

- İhlalin niteliğini açıklar,
- Bilgi güvenliği yetkilisi veya daha fazla bilgi edinmek için iletişime geçilebilecek diğer bir kişinin kimliği ve iletişim bilgilerini içerir,
- Kişisel veri güvenliği ihlalinin muhtemel sonuçlarını açıklar,

- Uygun hallerde, doğacak olumsuz etkileri azaltmak için alınanlar dahil olmak üzere kişisel veri güvenliği ihlaline karşı alınan ve alınması önerilen tedbirleri belirtir.

Denetim makamına bildirim 72 saat içinde yapılamazsa bildirim gecikmenin sebeplerini de içermelidir.

Veri işleyen, bir kişisel veri güvenliği ihlalinden haberdar olur olmaz gecikmeksizin ihlali veri sorumlusuna bildirir.

Aynı anda sağlanması mümkün olmayan hallerde bilgi, gecikmeye mahal bırakmadan aşama aşama temin edilebilir.

İhlale ilişkin koşullar, etkileri ve ihlali telafi etmek için yapılanlar dahil olmak üzere kişisel veri güvenliği ihlalleri veri sorumlusu tarafından kayda geçirilir. Kayıtlar denetim makamının, bildirim yükümlülüğüne uyulduğunu tespit edebilmesine uygun olmalıdır.

Her ne kadar Tüzük'te veri sorumlusunun veri işlemenin mevcut risklerini göz önüne alarak, uygun teknik ve organizasyonel önlemleri alması gerektiği düzenlenmiş olsa da Tüzük ayrıca işlemenin özellikli riskler oluşturduğu hallerde 'veri koruması etki değerlendirmesi' olarak adlandırılan bir denetim yapılmasını ve yetkili denetim makamının ön görüşüne başvurulması gerektiğini öngörmüştür. Bu sistem, Tüzük'le veri koruma hukukuna dahil olmuştur.

Yönerge ise otomatik işleme yapacak veri sorumlularının denetim makamına önceden bildirimde bulunmasını ve risk oluşturan veri işlemelerinin bir 'ön denetleme' mekanizması işletilmek suretiyle denetim makamı tarafından denetlenmesini öngörmüştür.

Veri koruması etki değerlendirilmesi sisteminde ilk değerlendirme veri sorumlusu tarafından gerçekleştirilir. Değerlendirmenin sonucuna göre gerekirse denetim makamına başvurulur.

Özellikle yeni teknolojiler kullanan bir işleme türü, işlemenin tabiatı, kapsamı, bağlamı ve amaçları dikkate alındığında gerçek kişilerin hak ve özgürlüklerini önemli risk altına alıyorsa veri sorumlusu veriyi işlemeden önce planlanan işleme

faaliyetlerinin kişisel verilerin korunması üzerindeki etkisine yönelik bir değerlendirme gerçekleştirir. Veri sorumlusu, tek bir değerlendirme ile benzer önemli riskleri doğuran benzer işleme faaliyetlerini ele alabilir.

Veri koruması etki değerlendirmesi, özellikle şu hallerde yapılmalıdır:

- Otomatik işlemeye dayanan, gerçek kişiler hakkında hukuksal neticelere sebep olan ya da gerçek kişileri benzer surette önemli ölçüde etkileyen kararlara dayanak olan gerçek kişilerin kişisel özelliklerinin sistematik ve kapsamlı bir şekilde tespit edilmesi halinde,
- Özel nitelikli kişisel veri kategorileri veya cezai hüküm veya suçlarla ilgili verilerin geniş kapsamlı şekilde işlenmesi halinde,
- Kamuya açık bir alanın sistematik olarak geniş kapsamlı şekilde gözlemlenmesi halinde.

Denetim makamı, veri koruması etki değerlendirmesi yapılmasını gerektiren işleme faaliyetleri türlerinin bir listesini yapmak, bunu kamuya açıklamak ve bu listeleri Avrupa Veri Koruma Kurulu'na bildirmekle yükümlüdür.

Denetim makamı, veri koruması etki değerlendirmesi gerektirmeyen işleme faaliyetleri türlerinin de bir listesini yapabilir ve bunu kamuya açıklayabilir. Fakat denetim makamı bu listeleri Avrupa Veri Koruma Kurulu'na bildirir.

Veri koruması etki değerlendirmesinde en azından şunlar yer almalıdır:

- İlgili hallerde veri sorumlusunun gözettiği meşru menfaatler de dahil olmak üzere planlanan işleme faaliyetlerinin sistematik bir tarifi ve işlemenin amaçları,
- İşleme faaliyetlerinin amaçları bakımından ne kadar gerekli ve ölçülü olduğuna ilişkin değerlendirme,
- İlgili kişinin hak ve özgürlüklerine yönelik risklere ilişkin değerlendirme,
- İlgili kişilerin ve etkilenen sair bireylerin haklarını ve meşru menfaatlerini göz önüne alarak kişisel verilerin korunmasını sağlamak ve Tüzük'e uyulduğunu ortaya koymak için alınan önlemler, güvenlik tedbirleri ve mekanizmalar da dahil olmak üzere risklere karşı öngörülen tedbirler.

Tüzük'e göre ilgili veri sorumlusu veya veri işleyen tarafından Tüzük'ün 40. maddesinde belirtilen onaylanmış davranış kurallarına uyulması, özellikle veri koruması etki değerlendirmesi açısından söz konusu veri sorumluları veya veri işleyenler tarafından yapılan işleme uygulamalarının tesirinin değerlendirilmesinde göz önüne alınır.

Uygun durumlarda veri sorumlusu, ticari ya da kamusal menfaatlerin muhafazasına veya işleme faaliyetlerinin güvenliğine halel getirmeyecek şekilde ilgili kişilerin veya temsilcilerin planlanan işleme hakkında görüşlerini alır.

Bilgi güvenliği yetkilisinin atanmış olması durumunda veri sorumlusu, veri koruması etki değerlendirmesi sırasında bilgi güvenliği yetkilisinin tavsiyesine başvurmalıdır.

Veri sorumlusu, gerekli hallerde ve en azından işleme faaliyetlerinin oluşturduğu risk değiştiğinde veri işlemenin veri koruması etki değerlendirmesine uygun gerçekleştirilip gerçekleştirilmediğini değerlendirmek üzere bir inceleme yapmalıdır.

Veri sorumlusu, veri koruması etki değerlendirmesinin risklerin azaltılması için veri sorumlusu tarafından önlem alınmazsa veri işlemenin önemli risklere yol açacağını ortaya koyduğu hallerde işlemeden önce denetim makamının görüşüne başvurmalıdır.

Veri sorumlusu, denetim makamının görüşüne başvururken, denetim makamına şu bilgileri sağlamalıdır:

- İlgili hallerde ve özellikle bir teşebbüsler birliği dahilinde işleme söz konusu ise, veri sorumlusu, müteselsil veri sorumluları ve veri işleyenlerin sorumlulukları,
- Planlanan veri işlemenin amaçları ve vasıtaları,
- Tüzük uyarınca ilgili kişilerin hak ve özgürlüklerini korumak için öngörülen tedbirler ve güvenceler,
- Gerekli durumlarda, bilgi güvenliği yetkilisinin haberleşme verileri,
- Veri koruması etki değerlendirmesi,
- Denetim makamı tarafından talep edilen diğer bilgiler.

Bazı hallerde veri sorumlusu ve veri işleyen bir bilgi güvenliği yetkilisi atamakla yükümlüdür. Bu haller Tüzük'te şöyle sıralanmıştır:

- Veri işlemesi, yargısal faaliyette bulunan mahkemeler hariç olmak üzere, bir kamu kurumunca gerçekleştiriliyorsa,
- Veri sorumlusunun ya da veri işleyenin esas faaliyetleri, tabiatı, kapsamı ve/ya da maksatları gereği ilgili kişilerin nizamlı ve sistemli şekilde geniş kapsamlı gözlemlenmesi ile ilgiliyse,
- Veri sorumlusunun veya veri işleyenin esas faaliyetleri, Tüzük'ün 9. maddesinde belirtilen hassas verilerin ya da 10. maddede belirtilen cezai düzenlemeler ve suçları konu alan kişisel verilerin geniş çapta işlenmesine ilişkinse.

Tüzük'ün 39. maddesine göre bilgi güvenliği yetkilisinin asgari görevleri şunlardır:

- Veri sorumlusuna veya veri işleyene ve Tüzük uyarınca işleme gerçekleştirilen çalışanlarına, Tüzük ve diğer AB veya AB üyesi devlet kişisel veri koruma mevzuatı hakkında bilgi ve tavsiye vermek,
- Tüzük ve diğer AB veya AB üyesi devlet kişisel veri koruma hükümleri ile sorumluluk dağılımı, işleme faaliyetlerine katılan çalışanların bilinçlerinin artırılması, eğitimi, denetimler hakkındakiler esas teşkil etmek üzere veri sorumlusunun ya da veri işleyenin kendi politikalarına uyulmasını denetlemek,
- Talep edilmesi halinde veri koruma etki değerlendirmesi hakkında tavsiye vermek ve uygulamasını takip etmek,
- Denetim makamı ile işbirliği yapmak,
- İşlemeye ilişkin konularda ve ilgili diğer tüm hallerde bilgi vermek için denetim makamının iletişim noktası olmak.

Bir teşebbüsler birliği, bilgi güvenliği yetkilisinin her bir işletme tarafından kolayca erişilebilmesi şartıyla, tek bir bilgi güvenliği yetkilisi atayabilir.

Veri sorumlusunun veya veri işleyenin bir kamu kurumu veya kuruluşu olduğu hallerde organizasyonel yapıları ve büyüklükleri dikkate alınarak birkaç kamu kurumu veya kuruluşuna tek bir bilgi güvenliği yetkilisi atanabilir.

Tüzük'ün 37. maddesinin 1. fıkrasında sayılan veri sorumlusu veya veri işleyen tarafından bilgi güvenliği yetkilisi atanmasının zorunlu olduğu haller dışında, veri sorumlusu ya da veri işleyen kategorilerini temsil eden dernekler ve diğer kuruluşlar bir bilgi güvenliği yetkilisi atayabilir ya da AB veya AB üyesi devlet hukuku bilgi güvenliği yetkilisi atamalarını zorunlu kılabilir. Bilgi güvenliği yetkilisi, veri sorumlularını veya veri işleyenleri temsil eden söz konusu dernek veya diğer kuruluşlar adına hareket edebilir.

Bilgi güvenliği yetkilisi, özellikle kişisel verilerin korunması hukuku ve uygulaması hakkında uzmanlık bilgisi başta olmak üzere mesleki yetileri ve Tüzük'ün 39. maddesinde sayılan bilgi güvenliği yetkilisinin görevlerini yerine getirme yetisi dikkate alınarak tayin edilir.

Bilgi güvenliği yetkilisi, veri sorumlusunun veya veri işleyenin çalışanı olabileceği gibi vazifelerini hizmet sözleşmesi kapsamında ifa da edebilir.

Veri sorumlusu veya veri işleyen, bilgi güvenliği yetkilisinin iletişim bilgilerini yayınlar ve denetim makamına bildirir.

Veri sorumlusu ya da veri işleyen, bilgi güvenliği yetkilisinin, kişisel verilerin işlenmesine ilişkin tüm meselelere uygun tarzda ve uygun müddet içinde dahil olmasını sağlamalıdır.

Veri sorumlusu ve işleyicisi; bilgi güvenliği yetkilisini vazifesini ifa etmesi, kişisel verilere ve işleme faaliyetlerine erişebilmesi ve uzmanlığını sürdürebilmesi için gerekli kaynakları sağlayarak bilgi güvenliği yetkilisinin görevlerini ifa etmesi için desteklemelidir.

Veri sorumlusu veya veri işleyen, bilgi güvenliği yetkilisinin, söz konusu görevlerinin ifasına ilişkin olarak hiçbir talimat almamasını sağlamalıdır. Bilgi güvenliği yetkilisi, görevlerini ifa ettiği için veri sorumlusu veya veri işleyen tarafından görevden alınamaz veya cezalandırılamaz. Bilgi güvenliği yetkilisi, doğrudan veri sorumlusunun veya veri işleyenin en üst yönetim seviyesine rapor vermelidir.

İlgili kişiler, kişisel verilerinin işlenmesine ve Tüzük'ten kaynaklanan haklarını kullanmalarına ilişkin tüm konularda bilgi güvenliği yetkilisi ile iletişime geçebilir.

Bilgi güvenliği yetkilisi, AB veya AB üyesi devlet hukukuna uygun olarak görevlerinin ifasında sır saklama veya gizlilik yükümlülüğü altında olmalıdır.

Bilgi güvenliği yetkilisi başka görev ve yükümlülükler de ifa edebilir. Veri sorumlusu veya veri işleyen, söz konusu görev ve yükümlülüklerin bir menfaat çatışmasına neden olmasını önlemelidir.

Tüzük'ün 32. maddesine göre veri sorumlusunun işlemenin güvenliği kapsamında işleme sistemleri ve hizmetlerinin gizliliğini sağlama yükümlülüğü vardır.

Tüzük'ün 28. maddesine göre veri işleyen, kişisel verileri işlemeye yetkili kişiler yasal olarak gizlilik yükümlülüğü altında değillerse bunu hukuken üstlenmelerini sağlamalıdır.

Tüzük'ün 38. maddesine göre bilgi güvenliği yetkilisi, AB veya AB üyesi devlet hukukuna uygun olarak görevlerinin ifasında sır saklama veya gizlilik yükümlülüğü altında olmalıdır.

### 2.14.9.İlgili kişilerin haklarının korunması

Tüzük'ün 12. maddesine göre veri sorumlusu, ilgili kişiye verilmesi gereken bilgilerin sağlanmasında ve her türlü iletişimin gerçekleştirilmesinde kısa, şeffaf, anlaşılması ve erişimi basit bir biçim ve bunları sağlayan bir dil kullanılması için gerekli tedbirleri almalıdır. İlgili kişinin çocuk olduğu durumlarda bu hususa daha ehemmiyet verilmelidir. Bilgi sağlama için herhangi bir şekil öngörülmemiştir. Yazılı veya elektronik yöntem ile de bilgi sağlanabilir. Fakat sözlü bilgi verilmesi için ilgili kişi, sözlü bilgi verilmesi yönünde talepte bulunmalı ve kimliğini ispat etmelidir.

Veri sorumlusu, Tüzük'ün ilgili kişiye sağladığı hakların kullanılmasını kolaylaştırmalıdır.

Tüzük'ün 11. maddesine göre veri sorumlusunun kişisel verileri işleme amacının gerçekleşmesi için ilgili kişinin kimliğinin belirlenmesi gerekli değilse veri sorumlusunun sadece Tüzük'e uymak amacıyla ilgili kişinin kimliğini belirlemek için ilave bilgi saklamak, toplamak ya da işlemek mecburiyeti yoktur. Bu düzenlemenin

amacı, veri sorumlularını sadece ilgili kişiyi belirleyebilmek için gerekli olandan fazla kişisel verileri bulundurmak külfetinden kurtarmaktır.[238]

Yukarıda belirtildiği üzere veri sorumlusu tarafından kimliğin saptanmasının gerekmediği hallerde veri sorumlusu, ilgili kişinin kimliğini belirleyemediğini ispatlayabilirse mümkünse ilgili kişiyi bu yönde haberdar etmelidir. İlgili kişi, kimliğinin tespit edilmesini sağlayabilecek ek bilgileri sağlamadığı müddetçe Tüzük'ün 15-20 maddelerinde ilgili kişilere tanımış olduğu haklarını kullanamaz. Bu durumda veri sorumlusu da ilgili kişinin kimliğini belirleyemediğini ispat etmedikçe ilgili kişinin Tüzük'ün 15-20. maddelerinden doğan haklarını kullanma talebini reddedemez.

Veri sorumlusu, ilgili kişinin Tüzük'ün 15-20 maddelerine dayanan talebi üzerine gerçekleştirilen eylemler hakkında gecikmeksizin ve her şartta talebin alınmasından itibaren bir ay içinde ilgili kişiye bilgi vermekle yükümlüdür. Bu süre gerekli hallerde iki ay daha uzatılabilir. Sürenin uzatılması halinde veri sorumlusu, talebin alınmasından itibaren bir ay içinde sürenin uzatıldığını ve uzatılma gerekçelerini ilgili kişiye bildirmelidir. Eğer ilgili kişi, Tüzük'ten doğan haklarını kullanma talebini veri sorumlusuna elektronik yollarla iletmişse imkan dahilinde ve ilgili kişi aksini talep etmedikçe bilgi elektronik yolla ilgili kişiye iletilmelidir.

Veri sorumlusu, ilgili kişinin talebi üzerine harekete geçmezse; gecikmeden ve her şartta talebin alınmasından itibaren bir ay içinde gecikmenin gerekçelerinin neler olduğu, ilgili kişinin denetim makamına şikayet hakkı olduğu ve sair yasal yollara başvuru hakkı olduğu hususunda ilgili kişiyi bilgilendirmelidir.

Tüzük'ün 13. ve 14. maddelerinde belirtilen bilgiler ve 15-22 ve 34. maddeleri kapsamındaki bildirimler ve eylemler ücret talep etmeden sunulmalıdır. Fakat ilgili kişinin talepleri açıkça dayanaksız veya aşırı ise veri sorumlusu, talep edilen bilgiyi veya bildirimi sağlamanın veya harekete geçmenin idari masraflarını dikkate alarak makul bir ücret talep edebileceği gibi talep üzerine harekete geçmeyi reddedebilir.

İlgili kişinin taleplerinin açıkça dayanaksız ve aşırı olduğunu ispat yükü veri sorumlusundadır.

[238]Safarı , s.829'dan aktaran Develioğlu , 2017 , **a.g.k.** , 118.

Eğer veri sorumlusu, Tüzük'ün 15-21 maddeleri kapsamında talepte bulunan ilgili kişinin kimliğinden makul sayılabilecek bir şüpheye düşerse ilgili kişinin kimliğini doğrulamak için ek bilgi talep edebilir.

Veri sorumlusu tarafından ilgili kişiye temin edilecek bilgiler, yapılması planlanan kişisel veri işlemesini kolay anlaşılacak biçimde tarif etmek için standartlaştırılmış simgelerle sunulabilir. Elektronik yollarla sunulmuş olan simgelerin makine tarafından okunabilir olması gerekir. AB komisyonu, simgeler ile sunulabilecek bilgileri ve standart simgelerin sunulma işleyişlerini belirleme yetkisine sahiptir.

Tüzük'ün 77. maddesine göre diğer idari ve yasal yollara başvurma hakkı saklı kalmak kaydıyla her ilgili kişi kendisiyle ilgili kişisel verilerin işlenmesinin Tüzük'ü ihlal ettiğini düşünmesi halinde olağan ikametgahı, işyeri ya da ihlalin gerçekleştiği iddia edilen yer denetim makamına şikayette bulunmak hakkına sahiptir.

Şikayetin yapıldığı denetim makamı, müştekiyi şikayetin durumu ve sonucu hakkında bildirmekle yükümlüdür. Tüzük'ün 78. maddesi uyarınca bir denetim makamına karşı yasal yollara başvurma hakkının varlığı da denetim makamının bildirmesi gerekenler arasında yer almaktadır.

Tüzük'ün 78. maddesine göre her gerçek ve tüzel kişinin denetim makamının kendisi hakkındaki hukuken bağlayıcı kararlarına karşı etkili yasal yollara başvurma hakkı vardır.

Her ilgili kişi, yetkili denetim makamının kendisine Tüzük'ün 77. maddesi uyarınca yapılan bir şikayeti incelememesi veya üç ay içinde şikayetin durumu veya sonucu hakkında bilgilendirmemesi durumunda etkili yasal yollara başvurabilir.

Bir denetim makamı aleyhine açılan davalarda yargılama yetkisi, denetim makamının bulunduğu AB üyesi devlet mahkemelerindedir.

Aleyhine yasal yollara başvurulan denetim makamının kararı, Avrupa Veri Koruma Kurulu'nun tutarlık mekanizması kapsamında verdiği bir görüşüne veya kararına dayanıyorsa denetim makamı, bu görüş veya kararı da ilgili mahkemeye iletmelidir.

Tüzük'ün 83. maddesine göre denetim makamı, Tüzük uyarınca verilen idari para cezalarının etkili, ölçülü ve caydırıcı olmasına önem vermelidir.

İdari para cezasının belirlenmesi, denetim makamının takdirinde olup ceza miktarı belirlenirken şu hususların dikkate alınacağı öngörülmüştür:

- İşlemenin tabiatı, ağırlığı ve süresi,
- İhlalin kasta veya ihmale dayanması,
- Veri sorumlusunun veya veri işleyenin zararın azaltılması için aldığı önlemler,
- Veri sorumlusu ve veri işleyenin sorumluluk derecesi,
- Veri sorumlusu ve veri işleyenin önceki ihlalleri,
- İhlali gidermek ve ihlalin olası etkilerini azaltmak için denetim makamı ile gerçekleştirilen işbirliğinin derecesi,
- İhlalden etkilenen kişisel veri kategorileri,
- Denetim makamının ihlalden haberdar olma şekli, özellikle veri sorumlusu ve veri işleyenin ihlali denetim makamına bildirip bildirmediği ve bildirdiyse ne ölçüde bildirdiği,
- Veri sorumlusu ve veri işleyene verilen düzeltici emirlere ne kadar uyulduğu,
- Veri sorumlusunun onaylanmış davranış kurallarına uyup uymadığı veya onaylanmış sertifikasının olup olmadığı,
- Somut olayın şartlarında yer alan hafifletici veya ağırlaştırıcı etkenler, örneğin ihlalden dolaylı veya doğrudan elde edilen maddi menfaatler veya sakınılan zararlar.

Bir veri sorumlusu veya veri işleyen kasten veya ihmalen aynı işleme faaliyeti veya bağlantılı işleme faaliyetleri için Tüzük'ün birden fazla hükmünü ihlal ederse toplam idari para cezası, en ağır ihlal için öngörülen ceza miktarını geçemez.

AB üyesi her devlet, kendi bünyesinde bulunan kamu kurum ve kuruluşlarına idari para cezası verilip verilmeyeceğine, verilecekse sınırlarına ilişkin kurallar belirleyebilir.

Tüzük'ün 84. maddesine göre AB üyesi devletler, Tüzük'ün ihlali halinde, özellikle 83. maddede öngörülen idari cezalara tabi olmayan ihlaller için uygulanacak diğer cezalar tesis edebilir ve bu cezai yaptırımların uygulanmasını sağlamak için gerekli tedbirleri almalıdır. Bu cezalar, idari para cezalarında olduğu gibi etkili, orantılı ve caydırıcı olmalıdır.

Tüzük'ün 79. maddesine göre Tüzük'ün 77. maddesi gereği denetim makamına şikayette bulunma hakkı dahil olmak üzere, idari ve mevcut diğer yargı dışı yollara başvuru hakkı saklı kalmak kaydıyla kişisel verilerinin Tüzük'e aykırı şekilde işlenmesi sebebiyle Tüzük'ten doğan haklarının ihlal edildiğini düşünen her ilgili kişi, yasal yollara başvurma hakkına sahiptir.

Veri sorumlusu ya da işleyicisine karşı dava, veri sorumlusunun ya da veri işleyicinin işletmesinin bulunduğu AB üyesi devlet mahkemeleri önünde açılır. Veri sorumlusunun ya da veri işleyenin kamu yetkilerini kullanan bir AB üyesi devlet kamu makamı olmadığı hallerde dava, ayrıca ilgili kişinin olağan yerleşim yerinin bulunduğu mahkemeler önünde açılabilir.

Tüzük'ün 81. maddesine göre bir AB üyesi devletin yetkili mahkemesi, başka bir AB üyesi devletin mahkemesinde derdest, aynı veri sorumlusu veya veri işleyen tarafından gerçekleştirilen işlemlere ilişkin olarak aynı konuyu ilgilendiren bir dava hakkında bilgiye sahipse diğer üye devletteki mahkeme ile söz konusu davanın varlığını teyit etmek için iletişime geçer.

İlk dava açılan mahkeme dışındaki diğer yetkili mahkemeler, aynı veri sorumlusu veya veri işleyen tarafından gerçekleştirilen işlemeye ilişkin aynı konuya dair bir dava olduğu hallerde, davalarını bekletebilir.

Söz konusu davanın ilk derece mahkemesinde derdest olduğu hallerde, taraflardan birinin başvurusu üzerine, ilk dava açılan mahkeme dışındaki diğer mahkemeler, ilk dava açılan mahkemenin yetkili olması ve mahkemenin hukukunun davaların birleşmesine imkan tanıması şartıyla, dava üzerindeki yetkisini reddedebilir.

Tüzük'ün 82. maddesinde ise tazminat hakkı düzenlenmiştir. Tüzük'ün 82. maddesine göre Tüzük'ün ihlali nedeniyle maddi ve manevi zarara uğrayan kişiler,

uğradığı zararın veri sorumlusu veya veri işleyen tarafından tazmin edilmesini isteyebilir.

Kişisel verilerin işlenmesine katılmış her bir veri sorumlusu, Tüzük'ü ihlal eden veri işlemesinin doğurduğu zarardan mesuldür. Veri işleyen ise Tüzük'ün özel olarak veri işleyenlere yönelttiği yükümlülüklere uymadığı veya veri sorumlusunun talimatlarına aykırı davrandığı hallerde işlemenin doğurduğu zarardan mesuldür. Fakat veri sorumlusu veya veri işleyen, zarar verici olaydan hiçbir şekilde sorumlu olmadığını kanıtlarsa sorumluluktan kurtulur.

Birden fazla veri sorumlusunun veya veri işleyenin ya da veri sorumlusu ve veri işleyenin birlikte kişisel veri işlemesine dahil olduğu ve tazminat sorumluluğunun doğduğu durumlarda; her bir veri sorumlusu ve veri işleyen, ilgili kişinin zararının tamamından sorumludur. Bu durumda her bir veri sorumlusu veya veri işleyen, kendisine düşen tazminat miktarı dışındaki tazminatı diğer veri sorumlularına veya veri işleyenlere rücu edebilir.

Tazminat davaları, Tüzük'ün 79/2 maddesinde belirtilen AB üyesi devlet hukukuna göre yetkili olan mahkemelerde açılır.

### 2.14.10.Denetim makamları

Tüzük, AB içinde kendisinin düzenli ve etkili bir şekilde uygulanması için aralarında işbirliği olan kurumların oluşturulmasını öngörmüştür.

Bu kurumlardan biri hukuki kişiliği olan Avrupa Veri Koruma Kurulu, diğeri her AB üyesi devlet tarafından tayin edilmesi gereken bir veya birden fazla denetim makamıdır.

Tüzük'ün 51.maddesine göre her bir üye devlet, gerçek kişilerin işlemeyle bağlantılı temel hak ve özgürlüklerini muhafaza etmek, AB bünyesinde serbest veri akışını basitleştirmek maksadıyla Tüzük'ün uygulanmasını gözetmekten sorumlu olan bir veya birden fazla bağımsız kamu kurumu oluşturmalıdır.

Her bir denetim makamı, Tüzük'ün AB içinde düzenli ve sistemli şekilde uygulanmasına katkı sağlamalıdır. Bu amacın gerçekleşmesi için denetim makamı, diğer denetim makamlarıyla ve AB komisyonu ile işbirliği yapar.

Denetim makamının bağımsızlığı, Tüzük'ün 52. maddesinde düzenlenmiştir. Buna göre her bir denetim makamı; Tüzük'ün tevdi ettiği görevlerini ifa ederken, yetkilerini kullanırken tam bağımsız şekilde davranmalıdır.

Denetim makamının üyeleri, görevlerini ifa ederken, yetkilerini kullanırken, bütün dış tesirlerden uzak kalmalı; hiçbir surette emir almamalıdır.

Her bir denetim makamının üyeleri, görevleri ile bağdaşmayacak her türlü davranıştan uzak durmalı ve görevleri süresince, ücret karşılığı olsun veya olmasın, bu nitelikteki işlerde çalışmaktan kaçınmalıdır.

Her bir üye devlet, denetim makamlarının görevlerini etkin bir şekilde ifa edebilmeleri ve selahiyetlerini kullanabilmeleri için gerekli insan kaynağını, teknik kaynakları, finansal kaynakları, mekanı, altyapıyı sağlar.

Her bir üye devlet, denetim makamlarının sadece ilgili denetim makamı üyesi veya üyelerinin talimatına bağlı olacak şekilde kendi kadrosu olmasını ve bu kadroyu seçmesini sağlamalıdır.

Her bir üye devlet, denetim makamlarının bağımsızlıklarını etkilememek koşuluyla finansal denetime tabi olmalarını ve kendi yıllık kamusal bütçelerine sahip olmalarını sağlamalıdır.

Denetim makamları arasındaki yetki dağılımına ilişkin kuralların yer aldığı Tüzük'ün 55. maddesine göre her bir denetim makamı, Tüzük'ün kendisine verdiği görevlerin ifası ve yetkilerin kullanılması için bağlı olduğu AB üyesi devlet sınırları içerisinde yetkilidir.

Kamu makamları ve özel kurumlar tarafından bir yasal yükümlülüğün ifası için kamu menfaati gereği ifa edilen vazife yahut veri sorumlusunun resmi yetkisinin icrası maksadıyla gerçekleştirilen kişisel veri işlemelerinde ilgili üye devletin denetim makamı yetkilidir.

Denetim makamlarının mahkemelerin yargı yetkisi kapsamındaki kişisel veri işleme faaliyetlerini denetleme yetkisi yoktur.

Sınır ötesi kişisel veri işlemelerinde veri işlemesini yapan veri sorumlusu veya işleyenin işletmesinin veya ana işletmesinin tabi olduğu denetim makamı, öncü denetim

makamı olarak hareket edecek; böylece AB bünyesindeki birden fazla işletmesi olan veya birden fazla ülkede faaliyet gösteren veri sorumluları ve veri işleyicileri**,** tek bir denetim makamı ile muhatap olacaklardır. Bunun ise veri sorumluları ve veri işleyiciler üzerindeki bürokratik yükü azaltacağı[239] ve özellikle uluslararası şirketler için avantajlı bir düzenleme olduğu[240] yönünde değerlendirmeler mevcuttur. Fakat AB bünyesinde bir işletmesi bulunmayan veri sorumluları ve veri işleyicilerinin bu düzenlemeden yararlanması mümkün değildir.[241] Tüzük'ün;

"*bu tüzük, birlik dahilindeki ilgili kişilerin kişisel verilerinin birlik dahilinde işletmesi bulunmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesi halinde, işleme faaliyetlerinin:*

*(a)ilgili kişiden bir ödeme istenip istenmediğine bakılmaksızın, birlik dahilinde bulunan ilgili kişilere mal veya hizmet sunulmasına*

*(b)Birlik dahilinde gerçekleşen davranışlarının gözlemlenmesine ilişkin olması halinde uygulanır*."

şeklindeki 3(2) maddesi gereği Tüzük kapsamında değerlendirilen veri sorumluları ve veri işleyicileri, bir AB üyesi devlet'te temsilci atasalar dahi işleme faaliyetlerini gerçekleştirdikleri her AB üyesi devletin denetim makamının yetki alanına ayrı ayrı girerler.

Tüzük'ün 56. maddesine göre bir tüzük ihlalinin veya bir şikayetin yalnızca kendi AB üyesi devlet sınırları içerisindeki bir işletmeye ilişkin olması veya kendi AB üyesi devlet sınırlarındaki ilgili kişileri önemli derecede etkilemesi durumunda ilgili denetim makamı bunu ele almaya yetkilidir. Bu durum ivedilikle öncü denetim makamına bildirilir ve öncü denetim makamı üç hafta içinde konuyu ele alıp almayacağını belirler. Eğer öncü denetim makamı, meseleyi kendi incelemeye karar verirse, Tüzük'ün 60.

[239]Barnard-Wills, David/Pauner Chulvı, Cristina/ De Hert, Paul, Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU, Computer Law & Security Review, 32, 2016, s. 590; Voss, Gregory W. , Looking at European Union Data Protection Law Reform Through a Different Prism:The Proposed EU General Data Protection Regulation Two Years Later, Journal of Internet Law, 17(9), March 2014, s.13; Voss, Gregory W. , One Year and Loads of Data Later, Where Are We? An Update on the Proposed European Union General Data Protection Regulation, Journal of Internet Law, 16 (10), April 2013 , s.14'ten aktaran Develioğlu , 2017 , **a.g.k.** , 139.

[240]Gılbert, Francoise, Eu General Data Protection Regulation: What Impact for Businesses Established Outside the European Union, Journal of Internet Law, May 2016, s.4-'ten aktaran Develioğlu , 2017 , **a.g.k.** , 139.

[241]Develioğlu , 2017 , **a.g.k.** , 139.

maddesinde düzenlenen işbirliği prosedürünü uygular. Bu durumda ilk denetim makamının öncü denetim makamına bir karar taslağı sunması mümkündür. Eğer öncü denetim makamı meseleyi kendi incelemeye karar vermezse ilk denetim makamı, meseleyi, Tüzük'ün 61. maddesinde düzenlenen karşılıklı yardımlaşma ve 62. maddesinde düzenlenen ortak operasyon kurallarına göre inceler. Her şeye rağmen öncü denetim makamı, veri işleyicisi ve veri sorumlusunun sınır ötesi veri işlemeleri için tek muhataptır.

İlgili denetim makamları ile öncü denetim makamı arasındaki işbirliği prosedürü Tüzük'ün 60. maddesinde düzenlenmiştir.

Öncü denetim makamı ile diğer denetim makamları, ortak bir görüşe varmak amacıyla karşılıklı işbirliği ve bilgi alışverişinde bulunurlar. Öncü denetim makamının bu işbirliği kapsamında bir veri sorumlusu veya veri işleyicisi hakkında inceleme yapılması ve alınan önlemlerin denetimi için diğer denetim makamlarından karşılıklı yardımlaşma ve ortak operasyon icra etmeyi talep etmesi mümkündür.

Tüzük'ün 61.maddesinde öngörülen denetim makamları arasındaki yardımlaşma kapsamında, denetim makamlarının talebin amacı ve gerekçelerini belirterek birbirinden yardım ve talep amacıyla sınırlı olmak üzere bilgi talep edebileceği öngörülmüştür. Bu talebe denetim makamları en geç bir ay içinde cevap vermelidir. Talep, sadece denetim makamının ilgili konuda yetkili olmaması ve talebin kabulünün Tüzük'ü veya sair yasal mevzuatı ihlal etmesi halinde reddedilebilir. Talebe bir ay içinde cevap verilmemesi durumunda talepte bulunan denetim makamı, AB üyesi devlet sınırları dahilinde geçici önlemler alabilir veya bu durumda ivedilik prosedürüne başvurma şartlarının gerçekleştiği varsayılarak Avrupa Veri Koruma Kurulu'ndan ivedilik kararı alınabilir.

Tüzük'ün 62. maddesine göre denetim makamları, münasip durumlarda diğer AB üyesi devlet denetim makamlarının üyelerinin kadrosunun dahil olduğu ortak operasyonlar icra edebilir.

Veri sorumlusunun veya veri işleyicisinin birden fazla AB üyesi devlette işletmeleri olması veya veri işleme faaliyetlerinin birden fazla ülkede önemli sayıda ilgili kişiyi önemli ölçüde etkilemesi halinde her bir AB üyesi devletin bir denetim makamının ortak operasyonlara katılma hakkı vardır.

Tutarlılık mekanizmasının düzenlendiği Tüzük'ün 63. maddesine göre Tüzük'ün AB dahilinde yeknesak şekilde uygulanmasına katkı sağlamak için denetim makamları birbirleriyle ve ilgili hallerde AB komisyonuyla tutarlılık mekanizması aracılığı ile işbirliği yaparlar. Tutarlılık mekanizmasının amacı, AB dahilinde etkisi olacak konularda karar alınırken Avrupa Veri Koruma Kurulu'nun denetim makamlarına görüş bildirmesini sağlamak[242] ve denetim makamları arasında bir çözüm yolu öngörmektir.[243]

İvedilik yönteminin düzenlendiği Tüzük'ün 66. maddesine göre istisnai durumlarda ilgili bir denetim makamı, ilgili kişilerin hak ve hürriyetlerini korumak için harekete geçilmesini gerektiren acil bir ihtiyaç olduğu görüşündeyse Tüzük'te öngörülen tutarlılık mekanizmasından veya işbirliği prosedüründen ayrılarak üç ayı geçmeyecek belirli bir süre için geçerli olacak şekilde ve kendi sınırları içinde hukuki sonuçlar doğurmak üzere acilen geçici tedbirler alabilir. Denetim makamı, gecikmeksizin, bu tedbirleri ve bu tedbirleri alma gerekçelerini ilgili diğer denetim makamlarına, Avrupa Veri Koruma Kurulu'na ve AB Komisyonu'na bildirir.

Bir denetim makamı, ivedilik prosedürü gereği bir tedbir aldığı ve nihai tedbirlerin acilen alınması gerektiği görüşünde olduğu hallerde Avrupa Veri Koruma Kurulu'ndan böyle bir görüş veya acil bir nihai karar vermesini talep edebilir.

İlgili kişilerin hak ve özgürlüklerini korumak için acilen harekete geçilmesi gereken bir durumda yetkili denetim makamı uygun bir tedbir almamışsa, her bir denetim makamı, acilen harekete geçilmesi ihtiyacı da dahil olmak üzere söz konusu görüşü veya kararı talep etme gerekçelerini açıklayarak Avrupa Veri Koruma Kurulu'ndan acil bir görüş veya acil bir nihai karar vermesini talep edebilir.

Avrupa Veri Koruma Kurulu'nun vermiş olduğu ivedi bir mütalaa yahut ivedi bir nihai karar salt çoğunluk ile iki hafta içinde alınır.

Tüzük'ün 57. maddesinde denetim makamlarının görevleri sayılmıştır. Buna göre her bir denetim makamı, diğer görevler saklı kalmak kaydıyla, ilgili AB üyesi devlet sınırları içerisinde:

- Tüzük'ün uygulanmasını gözetir ve temin eder.

[242]Develioğlu , 2017 , **a.g.k.** , 143.
[243]Barnard-Wills/Pauner Chulvı/De Hert s.590 ; Develioğlu , 2017 , **a.g.k.** , 143.

- Veri işlemeye ilişkin riskler, kurallar, güvenceler ve haklar konusunda kamu farkındalığını ve bilincini artırır.
- AB üyesi devlet hukukuna uygun olarak gerçek kişilerin işleme ile bağlantılı hak ve özgürlüklerinin korunması ile ilgili kanuni ve idari tedbirler hususunda ulusal parlamentoya, hükümete ve sair müesseselere danışmanlık yapar.
- Veri sorumluları ve veri işleyenleri bu Tüzük'ten kaynaklanan yükümlülükleri konusunda bilinçlendirir.
- Talep üzerine, ilgili kişilere bu Tüzük'ten kaynaklanan haklarının kullanılmasına ilişkin bilgi verir ve gerekirse, bu maksatla sair üye devletlerdeki denetim makamlarıyla işbirliği yapar.
- Şikayetleri ele alır ve uygun düştüğü ölçüde şikayetin konusunu araştırır; şikayet edeni, özellikle daha fazla araştırma veya sair denetim makamları ile işbirliği gerekliyse, süreç ve araştırmanın sonucu hakkında, makul süre içinde bilgilendirir.
- Bu Tüzük'ün uygulanmasında ve icrasında yeknesaklık sağlamak amacıyla diğer denetim makamlarıyla işbirliği yapar.
- Bu Tüzük'ün uygulanmasına ilişkin incelemeler yapar.
- Kişisel verilerin korunması alanındaki gelişmeleri takip eder.
- Standart sözleşmesel hükümleri belirler.
- Veri koruması etki değerlendirmesi gereklerine ilişkin bir liste oluşturur ve muhafaza eder.
- İşleme faaliyetleri hakkında tavsiye verir.
- Davranış kuralları oluşturulmasını teşvik eder, davranış kuralları hakkında görüş bildirir ve kuralları tasdik eder.
- Sertifikasyon mekanizmaları ve veri koruması mühür ve markalarının tesisini teşvik eder ve sertifikasyon kriterlerini tasdik eder.
- Sertifikasyonları düzenli olarak değerlendirir.
- Davranış kurallarını denetleyen kuruluşların ve sertifikasyon kuruluşlarının akreditasyon ölçütlerini tanzim eder ve yayınlar.
- Davranış kurallarını denetleyen kuruluşların ve sertifikasyon kuruluşlarının akreditasyonlarını gerçekleştirir.

- Sözleşmesel hüküm ve düzenlemelere izin verir.
- Bağlayıcı kurumsal kuralları onaylar.
- Avrupa Veri Koruma Kurulu'nun faaliyetlerine katkı sağlar.
- Tüzük ihlallerine ve uygulanan tedbirlere ilişkin olarak kayıt tutar.
- Kişisel verilerin korunmasına ilişkin diğer görevleri ifa eder.

Denetim makamının inceleme (araştırma) yetkileri, düzeltici yetkileri ve istişari yetkileri vardır. Denetim makamının bu yetkileri, Tüzük'ün 58. maddesinde düzenlenmiştir.

Denetim makamının inceleme (araştırma) yetkileri şunlardır:

- Veri sorumlusuna ve veri işleyene ve ilgili hallerde veri sorumlusunun veya veri işleyenin temsilcisine, görevlerinin ifası için gerekli bilgileri sağlamalarını emretmek
- Kişisel veri denetimleri şeklinde incelemeler yapmak
- Verilen sertifikaları değerlendirmeye tabi tutmak
- Tüzük'ün ihlal edildiği iddialarını veri sorumlusuna veya veri işleyene bildirmek
- Veri sorumlusundan ve veri işleyenden, görevlerinin ifası için gerekli bütün kişisel verileri alabilmek
- Veri sorumlusuna ve veri işleyene ait mekanlara erişim elde etmek

Denetim makamının düzeltici yetkileri şunlardır:

- İşleme faaliyetlerinin Tüzük'ü ihlal etmesi ihtimal dahilinde olan veri sorumlularını veya veri işleyenlerini uyarmak
- İşleme faaliyetleri Tüzük'ü ihlal etmiş olan veri sorumluları veya veri işleyenlere kınama vermek
- Veri sorumlularına veya veri işleyenlere ilgili kişilerin Tüzük uyarınca haklarını kullanmak yönündeki taleplerine uymalarını emretmek
- Veri sorumlularına veya veri işleyenlere, işleme faaliyetlerini belirli şekilde ve belirli süre içinde Tüzük hükümlerine uyumlu hale getirmelerini emretmek

- Veri sorumlusuna kişisel veri güvenliği ihlallerini ilgili kişiye bildirmesini emretmek
- İşleme yasağı gibi geçici veya kesin kısıtlamalara hükmetmek
- Kişisel verilerin düzeltilmesini, silinmesini veya işlemenin sınırlandırılmasını ve kişisel verilerin ifşa edildiği aktarılanlara bu eylemlerin bildirilmesini emretmek
- Verilen sertifikaları geri almak, sertifikasyon kuruluşuna sertifikanın geri alınmasını veya sertifikasyon şartları karşılanmadıysa veya artık karşılanmıyorsa sertifikanın verilmemesini emretmek
- İdari para cezasına hükmetmek
- Üçüncü ülke veya uluslararası kuruluşta bulunan bir aktarılana veri akışının askıya alınmasını emretmek

Denetim makamının istişari yetkileri de dahil olmak üzere diğer yetkileri şunlardır:

- Öngörüş mekanizmasına uygun olarak veri sorumlularına tavsiye vermek;
- Kendiliğinden veya talep üzerine, ulusal meclise, AB üyesi devlet hükümetine veya AB üyesi devlet hukukuna uygun olarak diğer kuruluşlara ve kamuya kişisel verilerin korunmasına ilişkin her konuda görüşler sunmak;
- AB üyesi devlet kanunu'nun böyle bir izin araması halinde, işlemelere izin vermek;
- Taslak davranış kuralları hakkında fikir bildirmek ve onları onaylamak;
- Sertifikasyon kuruluşlarına akreditasyon vermek;
- Sertifikasyon vermek ve sertifikasyon ölçütlerini onaylamak;
- Standart kişisel verilerin korunması hükümlerini kabul etmek;
- Sözleşmesel hükümlere izin vermek;
- İdari anlaşmalara izin vermek;
- Bağlayıcı kurumsal kuralları onaylamak.

Tüzük'ün 58. maddesine göre denetim makamının kendisine sağlanan yetkilerini kullanması, birtakım tedbirlere tabi olmalıdır.

Her bir AB üyesi devlet kendi denetim makamının Tüzük ihlallerini yargı makamlarının dikkatine sunma, uygun durumlarda Tüzük'ü uygulamak için yasal süreçler başlatma veya yasal süreçlere dahil olma hakkını kanun yoluyla öngörmelidir.

Her bir AB üyesi devlet, yasal düzenlemeler yoluyla kendi denetim makamına Tüzük'ün 58. maddesinde sayılan yetkileri dışında ek yetkiler sağlayabilir.

Tüzük'ün 59. maddesi uyarınca her bir denetim makamının, faaliyetlerine ilişkin hazırladığı yıllık raporlar; ulusal meclise, hükümete, AB üyesi devlet hukukunca belirlendiği şekilde sair kurumlara iletilir; AB Komisyonuna ve Avrupa Veri Koruma Kurulu'na sunulur.

### 2.14.11. Avrupa veri koruma kurulu

Yukarıda, Tüzük'ün AB içinde kendisinin düzenli ve etkili bir şekilde uygulanması için aralarında işbirliği olan kurumların oluşturulmasını öngördüğünden ve bu kurumlardan birinin de hukuki kişiliği olan Avrupa Veri Koruma Kurulu olduğundan bahsedilmişti.

Denetim makamları arasındaki koordinasyonu ve iletişimi sağlamak ve uyuşmazlıkları çözümlemek için Tüzük'ün kurduğu bir kurumdur.[244]

Tüzük'ün 68. maddesine göre Avrupa Veri Koruma Kurulu, hukuki kişiliği olan bir AB kuruluşu olarak kurulmuştur.

Avrupa Veri Koruma Kurulu'nun yapısı, Tüzük'ün 68. maddesinde öngörülmüştür:

Kurulun temsilcisi, kurulun başkanıdır.

Kurul, her bir AB üyesi devletin bir denetim makamının başkanı ve Avrupa Veri Koruma Denetmeni ile temsilcilerinden oluşur.

Eğer bir AB üyesi devlette AB Genel Veri Koruma Tüzüğü uyarınca hükümlerin uygulanmasını gözetmekten sorumlu birden fazla denetim makamı varsa, ilgili AB üyesi devlet hukuku uyarınca kurula ortak bir temsilci atanır.

[244]Barnard-Wills/Pauner Chulvi/De Hert, s.591'den aktaran Develioğlu , 2017 , **a.g.k.** , 148.

AB komisyonu, Avrupa Veri Koruma Kurulu'nun toplantılarına ve faaliyetlerine oy hakkı olmadan belirlediği bir temsilci vasıtasıyla katılabilir. Avrupa Veri Koruma Kurulu başkanı, Avrupa Birliği Komisyonu'na kurulun faaliyetleri hakkında bilgi verir.

Avrupa Veri Koruma Kurulu, bağımsızdır ve hiçbir gerçek veya tüzel kişiden talimat almaz.

Kurulun esas görevi, resen veya AB komisyonunun talebiyle Tüzük'ün yeknesak bir şekilde uygulanmasıdır. Bunun sağlanması için Tüzük, Avrupa Veri Koruma Kurulu'nun görevlerini şöyle sıralamıştır:

- Tüzük'ün doğru uygulanmasını gözetir ve sağlar,
- AB dahilinde, kişisel verilerin korunmasına ilişkin her konuda AB Komisyonu'na danışmanlık yapar,
- Bağlayıcı kurumsal kurallar için veri sorumluları, veri işleyicileri ve denetim makamları arasındaki bilgi paylaşımının biçimi ve prosedürü konusunda AB Komisyonu'nun danışmanlığını yürütür,
- Kamuya açık iletişim hizmetlerinden kişisel verilerin bağlantılarının, kopyalarının silinmesine yönelik işleyişlere ilişkin rehberler ve tavsiyeler yayınlar,
- Kendiliğinden veya bir kurul üyesinin veya AB Komisyonu'nun talebiyle, Tüzük'ün yeknesak uygulanmasını teşvik amacıyla rehber ve tavsiyeler yayınlar,
- Profillemeye dayalı kararların kriterlerini ve koşullarını belirlemek için rehber ve tavsiyeler yayınlar,
- Kişisel veri güvenliğinin ihlali sayılan hallerin tespiti ve bu ihlallere karşı yapılacak ihbarlara yönelik tavsiye ve rehber yayınlar,
- Kişisel veri güvenliği ihlalinin gerçek kişilerin hak ve özgürlüklerini sokacağı yüksek risk durumlarına ilişkin tavsiye ve rehber yayınlar,
- Bağlayıcı kurumsal kurallar ve onlara dayanan aktarımlar hakkındaki şartlara ilişkin rehber ve tavsiyeler yayınlar,
- AB Komisyonu'na uygunluk kararının olmadığı durumlarda AB üyesi olmayan üçüncü ülkelere ve uluslararası kuruluşlara yapılan kişisel veri aktarımlarının ölçüt ve koşullarına ilişkin rehber ve tavsiyeler yayınlar,

- Denetim makamlarının yetkilerinin kullanılmasına ilişkin rehberler hazırlar,
- İdari para cezalarının belirlenmesine ilişkin olarak denetim makamları için rehberler hazırlar,
- Yayınladığı rehber ve tavsiyelerin uygulanmasını denetler,
- Gerçek kişilerin tüzük ihlallerini bildirmesine ilişkin ortak usuller belirlemek amacıyla rehber, tavsiye ve uygulama örnekleri yayınlar,
- Davranış kurallarının yazılmasını ve kişisel veri koruması sertifikasyon mekanizmaları ile kişisel veri koruması mühür ve markalarının tesisini teşvik eder,
- Sertifikasyon kuruluşlarına akreditasyon verir ve akreditasyonları düzenli olarak değerlendirir. Akreditasyon verilmiş kuruluşlara ilişkin ve üçüncü ülkelerde yerleşik akreditasyon sahibi veri sorumluları veya veri işleyicilere ilişkin kamuya açık sicil tutar,
- Sertifikasyon şartlarına ilişkin AB Komisyonu'na görüş bildirir,
- Standartlaştırılmış simgelere ilişkin AB Komisyonu'na görüş bildirir,
- Bir üçüncü ülke veya uluslararası kuruluşta bulunan korumanın seviyesinin yeterli olup olmadığının değerlendirilmesine ilişkin olarak AB komisyonuna görüş bildirir,
- Tutarlılık mekanizması kapsamında denetim makamlarının taslak kararları hakkında görüş bildirir, uyuşmazlık çözümü ve ivedilik prosedürü kapsamında bağlayıcı kararlar verir,
- Denetim makamları arasında işbirliğini, bilgi paylaşımını ve iyi uygulamaları teşvik eder,
- Denetim makamları arasında ortak eğitim programlarını teşvik eder ve personel değiş tokuşunu kolaylaştırır,
- Dünyadaki diğer denetim makamları ile mevzuata ve uygulamaya ilişkin bilgi birikimi ve dokümantasyon paylaşımını teşvik eder,
- AB seviyesinde yazılmış davranış kuralları hakkında görüş bildirir,
- Tutarlılık mekanizmasında ele alınan konular hakkında denetim makamları ve mahkemeler tarafından alınan kararlara ilişkin kamuya açık bir elektronik sicil tutar.

AB komisyonu, Avrupa Veri Koruma Kurulu'ndan tavsiye istediği durumlarda işin aciliyetini de göz önünde bulundurarak bir süre belirleyebilir.

Avrupa Veri Koruma Kurulu; rehber, tavsiye ve uygulama örneklerini AB Komisyonu'na ve 93. maddede AB komisyonuna yardımcı olması için teşekkül eden komiteye iletir ve kamuya sunar.

Avrupa Veri Koruma Kurulu, ilgili hallerde tarafların görüşünü alır ve makul süre içinde yorum yapmalarına imkân tanır. Avrupa Veri Koruma Kurulu, Tüzük'ün 76. maddesindeki "*usul kurallarına uygun olarak Avrupa Veri Koruma Kurulu'nun gerekli gördüğü hallerde, Kurul'un görüşmeleri gizli şekilde gerçekleştirilir*" hükmüne uymak koşuluyla bu görüş alma prosedürünün sonuçlarını kamuya sunar.

Tüzük'ün 71. maddesine göre Avrupa Veri Koruma Kurulu, gerçek kişilerin AB'de ve ilgili hallerde üçüncü ülkelerde ve uluslararası kuruluşlarda korunmasına ilişkin kamuoyuna sunulmak üzere bir yıllık bir rapor hazırlar ve Avrupa Parlamentosu'na, Avrupa Konseyine, AB Komisyonu'na iletir.

Tüzük'ün 72. maddesine göre Tüzük'te aksi öngörülmedikçe Avrupa Veri Koruma Kurulu, kararlarını üyelerinin salt çoğunluğu ile alır.

Tüzük'ün 73. maddesine göre Avrupa Veri Koruma Kurulu, üyelerinden salt çoğunluk ile başkan ve iki yardımcı seçer. Bunlar, bir kere yenilenebilecek şekilde beş sene görev yapar.

Tüzük'ün 74. maddesinde Avrupa Veri Koruma Kurulu başkanı'nın görevleri sıralanmıştır. Buna göre kurul başkanı;

- Kurulu toplantıya çağırır ve toplantı gündemini belirler;
- Kurul tarafından alınan kararları öncü denetim makamı ve ilgili denetim makamlarına bildirir;
- Kurulun görevlerini zamanında ifa etmesini sağlar.

Kurulun usul kuralları ile kurul başkanı ve yardımcıların arasındaki görev paylaşımını kurul belirler.

Avrupa Veri Koruma Kurulu'nun sekreteryası, Tüzük'ün 75. maddesinde düzenlenmiştir.

Avrupa Veri Koruma Kurulu'nun Avrupa Kişisel veri denetmeni tarafından temin edilen bir sekreteryası bulunmaktadır. Sekreterya, sadece kurul başkanından talimat alarak görevlerini yerine getirir.

Kurulun sekreteryası, kurulun gündelik işleyişini, yazışmalarını, tercüme işleri, toplantı, görüş ve kararlarının hazırlanmasından sorumludur.

Tüzük'ün 76. maddesine göre kurul, görüşmelerini gizli bir şekilde gerçekleştirme kararı alabilir.

## SONUÇ

Kişisel veriler, uluslararası kaynaklarda "gerçek kişiye ait belirli ve belirlenebilir her türlü bilgi" olarak tanımlansa da tüzel kişilerin de zamanla bu tanıma dahil edilerek koruma altına alındığı görülmektedir.

Kişisel verilerin korunması sorunu, sadece bireylerin özel hayatına ilişkin bir mesele değildir. Günümüz koşullarında küçük veya büyük şirketler ve devletler nezdinde kişisel verilerin korunması konusunu ana gündem olarak yerini korumaktadır. Kişisel verilerin korunması artık bir ulusal güvenlik meselesi haline gelmiştir. AB üyesi devletlerin bu konuda en başından beri duyarlı olduğu görülse de ABD başta olmak üzere diğer devletlerin bu konuda aynı hassasiyeti göstermediği, Avrupa Birliğini geriden takip ettikleri görülmektedir.

Kişisel verilerin korunmasına ilişkin ihtiyacın masaya yatırılması bilgisayarın gelişmesiyle başlamıştır. Zira bilgisayar, bilgilerin serbestçe dolaşabileceği bir mecra doğurmuştur. Bu durum bireylerin kaygılarını artırmış ve vatandaşlarının bu kaygısına kayıtsız kalamayan devletleri bir takım yasal düzenlemeler yapma mecburiyetine sürüklemiştir. Burada devletlerin tek kaygısının vatandaşlarının kişisel bilgilerini güvenceye almak olduğunu söylemek gerçeğe aykırı bir yaklaşımdır. Zira devletler, öncelikle diğer devletlerle olan ekonomik etkileşiminin sekteye uğramasından endişe ettikleri için kişisel verilerin korunmasını gündemlerine almışlardır. Dolayısıyla tamamıyla insan haklarına saygı düşüncesinin egemen olduğu bir yasalaşma sürecinden bahsedilemez. Fakat buna yönelik girişimlerin dolaylı olarak insan haklarının da korunmasına hizmet ettiği göz ardı edilemez.

Kişisel verilerin korunmasının temelinin ilk olarak hekimlerin sır saklama yükümlülüğünün var olduğunun kabulüyle ortaya çıktığı yönünde baskın bir görüş vardır. Bunu diğer meslek gruplarının sır saklama yükümlülükleri izlemiştir.

Kişisel verilerin korunmasına yönelik uluslararası kaynakların bir kısmının doğrudan veri korumaya yönelik hüküm ihtiva etmediği bazılarının ise sadece veri korumaya yönelik olduğu görülmektedir. Birinci gruptaki düzenlemelerin asıl amacının başta temel insan haklarını güvence altına almak olduğu, kişisel verilerin korunmasının bunun dolaylı sonucu olduğu görülmektedir. Örneğin AİHS'in, Medeni ve Siyasal Haklar Sözleşmesinin, İnsan Hakları Evrensel Bildirgesinin birinci gruba giren

düzenlemeler olduğu söylenebilir. İkinci gruptaki düzenlemeler ise kişisel verilerin yeterince korunmadığı kaygısıyla ortaya çıkmış, doğrudan kişisel verilerin korunması kaygısı güden düzenlemelerdir. AB'nin ve AK'nin veri korumaya yönelik düzenlemelerinin ikinci gruba girdiği söylenebilir.

Özellikle Avrupa kaynaklı veri koruma mevzuatlarının kişisel verilerin korunmasına yönelik teorik açıdan ve uygulama açısından iyi bir yol gösterici olduğu görülmektedir. Bu düzenlemeler incelendiğinde yasa koyucuların kişisel verilerin korunmasına yönelik hassasiyetleri, herhangi bir yasal boşluğun doğmamasına önem verdiklerini göstermektedir.

Kişisel verilerin korunmasına yönelik uluslararası kaynakların bazılarının bağlayıcılık vasfı taşımadığı, bazılarının ise bağlayıcı olduğu görülmektedir. Örneğin AİHS, Medeni ve Siyasal Haklar Sözleşmesi, 108 sayılı Sözleşme ve AB Genel Veri Koruma Tüzüğü gibi düzenlemelerin bağlayıcı olduğu; 95/46 sayılı Veri Koruma Yönergesi başta olmak üzere sair uluslararası düzenlemelerin bağlayıcı olmadığı görülmektedir.

Kişisel verilerin korunmasına yönelik mevzuatın içeriğine bakıldığında kişisel verilere ilişkin tanımlar getirdiği, kişisel verilerin korunması için bir takım denetim organları kurduğu, bireylere kişisel verilerin korunmasına yönelik haklar tanıdığı, verilerin korunmasından sorumlu merciler oluşturduğu ve bu mercilere bazı sorumluluklar yüklediği görülmektedir.

Kişisel verilerin gelişmesine ilişkin mevzuatlara bakıldığında bir kazuistikleşme olduğu görülmektedir. Teknolojinin gelişmesiyle doğru orantılı olarak kişisel verilere ilişkin sorunların da çeşitlenmesi, buna ilişkin çözümlerinde çeşitlenmesi gerekliliğini ortaya çıkarmıştır. Bu da yasa koyucuların mevzuatta her ayrıntıyı düzenlemeleri ihtiyacını doğurmuştur. Örneğin *Yönerge*'nin yürürlüğe girmesi, zamanla ortaya çıkan meselelere çözüm getirmediği için bu Yönerge'yi tamamlayıcı yönergelerin yürürlüğe konduğu görülmektedir. *Yönerge*'yi telekomünikasyon alanında tamamlayan 97/66 sayılı Direktif ve Elektronik İletişim alanında tamamlayan 2002/58 sayılı Elektronik İletişim Direktifi buna örnek gösterilebilir. Bu husus bir gerçeği de ortaya koymaktadır ki kişisel verilerin korunması gibi durağan olmayan bir alanda ortaya konan bir mevzuatın uzun soluklu çözüm getireceği öngörülemez. Bu konudaki diğer bir örnek de

AİHS'in 8. maddesidir. AİHS, özel hayatın korunmasına ilişkin evrensel nitelikte bağlayıcılığı olan bir hükümdür. Fakat AİHS'in 8. maddesini kişisel verilerin koruyan bir hüküm haline getiren, AİHM içtihatları olmuştur. AİHM, uhdesinde bulunan uyuşmazlıkları yorumlama yetkisi dahilinde kişisel verilerin korunmasına yönelik içtihatlar geliştirmiştir ve bu içtihatlar yol gösterici niteliktedir. Dolayısıyla kişisel verilerin korunmasında güçlü bir hukuki dayanak olan AİHS'in 8. maddesinin bu vasfını sürdürmesi, AİHM'in kişisel verilerin korunmasına verdiği önemin sona ermemesi ile bağlantılıdır. Bunun gibi ABAD'ın vermiş olduğu kararlar da kişisel verilerin korunması hususunda oluşturulan mevzuatların önemini ve canlılığını korumakta mahkemelerin önemli bir vazife ifa ettiğini göstermektedir. Zira ABAD da AİHM gibi vermiş olduğu kararlar ile bu mevzuatların uygulayıcılarına yol göstermekte, potansiyel mağdur olan bireylerin de korunması için gerekli ortamı hazırlamaktadır.

Kişisel verilerin korunmasına yönelik uluslararası mevzuatın yeterli korumayı sağlama noktasında bir gelişme kaydettiği görülmektedir. Zamanla her soruna çözüm getiren, her ayrıntıyı düzenleme altına alan mevzuatların yeterli korumayı sağlamadıklarını söylemek, bu konuda çaba gösterenlere bir haksızlık olacaktır. Burada korumasızlığı doğuracak olan; veri işleyicilerinin, veri sorumlularının, denetim makamlarının mevzuatı kötüniyetle uygulamaları ve mevzuattaki boşluklardan faydalanma çabası göstermeleri, yargı makamlarının da bireyi korumayan kararlar vermeleridir. Fakat esas sorun, bunlardan ziyade dünyada eşdeğer koruma düzeylerinin sağlanmamasıdır. Çünkü teknolojinin gelişmesiyle, iletişim olanaklarının çoğalmasıyla küçük bir köy haline gelen dünyada; bir devletin diğer devletlerle, bir devletin vatandaşlarının diğer devletin vatandaşlarıyla etkileşimden uzak kalması mümkün değildir. Ve her bir etkileşimin kişisel veriler üzerinde tesiri vardır. Bu etkileşimde taraflardan birinin yeterli koruma sağlaması, karşı tarafın yetersiz koruma düzeyi karşısında önemini yitirecektir. Bu sebeple kişisel verilerin korunması bazı devlet veya bireylerin kaygısı yerine tüm dünyanın kaygısı olmadıkça, kaygı duyan devlet veya bireylerin yeterli korumayı sağladıkları bir yanılgıdan ibaret olacaktır.

Kişisel verilerin korunmasında ortak kaygının oluşması da ortak bilincin gelişmesiyle mümkün olacaktır. Burada devletlerin birbirini teşvik etmesi ve zorlaması gerekmektedir. Nasıl ki nükleer silahlanmaya karşı gerekli hassasiyeti göstermeyen

devletlere yaptırım uygulanıyorsa; yeterli veri koruma düzeyine ulaşmaya kayıtsız kalan ülkelere karşı da çeşitli yaptırımlar uygulanmalıdır. Zira kişisel verilerin korunması; ülkelerin bilinçlenmesini, kendiliğinden çaba göstermelerini beklemeyi gerektirmeyecek kadar aciliyeti olan bir meseledir.

## KAYNAKÇA


Ağıralan, E.(2015). *Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Mahremiyet Etki Değerlendirmesi*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü.

Akgül, Aydın.(2013). *Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi*. Yayımlanmış Doktora Tezi. Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü.

Akıncı, A. N.(2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*, T.C. Kalkınma Bakanlığı, Yayın No: 2968

Aksoy, H. C.(2008). *Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü.

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

Altuner, İ.(1990). Hipokrat Yemini. *Iğdır Üniversitesi Sosyal Bilimler Dergisi*, S:7, s.1-7

Arıklı, B.(2019). *KKTC hukukunda kişisel verilerin korunması*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi, Lisansüstü Programlar Enstitüsü.

Arslan, B. (2018). *Bulut Bilişim'in avantajları ve dezavantajları*. Yayımlanmamış Yüksek Lisans Projesi. İstanbul: Maltepe Üniversitesi Sosyal Bilimler Enstitüsü.

Aşıkoğlu, Ş. İ.(2018). *Avrupa Birliği Ve Türk Hukukunda Kişisel Verilerin Korunması Ve Büyük Veri*. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Avcı, Y.(2019). *Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.

Avcıoğlu, H. N. (2018). *Türk Hukukunda Kişisel Verilerin Korunması Hakkı.* Yüksek Lisans Tezi. Konya:KTO Karatay Üniversitesi, Sosyal Bilimler Enstitüsü

Aydın, S. E.(2014). *Aihm İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu*. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Ayözger, A. Ç.(2016). *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*. Yayımlanmamış Doktora Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Başalp, N. (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21 (1), 77-106.

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

Başar C. (2019).*Türk İdare Hukuku ve Avrupa Birliği Hukuku ışığında kişisel verilerin korunması*. Yayımlanmamış Doktora Tezi. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü.

Boydak, A. (2017). *İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış*. Türkiye Adalet Akademisi Dergisi , (30) , 321-336.

Boz, A.(2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü.

Bozkurt, E.(2003). *İnsan Haklarının Korunmasında Uluslararası Hukukun Rolü*. Ankara: Nobel Akademik Yayınları.

Çalık, T(2016). Birleşmiş Milletler İnsan Hakları Sözleşmeleri Kapsamında İnsan Haklarının Korunması. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*. S:24, 69-120.

Çelik, Y(2017). Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı. *Türkiye Adalet Akademisi Dergisi*. (32) , 391-410.

Çokmutlu, M.(2014). *Türk Ceza Hukukunda Kişisel Verilerin Korunması*. Yayımlanmamış Doktora Tezi. Kocaeli: Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü.

Dal, U. (2019). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti. *Kişisel Verileri Koruma Dergisi*, 1 (1) , 21-33.

Develioğlu, H. M.(2017) *6698 sayılı Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayıncılık.

Dinç, E.(2006). *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye'nin Durumu*. Yayımlanmamış Yüksek Lisans Tezi. Diyarbakır: Dicle Üniversitesi, Sosyal Bilimler Enstitüsü.

Dinkci, F.(2014). *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye Örneği*. Yayımlanmamış Yüksek Lisans Tezi. Ondokuz Mayıs Üniversitesi, Sosyal Bilimler Enstisüsü.

Dülger, M. V.(2018). İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C.5(1), 71-143.

Erdinç, G. H.(2017). *Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Teknik Üniversitesi Bilişim Enstitüsü.

Ersoy, U.(2009). *Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması"*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi, Sosyal Bilimler Enstitüsü.

Gözüm, Z. U.(2019). *Kişisel Verilerin Korunmasının İş İlişkisi Açısından Değerlendirilmesi*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü.

Gül, İ. ve Alagöz İ.(2016). *Yeni Bir Güvenlik Sorunu: Kişisel Verilerin Korunmasına Yönelik İhlaller ve Uluslararası Düzenlemeler*. Ankara: Yargı Yayınevi.

Gür, İ.(2009). *Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar Ve Çözüm Yolları*. Yayımlanmış Yüksek Lisans Tezi. Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü.

Hatipoğlu, S.(2019). *Kişisel Verilerin Korunması Ve İdarenin Sorumluluğu*. Yayımlanmamış Yüksek Lisans Tezi. Edirne: Trakya Üniversitesi Sosyal Bilimler Enstitüsü.

Helvacı, S., Erlüle, F.(2011). *Medeni Hukuk*. İstanbul: Legal Kitabevi.

Kağıtcıoğlu M.(2016). Kişisel Verileri Koruma Kurumu'na İdare Hukuku Çerçevesinden Bir Bakış. *Aurum Journal of Social Sciences*, 1 (2), 77-99.

Kalabalık, H.(2005). *İnsan Hakları Hukukuna Giriş*. Ankara: Seçkin Yayınları.

Kalabalık, H.(2017). *İnsan Hakları Hukuku*. Ankara:Seçkin Yayınları.

Karabulut, R.(2014). *Kişisel Verilerin Korunması ve Kolluk hizmetleri*. Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır: Dicle Üniversitesi, Sosyal Bilimler Enstitüsü.

Karınçu, S.(2019). *Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve İşlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*. 69 (1-2) , 317-334

Kaya M.B. ve Taştan F. G. (2019).*Kişisel Veri Koruma Hukuku*. İstanbul: Oniki Levha Yayınları.

Kılıç, K. (2016) *Kişisel Verilerin Korunması ve 6698 Sayılı Kanun*. Yayımlanmamış Yüksek Lisans Tezi. Erzurum: Atatürk Üniversitesi Sosyal Bilimler Enstitüsü.

Kılınç, D.(2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 61, S. 3, s. 1089-1170.

Korkmaz, İ.(2019). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*. Ankara: Seçkin Yayınları.

Küzeci, E.(2010). *Kişisel Verilerin Korunması*. Doktora Tezi, Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü.

Küzeci, E.(2018). *Kişisel Verilerin Korunması*. Ankara: Turhan Kitabevi.

Oğuz, S.(2018). Kişisel Verilerin Korunması Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi*. 13 (2) , 121-138

Orak, B. (2019). *Kişisel Sağlık Verilerinin Korunması*. Yüksek Lisans Tezi. Ankara: Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü

Özdemir, H.(2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Ankara: Seçkin Yayıncılık.

Öztunay, B.(2019). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşverenin Yönetim Hakkının Sınırları*. Yayımlanmamış Yüksek Lisans Tezi. İzmir: İzmir Ekonomi Üniversitesi Sosyal Bilimler Enstitüsü.

Selek, O.(2019). *Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması*. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 21(2), 911-951

Sert, Ş.(2019).*Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*. Ankara: Seçkin Yayınları

Solmaz E.(2019). Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı. *İdare Hukuku ve İlimleri Dergisi*, 18(1), 61-78.

Soysal T.(2019). Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi. *Uyuşmazlık Mahkemesi Dergisi*, 0 (13) , 339-422.

Şimşek, O.(2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*. İstanbul: Beta Yayınları.

Taştan, F. G.(2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. İstanbul: On İki Levha Yayınları.

Uncular, S.(2018). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. Ankara: Seçkin Yayınları.

Uyarer, S. G.(2019). *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Ankara:Seçkin Yayınları.

Uyarer, S. G.(2019). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Galatasaray Üniversitesi, Sosyal Bilimler Enstitüsü.

Uygun, M.(2010). *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi ışığında kişisel verilerin korunması*. Yayımlanmış Yüksek Lisans Tezi. Ankara:Gazi Üniversitesi, Sosyal Bilimler Enstitüsü.

Üzeltürk, H.(2018). Avrupa Birliği Genel Veri Koruma Düzenlemesi. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*. C.15, 2018/2, 161-179

Yıldırım, F. N.(2019). *Avrupa Birliği Ve Türk Hukukunda Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü.

Yılmaz, B.(2019). *Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. Yayımlanmış Doktora Tezi. Ankara: Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü.

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

Yücedağ N.(2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*.75 (2) , 765-790.

ABAD. *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.* 13/05/2014 , 131/12

ABAD. *Bodil Lindqvist*. 06/11/2003, C-101/01

AİHM. *Klass ve diğerleri ve. Almanya*. 21.05.1992 , 15473/89

AİHM. *Von Hannover ve Almanya* 24.06.2004, 59320/00

AİHM. *Rotaru ve Romanya kararı*. 05.07.2005, 28341/95

AİHM. *M.L ve W.W. v. Almanya*. 28.06.2018, 60798/10 , 65599/10

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5bd5c87b20ae83.54428221 (Erişim Tarihi:28.10.2018)

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5bd5c48c0f5de8.54075063 (Erişim Tarihi:28.10.2018)

https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (Erişim Tarihi:05.11.2018)

https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML(Erişim Tarihi:16.03.2019)

https://kisiselveri.com/9546ec-turkce (Erişim Tarihi:16.03.2019)

https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML(Erişim Tarihi:16.03.2019)

https://kisiselveri.com/9546ec-turkce (Erişim Tarihi:16.03.2019)

http://sosbilder.igdir.edu.tr (Erişim Tarihi:07.02.2019)

https://www.echr.coe.int/Documents/Convention_TUR.pdf (Erişim Tarihi:23.02.2019)

https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708

(Erişim Tarihi:26.02.2019)

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim Tarihi:26.02.2019)

https://www.refworld.org/pdfid/3ddcafaac.pdf (Erişim Tarihi:26.02.2019)

https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN(Erişim Tarihi:26.02.2019)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN

(Erişim Tarihi:26.02.2019)

http://www.oecd.org/internet/ieconomy/1840065.pdf (Erişim Tarihi:07.05.2019)

https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708

(Erişim Tarihi:26.02.2019)

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429
(Erişim Tarihi:26.02.2019)

https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708

(Erişim Tarihi:26.02.2019)

https://eur-lex.europa.eu/legal
content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=DE(Erişim Tarihi:26.02.2019)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp
(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp
(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim
Tarihi:25.02.2020)

http://hudoc.echr.coe.int/tur?i=001-45549 (Erişim Tarihi:22.01.2020)

http://hudoc.echr.coe.int/tur?i=001-112080 (Erişim Tarihi:22.01.2020)

http://hudoc.echr.coe.int/tur?i=001-69880 (Erişim Tarihi:22.01.2020)

http://hudoc.echr.coe.int/tur?i=001-183947 (Erişim Tarihi:23.01.2020)

https://eur-lex.europa.eu/legal
content/EN/TXT/HTML/?uri=CELEX:62012CJ0131_SUM&qid=1579769680599&fro
m=EN (Erişim Tarihi:23.01.2020)

http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_13.pdf

(Erişim Tarihi:23.02.2020)

https://www.un.org/en/universal-declaration-human-rights/( Erişim Tarihi:23.01.2020)

http://www.unicef.org.tr/files/bilgimerkezi/doc/insan%20haklari%20evrensel%20beyannemesi.pdf (Erişim Tarihi:02.11.2019)

https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf

(Erişim Tarihi:02.11.2019)

http://www.un.org.tr/humanrights/images/pdf/1-insan-haklari-evrensel-beyannamesi.pdf (Erişim Tarihi:02.11.2019)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

http://www.unicankara.org.tr/doc_pdf/metin133.pdf (Erişim Tarihi:16.03.2019)

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim Tarihi:16.03.2019)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://rm.coe.int/1680078b37 (Erişim Tarihi:24.01.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
(Erişim Tarihi:02.03.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ddcafaac

(Erişim Tarihi:20.03.2019)

https://www.refworld.org/pdfid/3ddcafaac.pdf ( Erişim Tarihi:05.03.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://eur-lex.europa.eu/legal
content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

(Erişim Tarihi:20.03.2019)

https://kisiselveri.com/9546ec-turkce (Erişim Tarihi:20.03.2019)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_8.pdf

(Erişim Tarihi:09.03.2020)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62001CJ0101&from=EN

(Erişim Tarihi:09.03.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:62012CJ0131_SUM&qid=1579769680599&from=EN (Erişim Tarihi:23.01.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/1997/wp4_en.pdf (Erişim Tarihi:27.04.2019)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:25.02.2020)

https://www.mbkaya.com/hukuk/veri-koruma-hukuku.pdf (Erişim Tarihi:11.04.2020)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31997L0066&from=EN

(Erişim Tarihi:05.05.2019)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=DE

(Erişim Tarihi:10.07.2019)

http://www.oecd.org/internet/ieconomy/1840065.pdf (Erişim Tarihi:07.05.2019)

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429 (Erişim Tarihi:07.05.2019)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=DE

(Erişim Tarihi:11.07.2019)

https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708

(Erişim Tarihi:06.07.2019)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

(Erişim Tarihi:27.08.2019)

https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (Erişim Tarihi:27.08.2019)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

(Erişim Tarihi:12.04.2020)

http://www.abgm.adalet.gov.tr/abadaletdivani/abadaletdivani.html

(Erişim Tarihi:05.12.2019)

http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_13.pdf

(Erişim Tarihi:05.12.2019)

http://openaccess.maltepe.edu.tr/xmlui/handle/20.500.12415/3403#sthash.ktM8Ai2q.diEHLBIN.dpbs (Erişim Tarihi:16.04.2020)

https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:32015L1535&from=EN

(Erişim Tarihi:09.09.2019)

https://en.wikipedia.org/wiki/Commission_nationale_de_l'informatique_et_des_libert%C3%A9s (Erişim Tarihi:25.03.2020)

https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

(Erişim Tarihi:13.04.2020)

https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:62012CJ0131_SUM&qid=1579769680599&from=EN (Erişim Tarihi:25.03.2020)