



Avrupa Konseyi 108+ Konvansiyonu Açıklayıcı Raporu

Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Sözleşme – 108+ Konvansiyon



www.coe.int/dataprotection

İçindekiler_

Bakanlar Komitesi'nin Kararı	3
Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Modernize Edilmiş Sözleşme.....	3
Açıklayıcı Rapor	14

Bakanlar Komitesi'nin Kararı

Bakanlar Komitesi'nin 128inci oturumu, Helsingör, 18 Mayıs 2018

Kararlar

Bakanlar Komitesi

1. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (ETS No.108) değiştiren taslak Protokole ilişkin Parlamenter Meclis'in 296 numaralı Görüşü'nü (2017) dikkate almış;
2. CM(2018)2-final dokümanında yer verilen Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (ETS No.108) değiştiren Protokol'ü kabul etmiş ve CM(2018)2-addfinal dokümanında yer verilen Açıklayıcı Rapor'u, Protokol'e ilişkin bir enstrüman olarak sunmuştur;
3. Modernize edilmiş Sözleşme nezdinde en kapsayıcı veri koruma yasal rejiminin oluşmasının kolaylaştırılması ve Konvansiyon Komitesi'nde devletlerin mümkün olan en yüksek seviyede temsil edilmesi için 108 Sayılı Sözleşme'ye hali hazırda Taraf Devletlerden Protokol'e katılımın hızlı ve maksimum sayıda olmasının önemini belirtmiş;
4. Protokol'ün 25 Haziran 2018'de¹ Parlamenter Meclis'in üçüncü yarı oturumu

5. sırasında Strazburg'da imzaya açılmasına karar vermiş;
6. Konvansiyon'a taraf üye devletleri ve diğer tarafların, Protokol'ün imzaya açılmasından itibaren üç sene içerisinde yürürlüğe girmesi için gereken aksiyonları, gecikmesizin almalarını ve derhal, her halükarda Protokol'ün imzaya açıldığı tarihten itibaren bir yıllık süreyi geçmemek üzere, yerel hukuklarında Protokol'ün bağlayıcılık kazanması, onaylanması veya kabul edilmesine yönelik ulusal hukuklarındaki prosedürleri derhal başlatmalarını önemle tavsiye etmiştir;
7. Protokol'ün Madde 37 (2) hükmü uyarınca değişik Konvansiyon'un yürürlüğe girmesini takiben sadece Protokol'ü kabul eden veya onaylayan devletlerin değişik Konvansiyon'dan doğan yükümlülüklerle bağlı olacağını altını çizmiş;
8. Bakanlarını, incelemeyen en geç bir ay önce Konvansiyon'a taraf her bir üye ülke ve diğer taraflarca Genel Sekreter'e sağlanan bilgiler doğrultusunda, ilk kez Protokol'ün imzaya açılması tarihinden bir yıl sonra ve senede iki defa Protokol'ün onaylanmasına ilişkin genel kapsamlı inceleme yapması için talimat vermiştir.

Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Modernize Edilmiş Sözleşme²

Giriş

Avrupa Konseyi üye devletleri ve diğer imzacı taraflar,

Avrupa Konseyi'nin amacının, özellikle hukukun üstünlüğüne ve insan hakları ile temel özgürlüklere saygılı olarak, üyeleri arasında daha yakın bir birliğin gerçekleştirilmesi olduğuna inanarak;

¹ Bakanlar Komitesi, imzaya açma tarihini 10 Ekim 2018 tarihine erteleme kararı almıştır.

² 18 Mayıs 2018'de Helsingör'de Bakanlar Komitesi tarafından 128inci oturumda kabul edilen Kişisel

Verilerin İşlenmesi Karşısında Bireylerin Korunması için Sözleşme'yi değiştiren protokol.

Veri işleme, kişisel veri akışlarındaki çeşitlilik, yoğunluk ve küreselleşme göz önünde bulundurulduğunda her bir bireyin insanlık onurunun, insan hakları ve temel özgürlüklerinin korunmasının ve kendi kişisel verilerini ve bunların işlenmesini kontrol etme hakkına dayanan kişisel özerkliğinin güvence altına alınmasının gerektiğine inanarak;

Kişisel verilerin korunması hakkının toplumdaki rolü dikkate alınarak değerlendirilmesinin ve bu hakkın, ifade özgürlüğü dahil olmak üzere diğer insan hakları ve temel özgürlükleri ile bağdaştırılması gerektiğinin üzerinde durarak;

İşbu Sözleşme'nin, içerisinde yer alan kuralların uygulanmasında resmi belgelere erişim hakkı ilkesini dikkate aldığını belirterek;

Gizliliğe saygı ve kişisel verilerin korunmasına ilişkin temel değerlerin küresel seviyeye taşınması gerektiğine inanarak ve bu şekilde insanlar arasında serbest bilgi akışına katkıda bulunarak;

Aşağıdaki hususlarda anlaşmışlardır:

Bölüm 1 – Genel Hükümler

Madde 1 – Konu ve Amaç

İşbu Konvansiyon'un amacı, uyruğu veya ikamet yeri ne olursa olsun kişisel verilerin işlenmesine ilişkin olarak her bireyin korunması ve bu şekilde, başta gizlilik hakkı olmak üzere bireylerin insan hakları ve temel özgürlüklerine gösterilecek saygıya katkıda bulunulmasıdır.

Madde 2 – Tanımlar

İşbu Konvansiyon'un amaçları bakımından:

- a. “Kişisel veri”, kimliği belirli veya belirlenebilir bir gerçek kişi (“ilgili kişi”) hakkındaki tüm bilgileri,
- b. “Veri İşleme”, elde etme, saklama, muhafaza etme, değiştirme, yeniden düzenleme, açıklama, elde edilebilir hale getirme, silme veya imha etme gibi kişisel veriler üzerinde gerçekleştirilen herhangi bir işlem veya işlem setini veya bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanmasını,
- c. Otomatik işleminin söz konusu olmadığı hallerde “veri işleme”, belirli bir kriter uyarınca erişilebilir veya yeniden düzenlenebilir olan yapılandırılmış kişisel veri seti içerisindeki kişisel veriler üzerinde gerçekleştirilen işlem veya işlem setini;
- d. “Veri sorumlusu”, tek başına ve diğerleri ile birlikte veri işlemeye ilişkin karar alma yetkisine haiz gerçek veya tüzel kişileri, kamu kurumunu, servisi, birimi veya diğer kuruluşları,
- e. “Alıcı”, verilerin açıklandığı veya erişime açıldığı gerçek veya tüzel kişileri, kamu kurumunu, servisi, birimi veya diğer kuruluşları,
- f. “Veri işleyen”, veri sorumlusu adına kişisel veri işleyen gerçek veya tüzel kişileri, kamu kurumunu, servisi, birimi veya diğer kuruluşları,

İfade etmektedir.

Madde 3 – Kapsam

1. Her bir Taraf, yetki alanındaki kamu sektöründe ve özel sektörde gerçekleşen veri işlemlerine işbu Konvansiyon'u uygulamayı ve bu şekilde her bireyin kişisel verilerinin korunması hakkını korumayı taahhüt ederler.
2. İşbu Konvansiyon, tamamen kişisel veya ev halkına ilişkin faaliyetler kapsamında bireyler tarafından gerçekleştirilen kişisel veri işlemlerine uygulanmayacaktır.

Bölüm 2 – Kişisel Verilerin Korunmasına İlişkin Temel İlkeler

Madde 4 – Tarafların Görevleri

1. Her bir Taraf, işbu Konvansiyon'un hükümlerine işlerlik kazandırmak amacıyla hukuklarında gerekli önlemleri alır ve bu hükümlerin etkin bir şekilde uygulanmasını temin eder.
2. Bu önlemler her bir Tarafça alınacak ve Konvansiyon'un onay veya Konvansiyon'a katılım tarihinde yürürlüğe girmiş olacaktır.
3. Her bir Taraf:
 - a. Konvansiyon'un hükümlerinin uygulanması için hukukunda aldığı önlemlerin etkinliğini Bölüm 5'te düzenlenen Konvansiyon Komitesi'nin değerlendirmesine izin vereceğini; ve
 - b. Bu değerlendirme sürecine aktif olarak katkıda bulunacağını taahhüt eder.

Madde 5 – Veri İşlemenin Meşruluğu ve Verilerin Niteliği

1. Veri işleme, gözetilen meşru amaca ilişkin olarak orantılı olur ve işlemenin tüm aşamalarında, kamusal veya özel menfaatler ile söz konusu haklar ve özgürlükler arasındaki adil dengeyi ortaya koyar.
2. Her bir Taraf, veri işlemenin, ilgili kişinin özgür, spesifik, bilgilendirmeye dayanan ve açık rızasına veya kanunla düzenlenen diğer bir meşru şarta dayalı olarak gerçekleşmesini sağlar.
3. İşlemeye konu kişisel veriler hukuka uygun olarak işlenir.
4. İşlemeye konu kişisel veriler:
 - a. Adil ve şeffaf bir şekilde işlenir;
 - b. Açık, belirli ve meşru amaçlarla toplanır ve bu amaçlara aykırı bir şekilde işlenmez; kamu menfaati kapsamında arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla veya istatistikî amaçlarla ikincil işleme, uygun güvencelere tabi olarak bu amaçlara uygun olur;
 - c. İşleme amaçlarına göre yeterli ve ilgili olur ve aşırı olmaz;
 - d. Doğruyu yansıtır ve gerektiğinde güncellenir;
 - e. İşleme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde işlenir.

Madde 6 – Özel Veri Kategorileri

1. Aşağıdakilerin işlenmesine ancak kanunla işbu Konvansiyon'un öngördüğü tedbirleri tamamlayan nitelikteki uygun güvencelerin düzenlendiği hallerde izin verilir;
 - Genetik veriler;
 - Suçlara, cezai kovuşturmaya, ceza mahkumiyetine ve ilgili güvenlik tedbirlerine ilişkin kişisel veriler;
 - Kişiyi ayırt edilebilir şekilde belirli kılan biyometrik veriler;

- Irk, etnik köken, siyasi düşünce, sendika üyeliği, dini ve diğer inançlar, sağlık veya cinsel hayata ilişkin bilgi sağlayan kişisel veriler.
- 2. Bu güvenceler, başta ayrımcılık riski olmak üzere, ilgili kişinin menfaatleri, hakları ve temel özgürlüklerine ilişkin hassas verinin işlenmesinden doğabilecek risklere karşı koruma sağlar.

Madde 7 – Veri Güvenliği

1. Her bir Taraf, veri sorumlusunun ve uygun olduğu ölçüde veri işleyenlerin, kişisel verilere yönelik kaza sonucu veya yetkisiz erişim, imha, kayıp, kullanım, değiştirme veya ifşa gibi risklere karşı uygun güvenlik tedbirlerini almalarını sağlar.
2. Her bir Taraf, veri sorumlularının, ilgili kişilerin hak ve temel özgürlüklerine ciddi şekilde müdahale edebilecek veri ihlallerini en azından Madde 15 anlamında yetkili gözetim otoritesine gecikmeksizin bildirmesini sağlar.

Madde 8 – İşlemenin Şeffaflığı

1. Her bir Taraf, veri sorumlusunun, kişisel verilerin adil ve şeffaf işlenmesinin sağlanması için gerekli her türlü ek bilgiler dahil olmak üzere ilgili kişileri aşağıdaki hususlarda bilgilendirmesini sağlar:
 - (a) Kimliği ve mutlak meskeni veya kuruluşu;
 - (b) Hedeflenen işlemenin hukuki dayanağı ve amaçları;
 - (c) İşlenen kişisel verilerin kategorileri,
 - (d) Varsa, kişisel verilerin alıcıları veya alıcı kategorileri; ve
 - (e) Madde 9’da belirtilen hakların kullanılma yolları.
2. İlgili kişinin ilgili bilgilere sahip olduğu hallerde birinci paragraf uygulanmaz.
3. Kişisel verilerin ilgili kişiden toplanmadığı hallerde veri sorumlusu, veri işlemenin açıkça kanun ile öngörüldüğü veya bilgilendirmenin mümkün olmadığı veya orantısız çaba gerektirdiği hallerde bu bilgileri sunmakla yükümlü değildir.

Madde 9 – İlgili Kişinin Hakları

1. Her birey aşağıdaki haklara sahip olacaktır:
 - a. İlgili kişinin görüşleri dikkate alınmadan tamamen otomatik yollarla veri işlenmesi sonucunda ilgili kişiyi esaslı bir şekilde etkileyen bir karara maruz kalmamak;
 - b. Makul aralıklarla ve aşırı gecikmeye veya masrafa maruz kalmadan kendisi ile ilgili kişisel veri işlemenin, istek üzerine, teyidini almak; işlenen verilere ilişkin anlaşılabilir bildirim elde etmek; işlenen kişisel verilerin kaynağına, saklama sürelerine ve veri sorumlusunun işlemenin şeffaflığını temin etmek üzere Madde 8 Paragraf 1 uyarınca sunması gereken diğer her türlü bilgiye ilişkin uygun tüm bilgileri elde etmek;
 - c. Veri işleme sonucu elde edilen sonuçların ilgili kişiye uygulandığı hallerde veri işleme faaliyetinin altında yatan mantığa ilişkin istek üzerine bilgi almak;
 - d. Veri sorumlusu tarafından işleme için ilgili kişinin menfaatlerine veya hak ve temel özgürlüklerine üstün gelen meşru temeller gösterilmedikçe, ilgili kişinin durumuna dayanarak kendisini ilgilendiren veri işlemeye herhangi bir zamanda itiraz etmek;
 - e. İşbu Konvansiyon’un hükümlerine aykırı bir şekilde işlenmekte olan veya işlenmiş verileri, istek üzerine, ücretsiz ve aşırı gecikme olmaksızın gerekli olan durumlarda düzeltmek veya sildirmek;
 - f. İşbu Konvansiyon nezdinde ilgili kişinin haklarının ihlal edilmesi halinde Madde 12 kapsamında başvuru yolundan yararlanmak;

- g. İşbu Konvansiyon nezdinde hakların kullanılmasında, uyuşuğu veya ikamet yeri ne olursa olsun Madde 15 anlamında gözetim otoritesinin desteğinden faydalanmak.
2. Karara, veri sorumlusunun tabi olduđu ve ayrıca ilgili kişinin haklarını, özgürlüklerini ve meşru menfaatlerini korumaya yönelik uygun tedbirler ortaya koyan bir kanun tarafından izin verilmişse paragraf 1.a uygulanmaz.

Madde 10 – Ek Yükümlülükler

1. Her bir Taraf, veri sorumlularının ve uygun olduđu ölçüde veri işleyenlerin işbu Konvansiyon'un getirdiğı yükümlülüklerle uymaları için uygun tedbirleri almalarını sağlar ve Madde 11 Paragraf 3 uyarınca getirilen iç hukuk düzenlemelerine tabi olarak kontrollerindeki veri işlemenin işbu Konvansiyon'un hükümlerine uygun olduğunu, özellikle Madde 15'te düzenlenen yetkili gözetim otoritesine karşı ortaya koyabilir.
2. Her bir Taraf, veri sorumlularının ve uygun olduđu ölçüde veri işleyenlerin, veri işlemeye başlamadan önce hedeflenen veri işlemenin ilgili kişilerin hak ve temel özgürlükleri üzerindeki olası etkilerini değerlendirmesini ve veri işlemeyi bu hak ve temel özgürlüklere müdahale riskinin önlenmesine veya minimize edilmesine yönelik tasarlamasını sağlar.
3. Her bir Taraf, veri sorumlularının ve uygun olduđu ölçüde veri işleyenlerin, kişisel verilerin korunması hakkının etkilerini dikkate alan teknik ve idari tedbirleri veri işlemenin tüm aşamalarında belirlemesini sağlar.
4. Her bir Taraf, ilgili kişinin menfaatleri, hakları ve temel özgürlüklerinden doğan riskleri göz önünde bulundurarak, işbu Konvansiyon'un hükümlerinin uygulanması anlamında paragraf 1, 2 ve 3 düzenlemelerinin uygulanmasını; verinin türü ve hacmi, işlemenin türü, kapsamı ve amacı ve uygun olduđu hallerde, veri sorumlusu ile veri işleyenin boyutuna göre iç hukukunda kabul edebilir.

Madde 11 – İstisnalar ve Kısıtlamalar

1. Kanun tarafından öngörülen, temel hak ve özgürlüklerin özüne saygılı ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli ve orantılı bir önlem oluşturması şartıyla Madde 5 Paragraf 4, Madde 7 Paragraf 2, Madde 8 Paragraf 1 ve Madde 9'a getirilebilecek istisnalar dışında işbu Bölümde düzenlenen hükümlere istisna getirilemez:
 - a. Ulusal güvenliğin, savunmanın, kamu güvenliğinin, devletin önemli ekonomik ve finansal çıkarlarının, yargının tarafsızlığı ve bağımsızlığın korunması, cezai suçların önlenmesi, soruşturulması ve kovuşturulması ve cezai yaptırımların infazı ve genel kamu menfaatinin diğere esaslı amaçlar,
 - b. İlgili kişinin veya diğere kişilerin, başta ifade özgürlüğü olmak üzere, hak ve temel özgürlüklerinin korunması.
2. İlgili kişilerin hak ve temel özgürlüklerinin ihlaline ilişkin tespit edilebilir bir riskin bulunmadığı hallerde kamu menfaati kapsamında arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla veya istatistikî amaçlarla veri işleme nezdinde Madde 8 ve 9'da düzenlenen hükümlerin uygulanmasına dair istisnalar kanunla düzenlenebilir.
3. İşbu maddenin paragraf 1'inde izin verilen istisnalara ek olarak, ulusal güvenlik ve savunma amaçları için gerçekleştirilecek işleme faaliyetleri özelinde her bir Taraf, kanunla ve demokratik bir toplumda gerekli ve orantılı bir tedbir olması şartıyla Madde 4 paragraf 3, Madde 14 paragraf 5 ve 6 ile Madde 15 paragraf 2 bent (a), (b), (c) ve (d) hükümlerine istisna getirebilir.

Bu husus, ulusal güvenlik ve savunma amaçlarıyla gerçekleştirilen işleme faaliyetlerinin ilgili Tarafın yerel hukuku uyarınca bağımsız ve etkin bir inceleme ve gözetime tabi olma gerekliliğine halel getirmez.

Madde 12 – Yaptırımlar ve Başvuru Yolları

Her bir Taraf, işbu Konvansiyon'un hükümlerinin ihlali için uygun adli ve adli olmayan yaptırımlar ve başvuru yolları belirlemeyi taahhüt eder.

Madde 13 – Genişletilmiş Koruma

İşbu bölümde yer alan hükümlerden hiçbiri, Tarafların, ilgili kişilere işbu Konvansiyon'da öngörülen daha fazla koruyucu önlem sağlaması imkanını sınırlayacak veya buna halel getirecek şekilde yorumlanamaz.

Bölüm 3 – Kişisel Verilerin Sınır Ötesi Akışı

Madde 14 – Kişisel Verilerin Sınır Ötesi Akışı

1. Taraflar, sadece kişisel verilerin korunması amacıyla, Konvansiyon'un diğer bir Tarafının yetkisine tabi bir alıcıya bu verilerin aktarımını yasaklayamaz veya özel bir izne tabi tutamaz. Ancak diğer bir Tarafa yapılacak veya diğer bir Taraftan Taraf olmayan bir kişiye aktarımın yapılması halinde Konvansiyon'un hükümlerinin uygulanmaması sonucunu doğuracak ciddi ve gerçek bir riskin söz konusu olması halinde veya bölgesel uluslararası bir organizasyona ait ülkelerce korumaya ilişkin kabul edilen uyumlulaştırılmış kurullarla tabi olması halinde bu Taraf, aktarımı yasaklayabilir veya özel bir izne tabi tutabilir.
2. Alıcının işbu Konvansiyon'a Taraf olmayan bir uluslararası organizasyon veya ülkenin yetkisine tabi olduğu hallerde, kişisel verilerin aktarımı ancak işbu Konvansiyon'un hükümleri temelinde uygun seviye korumanın temin edildiği hallerde mümkün olabilir.
3. Uygun seviye bir koruma aşağıdaki şekillerde temin edilebilir:
 - a. Uygulanacak uluslararası anlaşmalar ve sözleşmeler dahil olmak üzere ülkenin veya uluslararası organizasyonların kanunları; veya
 - b. Hukuken bağlayıcı ve yaptırım gücüne haiz metinler ile kabul edilen ve aktarıma ve ikincil işlemeye dahil olan kişilerce uygulanan geçişi veya onaylanmış standartlaştırılmış güvenceler.
4. Önceki paragraflardaki düzenlemelere halel gelmeksizin, her bir Taraf aşağıdaki hallerde kişisel verilerin aktarımına izin verebilir:
 - a. Uygun güvencelerin yokluğundan doğacak risklere ilişkin bilgilendirildikten sonra ilgili kişinin açık, belirli ve özgür rızasını vermesi; veya
 - b. Durum özelinde ilgili kişinin belirli menfaatlerinin gerektirmesi; veya
 - c. Başta önemli kamu menfaatleri olmak üzere üstün gelen meşru menfaatlerin kanunda öngörülmesi ve aktarımın demokratik bir toplumda gerekli ve orantılı bir tedbir niteliğinde olması; veya
 - d. İfade özgürlüğü için demokratik bir toplumda aktarımın gerekli ve orantılı olması.
5. Her bir Taraf, Madde 15 anlamında yetkili gözetim otoritesinin paragraf 3.b'de ve talep halinde, paragraf 4.b ve 4.c'de ifade edilen veri aktarımlarına ilişkin tüm ilgili bilgilere haiz olmasını sağlar.
6. Her bir Taraf ayrıca gözetim otoritesinin, veri aktaran kişinin güvencelerinin etkinliğini veya üstün gelen meşru menfaatlerin varlığını ortaya koymasını talep etmeye yetkili olmasını ve ilgili kişilerin hak ve temel özgürlüklerinin korunması amacıyla bu aktarımları yasaklayabilmesini, askıya alabilmesini veya şarta bağlayabilmesini sağlar.

Bölüm 4 – Gözetim Otoriteleri

Madde 15 – Gözetim Otoriteleri

1. Her bir Taraf, işbu Konvansiyon'un hükümleri ile uyumluluğu temin etmekle görevli bir veya birden çok otorite belirler.
2. Bu amaç çerçevesinde bu otoriteler:
 - a. Soruşturma ve müdahale yetkilerine haiz olacaktır;
 - b. Standartlaştırılmış güvencelerin onaylanması başta olmak üzere Madde 14'te düzenlenen veri aktarımlarına ilişkin fonksiyonları yerine getirecektir;
 - c. İdari yaptırım uygulamak başta olmak üzere işbu Konvansiyon'un hükümlerinin ihlaline ilişkin olarak karar verme yetkisine haiz olacaktır;
 - d. Yasal süreçlere dahil olma veya işbu Konvansiyon'un hükümlerinin ihlalini yetkili adli otoritelerin dikkatine sunma yetkisine haiz olacaktır;
 - e. Aşağıdaki hususlarda farkındalık yaratacaktır:
 - i. fonksiyonları, yetkileri ve faaliyetleri hakkında kamu farkındalığı;
 - ii. ilgili kişilerin haklarına ve bu hakların kullanılmasına ilişkin kamu farkındalığı;
 - iii. İşbu Konvansiyon altında sorumluluklarına ilişkin veri sorumluları ve veri işleyenler nezdinde farkındalık; çocukların ve diğer zarar görmesi muhtemel bireylerin veri koruma haklarına özel olarak dikkat edilecektir.
3. Yetkili gözetim otoriteleri, kişisel verilerin işlenmesini düzenleyen yasal veya idari metinlerin tekliflerine ilişkin olarak danışılır.
4. Her bir yetkili gözetim otoritesi, veri koruma haklarına ilişkin olarak ilgili kişilerce yapılan talepler ve şikayetlerle ilgilenir ve süreç hakkında ilgili kişileri bilgilendirir.
5. Gözetim otoriteleri, görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsız ve tarafsız bir şekilde hareket eder ve bu şekilde talimat beklemez veya kabul etmez.
6. Her bir Taraf, gözetim otoritelerinin etkin bir şekilde fonksiyonlarını yerine getirmeleri ve yetkilerini kullanmaları için gerekli kaynaklara sahip olmalarını sağlar.
7. Her gözetim otoritesi, faaliyetlerini gösteren periyodik raporlar hazırlar ve yayınlar.
8. Gözetim otoritelerinin üyeleri ve çalışanları, görevlerinin ifasında ve yetkilerinin kullanımında erişim sağladıkları veya sağlamış oldukları gizli bilgilere ilişkin olarak gizlilik yükümlülüğü ile bağlıdır.
9. Gözetim otoritelerinin kararları mahkemelerde temyiz edilebilir.
10. Gözetim otoriteleri, organların adli görevlerini yerine getirirken gerçekleştirdikleri işleme faaliyetleri nezdinde yetkili değildir.

Bölüm 5 – İş Birliği ve Karşılıklı Yardımlaşma

Madde 16 – Gözetim Otoritelerinin Belirlenmesi

1. Taraflar, işbu Konvansiyon'u uygulamak üzere iş birliği içerisinde bulunmayı ve birbirlerine karşılıklı yardımda bulunmayı kabul ederler.
2. Bu amaçla:
 - a. Taraflardan her biri, Madde 15 anlamında bir veya birden fazla gözetim otoritesi tayine ederek, bunların isim ve adreslerini Avrupa Konseyi Genel Sekreterine bildirir;
 - b. Birden fazla gözetim otoritesi tayin eden her bir Taraf, yukarıdaki bentte atıfta bulunulan bildirimde, bu mercilerin her birinin yetkisini belirtir.

Madde 17 – İş Birliği Biçimleri

1. Gözetim otoriteleri, aşağıdakiler başta olmak üzere görevlerinin yerine getirilmesi ve yetkilerinin kullanılmasının gerektirdiği ölçüde birbirleri ile iş birliğinde bulunur:
 - a. İlgili ve faydalı bilgilerin karşılıklı verilmesi ile karşılıklı yardımlaşmanın sağlanması ve kişisel verilerin korunması nezdinde işbu Konvansiyon'un kuralları ve güvencelere uygunluğun sağlanması şartıyla birbirleri ile iş birliğinin gerçekleştirilmesi;

- b. Soruşturmanın ve müdahalelerin koordine edilmesi veya ortak faaliyetlerde bulunulması;
 - c. Veri korumaya ilişkin mevzuat ve idari uygulama üzerine bilgi ve belge sağlanması.
2. Birinci paragrafta belirtilen bilgiler, işlenmekte olan kişisel verilerin iş birliği için esaslı nitelikte olduğu veya ilgili kişinin kişisel verilerinin sağlanmasına açık, belirli, özgür ve bilgiye dayanan rızasını verdiği haller dışında bu tür kişisel verileri içermez.

Madde 18 – İlgili Kişilere Yardım

1. Taraflardan her biri, uyuğu veya ikamet yeri ne olursa olsun tüm ilgili kişilere Madde 9'daki haklarını kullanmasında yardımcı olur.
2. İlgili kişinin diğer bir Tarafın ülkesinde ikamet ettiği hallerde bu kişiye, talebini bu Tarafça belirlenen gözetim otoritesi aracılığı ile yapma imkanı tanınmalıdır.
3. Yardım talebi, gerekli tüm bilgileri ve bunların yanı sıra özellikle aşağıdakilerle ilgili bilgileri içerir:
 - a. Talepte bulunan ilgili kişinin isim ve adresi ile bu kişiyi belirlemeye yarayan diğer tüm hususlar,
 - b. Talebin konusu işleme veya bu işlemenin veri sorumlusu,
 - c. Talebin amacı.

Madde 19 – Güvenceler

1. Bir başka gözetim otoritesinde bilgi alan bir gözetim otoritesi bu bilgiyi, ne bir talebi desteklemek suretiyle ne de kendi talebine cevap olarak, talepte belirtilen amaçlar dışında kullanabilir.
2. Bir gözetim otoritesi hiçbir durumda kendi inisiyatifiyle ve ilgili kişinin açık onayı olmaksızın ilgili kişi adına bir talepte bulunmaya yetkili kılınmayacaktır.

Madde 20 – Taleplerin Reddi

1. Madde 17 uyarınca kendisine talep yöneltilen bir gözetim otoritesi, aşağıdaki haller dışında talebe uymayı reddedemez:
 - a. Talep, yetkilerine uygun değilse;
 - b. Talep, işbu Konvansiyon hükümlerine uygun değilse;
 - c. Talebin yerine getirilmesi, bunu yerine getirecek otoriteyi belirleyen devletin egemenliğine, ulusal güvenliğine veya kamu düzenine veya bu devletin yetkisi altındaki bireylerin haklarına ve temel özgürlüklerine aykırı ise.

Madde 21 – Giderler ve Prosedürler

1. Tarafların Madde 17 uyarınca birbirlerine karşı gerçekleştirdikleri iş birliği ve karşılıklı yardım ile Madde 9 ve 18 uyarınca ilgili kişilere yaptıkları yardım, uzman ve tercüman ücretleri dışında, hiçbir masraf veya harcı gerektirmeyecektir. Bu masraf ve harçlar, talepte bulunan Tarafça karşılanacaktır.
2. İlgili kişi, bir başka Tarafın ülkesinde kendi hesabına yapılan işlemlerle ilgili olarak, bu Tarafın ülkesinde ikamet eden kişilerce yasal olarak ödenmesi gereken harç ve masraf dışında, hiçbir harç ve masraf ödemek zorunda olmayacaktır.
3. İş birliği ve yardımla ilgili diğer hususlar ve özellikle yardımın şekli ve usulü ile kullanılacak dile ilişkin konular, ilgili Taraflar arasında doğrudan karşılaştırılacaktır.

Bölüm 6 – Konvansiyon Komitesi

Madde 22 – Komitenin Oluşumu

1. İşbu Konvansiyon'un yürürlüğe girmesinden sonra bir Konvansiyon Komitesi kurulur.
2. Taraflardan her biri, komiteye bir asıl temsilci ve bir temsilci vekili tayin eder. Konvansiyon'a taraf olmayan herhangi bir Avrupa Konseyi üye devleti komitede bir gözlemci tarafından temsil edilme hakkına sahiptir.
3. Konvansiyon Komitesi, Tarafların temsilcilerinin üçte ikisi çoğunluğu ile alacağı bir karar ile toplantılarda temsil edilmek üzere bir gözlemci çağırabilir.
4. Avrupa Konseyi üyesi olmayan herhangi bir Taraf, Bakanlar Komitesi'nin işbu Taraf ile akdettiği sözleşmede belirlenen usuller uyarınca Konvansiyon Komitesi'nin faaliyetlerinin fonlanmasına katkıda bulunur.

Madde 23 – Komitenin İşlevleri

1. Konvansiyon Komitesi:
 - a. Konvansiyon'un uygulanmasını kolaylaştırmak veya iyileştirmek amacıyla tavsiyelerde bulunabilir;
 - b. Madde 25 uyarınca işbu Konvansiyon'da değişiklik yapılması için önerilerde bulunabilir;
 - c. Madde 25 paragraf 3 uyarınca kendisine iletilen Konvansiyon değişikliği önerileri üzerinde görüş bildirir;
 - d. İşbu Konvansiyon'un yorumlanması veya uygulanmasına ilişkin her türlü soruya yönelik görüş belirtebilir;
 - e. Konvansiyon'a herhangi bir yeni katılımdan önce, adayın kişisel veri koruma seviyesine ilişkin Bakanlar Komitesi için bir görüş hazırlar ve gerekmesi halinde işbu Konvansiyon'un hükümlerine uygunluk için alınması gereken güvenceleri tavsiye eder;
 - f. Bir devletin veya uluslararası organizasyonun talebi üzerine bu devletin veya uluslararası organizasyonun sunduğu kişisel veri koruma seviyesinin işbu Konvansiyon'un hükümleri ile uyumlu olmadığını değerlendirebilir ve gerekli olması halinde bu uyumluluğun sağlanması için alınabilecek güvenceleri tavsiye edebilir;
 - g. Madde 14'te belirtilen standartlaştırılmış güvence modelleri oluşturabilir veya onaylayabilir;
 - h. İşbu Konvansiyon'un Taraflarca uygulanmasını inceler ve bir Tarafın işbu Konvansiyon ile uyumlu olmaması halinde alınabilecek güvenceleri tavsiye eder;
 - i. Gerekli olması halinde işbu Konvansiyon'un uygulanmasına ilişkin tüm zorlukların dostane çözümlerini kolaylaştırır.

Madde 24 – Usul

1. Konvansiyon Komitesi, Avrupa Konseyi Genel Sekreteri tarafından toplantıya çağırılır. Komite ilk toplantısını, işbu Konvansiyon'un yürürlüğe girmesini izleyen on iki ay içerisinde yapar. Komite, müteakip toplantılarını yılda en az bir defa yapar ve Tarafların temsilcilerinin üçte birinin talebi üzerinde herhangi bir zamanda toplanır.
2. Konvansiyon Komitesi, her toplantı sonunda, yaptığı çalışmalar ve Konvansiyon'un işleyişi hakkında Avrupa Konseyi Bakanlar Komitesi'ne bir rapor sunar.
3. Konvansiyon Komitesi'ndeki oylama düzenlemeleri, Protokol CETS (*Avrupa Konseyi Sözleşme Serileri*) No.[223]'e eklenen Usul Kuralları için belirlenen unsurlardır.
4. Konvansiyon Komitesi kendisinin Usul Kuralları'nın diğer unsurlarının ve özellikle objektif kriterler temelinde Madde 4 paragraf 3 ve Madde 23 bent (e), (f) ve (h)'de belirtilen değerlendirme ve inceleme için usul belirler.

Bölüm 7 – Değişiklikler

Madde 25 – Değişiklikler

1. Taraflardan biri, Avrupa Konseyi Bakanlar Komitesi veya Konvansiyon Komitesi, işbu Konvansiyon'da değişiklik yapılmasını önerebilir.
2. Her değişiklik önerisi, Avrupa Konseyi Genel Sekreteri tarafından işbu Konvansiyon'un Taraflarına, Avrupa Konseyi'nin diğer üye devletlerine, Avrupa Birliği'ne ve Madde 28 uyarınca işbu Konvansiyon'a katılım için çağırılan tüm üye olmayan devletlere ve uluslararası organizasyonlara bildirilir.
3. Taraflardan biri veya Bakanlar Komitesi tarafından yapılan her değişiklik önerisi, Bakanlar Komitesi'ne değişiklik hakkında görüş sunacak olan Konvansiyon Komitesi'ne bildirilir.
4. Bakanlar Komitesi, teklif edilen değişikliği ve Konvansiyon Komitesi tarafından sunulabilecek her türlü görüşü dikkate alarak söz konusu değişikliği kabul edebilir.
5. Bakanlar Komitesi tarafından bu maddenin dördüncü fıkrasına göre kabul edilen her türlü değişiklik metni, kabul için Taraflara iletilir.
6. İşbu maddenin dördüncü fıkrası uyarınca kabul edilen herhangi bir değişiklik, tüm Tarafların ilgili değişikliği kabul ettiklerini Genel Sekreter'e bildirimlerini izleyen otuzuncu günde yürürlüğe girer.
7. Ayrıca Bakanlar Komitesi, Konvansiyon Komitesi'ne danıştıktan sonra, belirli bir değişikliğin, kabule açıldığı tarihten itibaren üç yıllık bir sürenin sona ermesi ile yürürlüğe gireceğine, bir Tarafın Avrupa Konseyi Genel Sekreteri'ne ilgili yürürlüğe giriş hakkında itiraz bildirmediği hallerde oy birliği ile karar verebilir.

Bölüm 8 – Son Hükümler

Madde 26 – Yürürlüğe Giriş

1. İşbu Konvansiyon, Avrupa Konseyi üye devletlerinin ve Avrupa Birliği'nin imzasına açıktır. Onay, kabul ya da uygun bulmaya tabidir. Onay, kabul ya da uygun bulma belgeleri, Avrupa Konseyi Genel Sekreteri'ne teslim edilir.
2. İşbu Konvansiyon, en az beş Avrupa Konseyi üye devletinin, yukarıdaki fıkra hükümleri uyarınca Konvansiyon ile bağlı olma yönündeki rızalarını ifade ettikleri tarihten itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.
3. Sonradan Konvansiyon ile bağlı olmak istediğini beyan eden herhangi bir Taraf; onay, kabul ya da uygun bulma belgesini teslim etme tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

Madde 27 – Üye Olmayan Devletlerin veya Uluslararası Organizasyonların Katılımı

1. İşbu Konvansiyon'un yürürlüğe girmesinden sonra, Avrupa Konseyi Bakanlar Komitesi, işbu Konvansiyon'un Taraflarına danıştıktan ve oybirliği ile onaylarını aldıktan sonra ve Madde 23 bent (e) uyarınca Konvansiyon Komitesi tarafından hazırlanan görüş doğrultusunda, Avrupa Konseyi'ne üye olmayan herhangi bir devleti veya uluslararası organizasyonu, Avrupa Konseyi Statüsü'nün 20inci maddesinin (d) fıkrasında öngörülen çoğunlukla ve Bakanlar Komitesi'ne katılma hakkına sahip Taraf devlet temsilcilerinin oybirliği ile işbu Konvansiyon'a katılmaya davet edebilir.

2. Yukarıdaki birinci paragraf uyarınca işbu Konvansiyon'a katılan herhangi bir devlet veya uluslararası organizasyon için işbu Konvansiyon, katılma belgesinin Avrupa Konseyi Genel Sekreteri'ne tevdi edildiği tarihten sonraki üç aylık dönemin bitimini izleyen ayın ilk günü yürürlüğe girer.

Madde 28 – Ülkesel Hükümler

1. Herhangi bir devlet, Avrupa Birliği veya diğer uluslararası organizasyon, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerini tevdi ederken, Konvansiyon'un uygulanacağı ülkeyi veya ülkeleri belirtebilir.
2. Herhangi bir devlet, Avrupa Birliği veya diğer uluslararası organizasyon, daha sonraki bir tarihte Avrupa Konseyi Genel Sekreteri'ne iletilen bir bildirimle, işbu Konvansiyon'un uygulama alanını, bildirimde belirtilen başka herhangi bir ülkeye teşmil edebilir. Konvansiyon, söz konusu ülke bakımından, söz konusu beyanın Genel Sekreter tarafından alınma tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.
3. Yukarıdaki iki fıkra uyarınca yapılan herhangi bir bildirim, söz konusu bildirimde belirtilen herhangi bir ülke bakımından Avrupa Konseyi Genel Sekreteri'ne iletilen bir bildirim ile geri çekilebilir. Söz konusu geri çekme, söz konusu bildirim Genel Sekreter tarafından alınma tarihinden itibaren altı aylık sürenin sona ermesini takip eden ayın ilk günü geçerlilik kazanır.

Madde 29 – Çekinceler

1. İşbu Konvansiyon hükümlerine hiçbir çekince konulamaz.

Madde 30 – Fesih

1. Taraflardan herhangi biri, herhangi bir zamanda Avrupa Konseyi Genel Sekreteri'ne iletilecek bir bildirim yoluyla işbu Konvansiyon'u feshedebilir.
2. Söz konusu fesih, söz konusu bildirim Genel Sekreter tarafından alınma tarihinden itibaren altı aylık sürenin sona ermesini takip eden ayın ilk günü geçerlilik kazanır.

Madde 31 – Bildirimler

1. Avrupa Konseyi Genel Sekreteri, Konsey üyesi devletlere ve işbu Konvansiyon'un her Tarafına aşağıdaki hususları bildirecektir:
 - a. Her imzayı,
 - b. Tevdi edilen her onay, kabul, uygun bulma veya taraf olma belgesini;
 - c. Madde 26, 27 ve 28 uyarınca işbu Konvansiyon'un her yürürlüğe giriş tarihini;
 - d. İşbu Konvansiyon ile ilgili diğer her tür belge, bildirim ya da muhaberatı.

Protokol'e Ek: Konvansiyon Komitesi'nin Usul Kuralları'nın Unsurları

1. Her bir Tarafın oy kullanma hakkı ve bir oyu vardır.
2. Tarafların temsilcilerinin üçte ikisinin çoğunluğu, Konvansiyon Komitesi'nin toplantıları için yeterli çoğunluğu sağlar. Protokol'ün, Konvansiyon'a taraf tüm devletler nezdinde yürürlüğe girmesinden önce Madde 37 paragraf 2 uyarınca yürürlüğe girmesi halinde Konvansiyon Komitesi'nin toplantıları için yeterli çoğunluk, Protokol'ün 34 Tarafından daha az olmayacaktır.

3. Madde 23 kapsamındaki kararlar beşte dört çoğunluk ile alınır. Madde 23 bent (h) uyarınca alınan kararlar, Konvansiyon'a Taraf olan bölgesel bir entegrasyon organizasyonuna üye olmayan Taraf devletlerin oylarının çoğunluğu dahil olmak üzere beşte dört çoğunlukla alınır.
4. Konvansiyon Komitesi'nin Madde 23 bent (h) uyarınca aldıkları kararlarda incelemeye ilişkin Taraf oy kullanmaz. Bu tür bir kararın bölgesel entegrasyon organizasyonunun yetkisi kapsamındaki bir hususa ilişkin olması halinde ne organizasyon ne de üye devletleri oy kullanır.
5. Usule ilişkin konulardaki kararlar basit çoğunluk ile alınır.
6. Bölgesel entegrasyon organizasyonları, yetkileri kapsamındaki hususlarda Konvansiyon Komitesi'ndeki oy haklarını, Konvansiyon'a Taraf üye devletlerin sayısına eşit sayıda oy ile kullanabilir.
7. Oylama durumunda tüm Taraflar, oylamanın konusu ve zamanı konusunda ve oylamanın Taraflarca bireysel olarak veya üye devletler adına bölgesel entegrasyon organizasyonu tarafından gerçekleştirileceği hakkında bilgilendirilmiş olmalıdır.
8. Konvansiyon Komitesi, ancak oybirliği ile değiştirilebilen oylama düzenlemeleri ve Konvansiyon Madde 25'in uygulandığı düzenlemeler dışında Usul Kuralları'nı üçte ikilik çoğunluk ile değiştirebilir.

Açıklayıcı Rapor

I. Giriş

1. Kovansiyon 108 (bundan sonra "Konvansiyon" olarak anılacaktır) olarak da bilinen Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, imzaya açılmasından bu yana geçen 35 yılda 40'tan fazla Avrupa ülkesinde uluslararası veri koruma hukukuna temel teşkil etti. Bunun yanında Avrupa kıyılarının çok ötesindeki politika ve mevzuatı da etkiledi. Yeni bilgi ve iletişim teknolojilerinin (IT) artan kullanımı, işleme faaliyetlerinin küreselleşmesi ve kişisel verilerin her zamankinden daha yoğun akışından kaynaklanan gizlilik problemlerinin daha iyi ele alınması için Konvansiyon'un yenilenmesi, aynı zamanda değerlendirme ve takip mekanizmasının güçlendirilmesi gerektiği, insan hakları ve temel özgürlüklere, özellikle de özel hayatın gizliliği hakkına yönelik her geçen gün yeni zorlukların doğmasıyla açıkça ortaya çıktı.
2. Yenileme sürecinin aşağıdaki yönleri bakımından geniş bir fikir birliğine varılmıştır: Konvansiyon'un hükümlerinin genel ve teknolojik açıdan tarafsız niteliği korunmalıdır; Konvansiyon'un diğer yasal çerçevelerle tutarlılığı ve uyumluluğu korunmalıdır; Konvansiyon'a evrensel bir standart olma potansiyeli kazandıran açık karakterinin yeniden tasdik edilmesi gerekmektedir. Konvansiyon'un metni genel niteliktedir ve Bakanlar Komitesi'nin ilgili paydaşların katılımıyla hazırladığı önerileri gibi bağlayıcı olmayan, daha ayrıntılı sektörel hukuk metinleriyle desteklenebilir.
3. Yenileme çalışması, uluslararası veri koruma belgelerinin aynı doğrultudaki çeşitli reformları kapsamında ve 1980 (2013'te gözden geçirilmiş) Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri, 1990 Birleşmiş Milletler Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin

Rehber İlkeleri, 1995'ten bu yana Avrupa Birliği (AB) düzenlemeleri³, Asya-Pasifik Ekonomik İşbirliği Gizlilik Çerçevesi (2004) ve 2009 tarihli Kişisel Verilerin İşlenmesi bakımından Gizliliğin Korunmasına İlişkin Uluslararası Standartlar⁴ dikkate alınarak gerçekleştirilmiştir. Çalışmalar özellikle AB veri koruma reform paketi gözetilerek aynı doğrultuda yürütülmüştür ve her iki yasal çerçeve arasında tutarlılığın sağlanması için büyük özen gösterilmiştir. AB veri koruma düzenlemeleri esası belirler ve özellikle uluslararası aktarımla ilgili olarak Konvansiyon 108'e katılımı dikkate alarak Konvansiyon'un ilkelerini derinleştirir⁵.

4. Konvansiyon'un 18inci maddesi gereği oluşturulan Danışma Komitesi, 29uncu Genel Kurul toplantısında (27-30 Kasım 2012) kabul edilen ve Bakanlar Komitesi'ne sunulan taslak yenileştirme önerileri hazırlamıştır. Bakanlar Komitesi daha sonra, yenileştirme önerilerini tamamlama görevi ile geçici veri koruma Komitesini (CAHDATA) görevlendirmiştir. Bu, CAHDATA'nın üçüncü toplantısı (1-3 Aralık 2014) vesilesiyle tamamlanmıştır. AB veri koruma çerçevesinin tamamlanmasının ötesinde, olağanüstü sorunları incelemek amacıyla başka bir CAHDATA kurulmuştur. Son CAHDATA toplantısında (15-16 Haziran 2016) Komite, tekliflerini tamamlamış, değerlendirilmesi ve kabulü için Bakanlar Komitesine iletmiştir.

5. Bu açıklayıcı raporun metni, Konvansiyon hükümlerinin uygulanmasına rehberlik etmek ve yardım etmek amacıyla hazırlanmıştır ve hazırlayanların Konvansiyon'un işleyişini nasıl öngördüğüne işaret etmektedir.

6. Bakanlar Komitesi açıklayıcı raporu onaylamıştır. Bu bakımdan, açıklayıcı rapor, Konvansiyon'da kullanılan belirli terimlerin anlamlarını tayin eden kaynaklardan birini oluşturur (not: ref. Madde 31, Birleşmiş Milletler Viyana Antlaşmaları Hukuku Sözleşmesi'nin 1. ve 2. fıkraları).

Protokol, 18 Mayıs 2018 tarihinde Bakanlar Komitesi tarafından kabul edilmiştir. Protokol eki, Protokol'ün ayrılmaz bir parçasını teşkil eder ve Protokol'ün diğer hükümleriyle aynı hukuki değere sahiptir.

Bu Protokol, 10 Ekim 2018 tarihinde Strazburg'da imzaya açılmıştır.

II. Yorumlar

7. Bu Protokol'ün amacı, Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (ETS No. 108) ve denetleyici makamlar ve sınır aşan veri akışına ilişkin Ek Protokolü'nü (ETS No. 181) yenilemek ve uygulamalarını güçlendirmektir. Yürürlüğe girmesinden itibaren Ek Protokol, tadil edilmiş şekliyle Konvansiyon'un ayrılmaz bir parçası olarak kabul edilecektir.

8. Konvansiyon 108'e ve ek protokolüne ilişkin açıklayıcı raporlar, tarihsel bağlamı vermeleri ve her iki belgenin gelişimini tasvir etmeleri bakımından konuyla ilgilidirler ve bu amaçlar için mevcut dokümanla birlikte okunabileceklerdir.

Önsöz

³ Genel Veri Koruma Regülasyon (AB) 2016/679 ("GDPR") ve Polis ve Yargı Makamları Veri Koruma Direktifi (AB) 2016/680 ("Polis Direktifi").

⁴ 31. Uluslararası Veri Koruma ve Gizlilik Yetkilileri Konferansı, Madrid 4-6 Kasım 2009

⁵ Bkz. GDPR Giriş Hükümü 105

9. Önsöz, imzacı devletlerin insan haklarına ve temel özgürlüklere olan bağlılığını teyit eder.

10. Konvansiyon'un temel amacı, bireyleri kişisel verilerinin başkaları tarafından işlendiğini bilecek, anlayabilecek ve kontrol edebilecek bir duruma getirmektir. Buna göre önsöz, özellikle kişisel özerklik hakkı ve bireyin mahremiyet hakkından ve ayrıca kişilerin saygınlığından kaynaklanan kişisel verilerini kontrol etme hakkını açıkça ifade eder. İnsanın saygınlığı, bireylerin yalnızca nesne olarak değerlendirilmemeleri için kişisel verileri işlerken güvencelerin kullanılmasını gerektirir.

11. Kişisel verilerin korunması hakkının toplumdaki rolünü göz önüne alarak önsöz; bireylerin çıkarlarının, haklarının ve temel özgürlüklerinin, gerektiğinde birbirleriyle uzlaştırılması gerektiği ilkesini vurgulamaktadır. Konvansiyon'un, bilgilerin işlenmesi ve kişisel verilerin korunması ile ilgili belirli şartlar ve kısıtlamalar getirdiği farklı menfaatler, haklar ve temel özgürlükler arasında dikkatli bir denge sağlamayı amaçlar. Veri koruma hakkı, örneğin görüş belirtme ve bilgi alma ve verme özgürlüğünü içeren Avrupa İnsan Hakları Sözleşmesinin 10. Maddesinde (ETS No. 5) belirtilen "ifade özgürlüğü" ile birlikte ele alınır. Ayrıca Konvansiyon, mutlak olmayan veri koruma hakkının kullanılmasının, kamunun resmi belgelere erişimini engellemek için genel bir araç olarak kullanılmaması gerektiğini vurgulamaktadır⁶.

12. Konvansiyon 108, koyduğu ilkeler ve içerdiği değerler aracılığıyla uluslararası veri akışları için bir çerçeve sağlayarak bireyi korur. Küresel bilgi akışları modern toplumda giderek daha önemli bir rol oynaması, temel hak ve özgürlüklerin kullanılmasını sağlayarak yeniliği tetiklediği, sosyal ve ekonomik ilerlemeyi geliştirdiği, aynı zamanda kamu güvenliğini sağlamada hayati bir rol oynadığı için önemlidir. Bir bilgi ve iletişim toplumunda kişisel verilerin akışı, bireylerin temel hak ve özgürlüklerine saygı duymalıdır. Ayrıca, yenilikçi teknolojilerin geliştirilmesi ve kullanılması da bu haklara saygı göstermelidir. Bu, yeniliklere ve yeni teknolojilere güven tesis etmeye yardımcı olacak ve gelişimlerini daha da kolaylaştıracaktır.

13. Gözetim otoriteleri arasındaki uluslararası işbirliği, bireylerin etkin bir şekilde korunmasında temel unsurlardan biri olduğundan Konvansiyon, soruşturma ve icra konusunda işbirliği ve bilgi alışverişi için uygun yasal temeli sağlayarak özellikle Tarafların karşılıklı yardımda bulunmalarını destekler ve bu işbirliğini güçlendirmeyi amaçlar.

Bölüm 1 – Genel Hükümler

Madde 1 – Konu ve Amaç

14. İlk madde, Konvansiyon'un konu ve amacını açıklar. Bu madde, koruma konusuna odaklanmaktadır: bireyler, kişisel verileri işlendiğinde korunmalıdır⁷. Çok yakın geçmişte veri koruma, AB'nin Temel Haklar Şartı'nın 8. Maddesinde ve aynı zamanda Konvansiyon'a Taraf devletlerin anayasalarında temel bir hak olarak yerini almıştır.

15. Konvansiyon'da belirtilen güvenceler, uyuşuğu veya ikametgahı ne olursa olsun her bireye verilmektedir. Vatandaşlarla üçüncü ülke uyrukları arasında bu teminatların

⁶ Bkz. Resmi Belgelere Erişim Konusunda Avrupa Konseyi Sözleşmesi (CETS No. 205).

⁷ "Kişisel verilerin korunması, bir kişinin 8inci maddede güvence altına alınan özel ve aile yaşamına saygı hakkından yararlanma konusunda temel öneme sahiptir."- AİHM, MS v. Sweden, (Başvuru No. 20837/92),1997, paragraf 41.

uygulanmasında ayrımcılığa izin verilmemektedir⁸. Veri korumasını bir devletin kendi vatandaşlarına veya yasal olarak ikamet eden yabancı uyruklulara sınırlayan hükümler, Konvansiyon ile uyumlu değildir.

Madde 2 – Tanımlar

16. Bu Sözleşmede kullanılan tanımlar, belirli temel kavramları ifade eden terimlerin ulusal mevzuatlarda yeknesak uygulanmasını sağlamak içindir.

(a) bendi - "kişisel veri"

17. “Kimliği belirlenebilir kişi”, doğrudan veya dolaylı olarak kimliği belirlenebilen kişi anlamına gelir. Bir kişi, kimliği makul olmayan bir zaman, çaba veya kaynak gerektiriyorsa “kimliği belirlenebilir” kabul edilmez. Örneğin, ilgili kişinin kimliğinin belirlenmesi aşırı karmaşık, uzun ve maliyetli işlemler gerektirdiğinde durum böyledir. Neyin “makul olmayan zaman, çaba veya kaynak” teşkil ettiği meselesi, duruma göre değerlendirilmelidir. Örneğin; işlemin amacı, maliyet, belirlemenin faydaları, veri sorumlusunun türü, kullanılan teknoloji vb. gibi objektif kriterler dikkate alınabilir. Ayrıca, teknolojik ve diğer gelişmelerle “mantıksız zaman, çaba veya diğer kaynaklar” algısı değişebilir.

18. “Kimliği belirlenebilir” kavramı, yalnızca bireyin kişisel veya yasal kimliğini değil aynı zamanda bir kişiyi “bireysel olarak tespit etmeye” ya da diğerlerinden ayırmaya (böylece farklı muamele görebilmesine) uygun olanları ifade eder. Bu “bireysel olarak tespit etme”, özellikle kişinin kendisine veya sayı, takma ad, biyometrik veya genetik veriler, konum verileri, bir IP adresi veya başka bir tanımlayıcıdan yola çıkarak bir cihaza veya bir cihaz kombinasyonuna (bilgisayar, cep telefonu, kamera, oyun cihazları vb.) atıfta bulunarak yapılabilir. Bir takma ad veya herhangi bir dijital tanımlayıcı/dijital kimliğin kullanılmasıyla, ilgili kişi hala belirlenebilir veya bireysel olarak tespit edilebilir olduğu için verileri anonim hale getirmez. Dolayısıyla takma adlı veriler kişisel veriler olarak kabul edilir ve Konvansiyon hükümleri kapsamındadır. Uygulanan takma ad verme tekniklerinin kalitesi, ilgili kişilere riskleri azaltmak için uygulanan önlemlerin uygunluğunu değerlendirirken gereğince dikkate alınmalıdır.

19. Veriler ancak ilgili kişinin kimliğinin yeniden belirlenmesi imkansız olduğu sürece veya bu yeniden belirleme işleme zamanındaki mevcut teknoloji ve teknolojik gelişmeler göz önünde bulundurulduğunda makul olmayan zaman, çaba veya kaynak gerektiriyorsa anonim olarak kabul edilmelidir. Anonim görünen veriler, herhangi bir belirgin tanımlayıcı unsur bulunmasa dahi, belirli durumlarda (makul olmayan zaman, çaba veya kaynaklar gerektirmeyen) bir bireyin kimliğinin belirlenmesine izin verebilir. Bu, örneğin veri sorumlusunun veya herhangi bir kimsenin, bireyi fiziksel, fizyolojik, genetik, ekonomik veya sosyal veriler gibi farklı veri türlerinin bir araya getirilmesiyle (örneğin, yaş, cinsiyet, meslek, coğrafi konum, aile durumu vb.) durumunda gerçekleşir. Bu durumda, veriler anonim olarak kabul edilemez ve Konvansiyon hükümleri kapsamına girer.

20. Veriler anonimleştirildiğinde, ilgili kişilerin yeniden belirlenmesini önlemek için uygun araçlar kullanılmalı, özellikle bireyin kimliğinin belirlenmemesini sağlamak için tüm teknik araçlar uygulanmalıdır. Teknolojik gelişimin hızlı ilerleyişi ışığında düzenli olarak yeniden değerlendirilmelidirler.

⁸ Bkz. Avrupa Konseyi İnsan Hakları Komisyonu, İnternette ve daha geniş dijital dünyada hukukun üstünlüğü, 8 Aralık 2014, s. 48, 3.3, Ayrımcılık Olmaksızın “Herkes”

(b) ve (c) bendi - "veri işleme"

21. "Veri işleme", kişisel verilerin toplanmasından başlar ve kısmen veya tamamen otomatik yollarla kişisel veriler üzerinde gerçekleştirilen tüm işlemleri kapsar. Otomatik olmayan yollarla veri işleme, veri sorumlusunun veya başka herhangi bir kişinin belirli kriterlere göre erişilebilen veya alınabilen, yapılandırılmış bir veri kümesi içinde ilgili kişi ile ilgili veri aramasına, birleştirmesine veya ilişkilendirmesine izin vererek kişisel veriler üzerinde gerçekleştirilen işlem veya işlem kümesi anlamına gelir.

(d) bendi - "veri sorumlusu"

22. "Sorumlu", işlemin amaç ve vasıtaları ile ilgili olarak karar alma yetkisine sahip kişi veya kuruluş anlamına gelir, bu yetkinin yasal bir unvan veya fiili durumdan kaynaklandığı olay bazında değerlendirilir. Bazı durumlarda, birden fazla veri sorumlusu veya ortak sorumlular olabilir (bir işlemde müştereken sorumlu ve büyük olasılıkla bu işlemin farklı yönlerinden sorumludurlar). Kişi veya kuruluşun veri sorumlusu olup olmadığını değerlendirirken, bu kişi veya kuruluşun işlemeyi haklı kılan sebepleri, diğer bir deyişle amaçlarını ve bunun için kullanılan vasıtaları belirleyip belirlemediğine özel olarak dikkat edilmelidir. Bu değerlendirme için diğer ilgili faktörler arasında kişi veya kurumun işleme yöntemleri, işlenecek verilerin seçimi üzerinde kontrolü ve bu bilgilere erişme izni olup olmadığı bulunur. Doğrudan veri sorumlusuna tabi olmayan ve veri sorumlusu adına ve yalnızca sorumlunun talimatlarına göre işlem yapanlar işleyen olarak kabul edilir. Veri sorumlusu, bir işleyenin verileri kendi adına işlemekte olduğu işlemlerden de sorumludur.

(e) bendi - "alıcı"

23. "Alıcı", kişisel verileri alan veya kişisel verilerin kullanıma sunulduğu bir birey veya kurumdur. Koşullara bağlı olarak, alıcı bir veri sorumlusu veya veri işleyen olabilir. Örneğin, bir işletme çalışanlarının belirli verilerini vergi amacıyla sorumlu olarak işleyecek bir devlet departmanına veya depolama hizmetleri sunan ve işleyen olarak görev yapan bir şirkete gönderebilir. Alıcı, bir kamu işlevini yerine getirme hakkı verilen bir kamu makamı veya tüzel kişisi olabilir, ancak makam veya tüzel kişi tarafından alınan verilerin, ilgili yasaya göre belirli bir soruşturma çerçevesinde işlendiği durumlarda o kamu makamı veya tüzel kişi alıcı olarak kabul edilmeyecektir. Kamu makamlarına yapılan açıklama talepleri her zaman yazılı, gerekçeli ve nadiren yapılmalı ve bir dosyalama sisteminin bütünüyle ilgili olmamalı veya dosyalama sistemlerinin birbirine bağlanmasına yol açmamalıdır. Kişisel verilerin bu kamu makamları tarafından işlenmesi, işlemin amaçlarına göre uygulanabilir veri koruma kurallarına uymalıdır.

(f) bendi - "veri işleyen"

24. "İşleyen", veri sorumlusu adına ve veri sorumlusunun talimatlarına göre veri işleyen (veri sorumlusunun çalışanları dışındaki) herhangi bir gerçek veya tüzel kişidir. Veri sorumlusu tarafından verilen talimatlar, veri işleyenin kişisel verilerle yapabileceklerine ilişkin verilen iznin sınırını belirler.

Madde 3 – Kapsam

25. Birinci fıkraya göre, her bir Taraf devlet kendi yargı yetkisine tabi olan hem kamu hem özel sektör dahilindeki tüm işlemlere Konvansiyon'u uygulamalıdır.

26. Korumanın kapsamının Tarafların “yargı yetkisine” bağlı tutulması, zamana yenik düşmeme ve sürekli teknolojik gelişmelere ayak uydurma amacı taşır.

27. İkinci fıkra, tamamen kişisel veya ev halkına ilişkin faaliyetler kapsamında gerçekleştirilen işlemleri Konvansiyon kapsamının dışında tutar. Bu dışlama, bireylere kendi özel alanlarında, özel yaşamlarını sürdürmeye yönelik faaliyetlere ilişkin veri işlemleri konusunda makul olmayan yükümlülükler yüklenmesini önlemeyi amaçlar. Tamamen kişisel veya ev halkına ilişkin faaliyetler, bireyin özel hayatı ile yakından ve objektif olarak bağlantılı olan ve başkalarının kişisel alanını önemli ölçüde etkilemeyen faaliyetlerdir. Bu faaliyetlerin mesleki veya ticari yönleri yoktur ve yalnızca özel resimlerin bilgisayara depolanması, arkadaşların ve aile üyelerinin iletişim bilgilerinin bir listesini oluşturmak, yazışmalar gibi kişisel veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetlerdir. Verilerin özel alan içerisinde paylaşılması, özellikle aile, dar bir arkadaş çevresi veya sınırlı büyüklükte bir çevre içinde ve kişisel bir ilişki veya belirli bir güven ilişkisine dayanan paylaşımı kapsar.

28. Faaliyetlerin “tamamen kişisel veya ev halkına ilişkin” olup olmadığı duruma göre değerlendirilir. Örneğin, kişisel verilerin çok sayıda kişiye veya internet sitesi gibi yerlerde açıkça özel alanın dışında kalan kişilere açık olması bu istisna kapsamına girmez. Benzer şekilde, insanlara ait görüntülerin, bir kişinin aile evinde ev sahiplerinin mülkünü, sağlığını ve yaşamını korumak amacıyla kurduğu, kısmen de olsa kamusal bir alanı kapsayan ve kişinin özel alanı dışına yöneltmiş, kamera sistemi vasıtasıyla sabit disk sürücüsü gibi sürekli bir kayıt cihazına kaydedilmesi tamamen “kişisel veya ev halkına ilişkin” bir faaliyet olarak kabul edilemez⁹.

29. Bununla birlikte Konvansiyon, bu tür tamamen kişisel veya ev halkına ilişkin kişisel verilerin işlenmesi için vasıta sağlayanların yürüttüğü veri işleme faaliyetlerine uygulanır.

30. Konvansiyon, gerçek kişi verilerinin işlenmesi ile ilgili olmakla birlikte, Taraflar iç hukuklarındaki korumayı, meşru çıkarlarını korumak amacıyla tüzel kişilere ilişkin verileri de kapsayacak şekilde genişletebilirler. Konvansiyon, sağ bireyler için geçerlidir: vefat eden kişilerin kişisel verilerine uygulanmaz. Ancak bu, Tarafların korumayı vefat eden kişileri de kapsayacak şekilde genişletmesini engellemez.

Bölüm 2 – Kişisel Verilerin Korunmasına İlişkin Temel İlkeler

Madde 4 – Tarafların Görevleri

31. Bu maddede belirtildiği üzere Konvansiyon, Taraflara hükümlerini iç hukuklarına aktarma ve etkin bir şekilde uygulanmalarını sağlama zorunluluğu getirmiştir; bunun nasıl yapılacağı uygulanan hukuka ve uluslararası anlaşmaların iç hukuka aktarılmasına ilişkin yaklaşıma bağlıdır.

32. “Tarafların iç hukuku” terimi, belirli bir ülkenin yasal ve anayasal sistemine göre, ister yazılı hukuk ister içtihat hukuku olsun, uygulanabilir tüm kuralları belirtir. Yasa, gerekli erişilebilirlik ve öngörülebilirlik niteliklerini karşılamalıdır. Yani bireylerin ve diğer kuruluşların beklenen hukuki sonuçlar ışığında kendi davranışlarını düzenlemelerine izin verecek kadar net olmalı ve yasadaki etkilenmesi muhtemel kişiler tarafından erişilebilmelidir. İç hukuk, kişilere borçlar yükleyen veya hak tanıyan kurallar (doğal veya hukuki) ya da kamu makamlarının kuruluşunu, yetki ve sorumluluklarını yöneten ya da usulü içeren kuralları kapsar. Özellikle, devletlerin anayasalarını, yasalarını ve bu yasalara dayanan

⁹ Bkz. Avrupa Adalet Divanı, František Ryneš v. Úřad, 11 Aralık 2014, C212/13k

tüm düzenleyici tedbirleri (kararnameler, düzenlemeler, emirler ve idari direktifler) içerir. Ayrıca, AB hukuku dahil olmak üzere, iç hukukta geçerli uluslararası sözleşmeleri de kapsar. Ayrıca, kamu hukuku ya da özel hukukun (sözleşmeler hukuku dahil), teamül hukuku ülkelerinde mahkeme kararları ya da tüm ülkelerde yazılı yasayı yorumlayan içtihat hukuku ile birlikte, genel nitelikli diğer tüm yasalarını içerir. Ek olarak, kanun koyucu tarafından verilen yetkiler kapsamında ve bağımsız kural koyma yetkileri uyarınca hareket eden meslek organlarının herhangi bir işlemini de içerir.

33. “Tarafların iç hukuku”, iyi uygulama ilkeleri veya mesleki ahlak ilkeleri gibi veri koruma alanındaki bağlayıcı olmayan düzenlemelerle güçlendirilebilir. Ancak, bu tür düzenlemeler Konvansiyon’a tam olarak uyulmasını sağlamak için kendi başına yeterli değildir.

34. Uluslararası organizasyonların¹⁰ söz konusu olduğu bazı durumlarda, bu tür kuruluşların kanunları üye devletlerde, her birinin ulusal hukuk sistemine bağlı olarak, doğrudan ulusal düzeyde uygulanabilir.

35. Konvansiyon hükümlerinin uygulanmasını sağlayan güvencelerin uygulamadaki etkinlik çok önemlidir. Gözetim otoritesinin (veya otoritelerinin) rolü, ilgili kişilere sunulan her türlü çözüm yolunun yanı sıra, bir Tarafın Konvansiyon hükümlerini uygulamadaki genel etkinliği değerlendirilirken dikkate alınmalıdır.

36. İkinci fıkrada ayrıca, Konvansiyon’un uygulanmasını sağlayan güvencelerin ilgili Taraflarca alınacağı ve bir Taraf onay veya katılma yoluyla Konvansiyon ile hukuki olarak bağlandığında yürürlüğe gireceği belirtilmiştir. Bu hüküm, Konvansiyon Komitesi’nin tüm “gerekli güvencelerin” alınıp alınmadığını doğrulamasını, Konvansiyon’a taraf olanların taahhütlerini yerine getirmelerini ve iç hukuklarında beklenen veri koruma seviyesini sağlamalarını temin etmeyi amaçlar. Bu doğrulama için kullanılan işlem ve kriterler, Konvansiyon Komitesi’nin usul kurallarında açıkça tanımlanacaktır.

37. Taraflar üçüncü fıkrada, Konvansiyon ilkelerinin uygulamasının (ve etkinliğini) düzenli olarak değerlendirilmesi amacıyla, taahhütlerine uygunluklarının değerlendirilmesine aktif olarak katkıda bulunacaklarına dair taahhütte bulunurlar. Taraflarca veri koruma yasasının uygulanmasına ilişkin raporların sunulması bu aktif katkının olası bir parçasıdır.

38. Konvansiyon Komitesi üçüncü fıkra uyarınca yetkilerini kullanırken, bir Tarafın Konvansiyon hükümlerine uygun olarak istisnalar ve kısıtlamalar kullanması halinde etkili güvenceleri alıp almadığını değerlendirmeyecektir. Buradan anlaşılacağı üzere, 11inci maddenin üçüncü fıkrası uyarınca bir Tarafın, Konvansiyon Komitesi’ne gizli bilgi vermesi gerekmez.

39. Bir Tarafın uygunluğunun değerlendirilmesi, Konvansiyon Komitesi tarafından oluşturulan ve usul kurallarında tam olarak açıklanan objektif, adil ve şeffaf bir prosedür temelinde Konvansiyon Komitesi tarafından yapılır.

Madde 5 – Veri İşlemenin Meşruluğu ve Verilerin Niteliği

40. Birinci fıkra veri işlemenin orantılı, izlenen meşru amaca uygun olması ve ilgili kişinin menfaatlerini, haklarını ve özgürlüklerini veya kamu yararını dikkate alması gerektiğini belirtir. Böyle bir veri işleme, menfaatlere, haklara ve özgürlüklere orantısız bir müdahaleye

¹⁰ Uluslararası organizasyonlar, uluslararası kamu hukukuna tabi organizasyonlar olarak tanımlanır.

yol açmamalıdır. Orantılılık ilkesine, ilk aşamada yani işlemin yapılıp yapılmayacağına karar verirken de dahil olmak üzere, tüm aşamalarda saygı duyulması gerekir.

41. İkinci fıkra, hukuki bir işleme faaliyeti için iki alternatif zorunlu ön koşul getirmektedir: Bireyin rızası veya kanunda öngörülen meşru bir temel. Beşinci maddenin 1, 2, 3 ve dördüncü fıkraları kümülatiftir ve veri işleme faaliyetinin meşruiyeti için bunlara saygı gösterilmelidir.

42. İlgili kişinin rızası serbestçe verilmiş, belirli bir konuya ilişkin, bilgilendirilmeye dayanmalı ve açık olmalıdır. Bu rıza, ya bir ifade (yazılı, elektronik yollar da dâhil, veya sözlü) ya da açık bir olumlu eylemle verilen ve belirli bir konuya ilişkin kişisel veri işleme teklifinin kabul edildiğini açıkça gösteren, kasıtlı bir tercihin serbest ifadesini temsil etmelidir. Sessizlik, hareketsizlik veya önceden onaylanmış formlar veya kutular bu nedenle rıza teşkil etmemelidir. Rıza aynı amaç veya amaçlarla gerçekleştirilen tüm işlem faaliyetlerini kapsamalıdır (çok amaçlı olması durumunda, her farklı amaç için rıza verilmelidir). Farklı rıza kararlarını gerektiren durumlar olabilir (örneğin, amaç aynı olsa bile verinin doğası farklı olduğunda- örneğin konum verileri ile sağlık verileri: bu gibi durumlarda, ilgili kişi konumunun işlenmesine izin verip sağlık verilerinin işlenmesine izin vermeyebilir). İlgili kişiye doğrudan veya dolaylı olarak, herhangi bir etki veya baskı (ekonomik veya başka bir nitelikte olabilir) uygulanamaz ve rızanın, ilgili kişinin gerçek veya özgür bir seçme şansının olmadığı veya etki altında kalmadan reddetme veya rızayı geri almanın mümkün olmadığı durumlarda serbestçe verildiği kabul edilmemelidir.

43. Bilimsel araştırmalar bağlamında, veri toplama sırasında bilimsel araştırma amaçlı kişisel veri işleminin amacını tam olarak belirlemek çoğu zaman mümkün değildir. Bu nedenle, ilgili kişilerin bilimsel araştırma için tanınmış etik standartlara uygun olarak bilimsel araştırmaların belirli alanlarına rıza göstermelerine izin verilmelidir. İlgili kişiler, amacın izin verdiği ölçüde, yalnızca belirli araştırma alanları veya araştırma projelerinin belli bölümleri için rıza gösterme fırsatına sahip olmalıdır.

44. Bilimsel araştırmalar bağlamında, veri toplama sırasında bilimsel araştırma amaçlı kişisel veri işleminin amacını tam olarak belirlemek çoğu zaman mümkün değildir. Bu nedenle, ilgili kişilerin bilimsel araştırma için tanınmış etik standartlara uygun olarak bilimsel araştırmaların belirli alanlarına rıza göstermelerine izin verilmelidir. İlgili kişiler, amacın izin verdiği ölçüde, yalnızca belirli araştırma alanları veya araştırma projelerinin belli bölümleri için rıza gösterme fırsatına sahip olmalıdır.

45. İlgili kişi, istediği zaman verdiği rızayı (işlemeye itiraz etme hakkından ayrı olarak) geri alma hakkına sahiptir. Bu, veri sorumlusunun rızanın geri çekildiğini öğrenmeden önce gerçekleştirdiği veri işleme faaliyetlerinin hukukiliğini etkilemeyecek, ancak kanunun öngördüğü meşru bir temelle gerekçelendirilmediği sürece verilerin işlenmesine devam etmesine izin vermeyecektir.

46. İkinci fıkrada atıfta bulunulan “kanunda öngörülen meşru temel” kavramı, diğerlerinin yanı sıra, ilgili kişinin taraf olduğu bir sözleşmenin (veya konuyla ilgili veri talebinde bulunulması durumunda) ifası için gerekli olan veri işleme; ilgili kişinin ya da başka bir kişinin hayati menfaatlerinin korunması için gerekli veri işleme; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için gerekli veri işleme; ve kamu yararı gerekçesiyle veya veri sorumlusunun veya üçüncü bir tarafın üstün gelen meşru menfaati için veri işlemeyi kapsar.

47. Kamu menfaati gerekçesiyle yapılan veri işleme; parasal, bütçe ve vergi ile ilgili konular, halk sağlığı ve sosyal güvenlik, cezai suçların önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması ve cezai cezanın uygulanması için yasalar tarafından düzenlenmelidir. Ulusal güvenlik önlemlerinin korunması, savunma, düzenlenmiş meslekler için etik ihlallerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması, medeni hukuk iddialarının uygulanması ve adli bağımsızlığın ve adli işlemlerin korunmasının yanı sıra kanun tarafından öngörülmalıdır. Veri işleme, örneğin, hayati tehlike arz eden bir salgının ve yayılmasının ya da insani acil durumların izlenmesi de dahil olmak üzere insani amaçlarla işlenen verilerde olduğu gibi, konuya ilişkin veriler hem kamu yararına hem de hayati menfaatlara hizmet edebilir. İkincisi, duruma göre değerlendirilecek olan acil durumlarla ilgili amaçlarla, sınırlı bir süre için, kayıp kişilerin kişisel verilerinin işlenmesinin gerekli olduğu doğal afet durumlarında ortaya çıkabilir¹¹. Ayrıca silahlı çatışmalar veya diğer şiddet eylemlerinde ortaya çıkabilir. Kişisel verilerin resmi makamlarca, resmi olarak tanınan dini derneklerin anayasa hukuku veya uluslararası kamu hukuku ile belirlenen amaçlara ulaşmak amacıyla işlenmesinin de kamu yararı temelinde gerçekleştirildiği kabul edilebilir.,

48. Hukuka uygun işleme şartları 3 ve dördüncü fıkralarda belirtilmiştir. Kişisel veriler hukuki, adil ve şeffaf bir şekilde işlenmelidir. Kişisel veriler açık, belirli ve meşru amaçlar için toplanmış olmalı ve söz konusu verinin işlenmesi bu amaçlara hizmet etmeli veya en azından bunlarla uyumsuz olmamalıdır. Belirli “amaçlara” yapılan atıf, verilerin tanımlanmamış, kesin olmayan veya muğlak amaçlarla işlenmesine izin verilmediğini gösterir. Amaç, bir yandan kişisel verilerin korunması, öte yandan diğer hakların korunması, örneğin, ilgili kişinin çıkarları ile veri sorumlusunun veya toplumun çıkarları arasında olduğu gibi, her durumda söz konusu olan tüm hakların, özgürlüklerin ve çıkarların dengelenmesini sağlamaktır; bu sebeple neyin meşru bir amaç olarak kabul edildiği duruma göre değişmektedir.

49. *Amaca uygun kullanım* kavramı, işlemin şeffaflığını, hukuki belirliliğini, öngörülebilirliğini veya adaletini engellememelidir. Kişisel veriler, ilgili kişinin beklemediği, uygunsuz veya sakıncalı olabilecek şekilde işlenmemelidir. Başkaca bir işleme amacının, kişisel verilerin başlangıçta toplandığı amaç ile uyumlu olup olmadığını tespit etmek için, veri sorumlusu, asıl işlemin yasallığıyla ilgili tüm gereklilikleri yerine getirdikten sonra, bunların yanında asıl amaçlar ve planlanan başkaca işleme amaçları arasında bağlantı; kişisel verilerin toplandığı bağlam, özellikle veri sorumlusuyla olan ilişkilerine dayanarak ilgili kişilerin makul kullanım beklentileri; kişisel verilerin niteliği; ilgili kişiler için planlanan başkaca işlemlerin sonuçları; ve hem asıl hem de planlanan ilave işleme faaliyetlerinde uygun önlemlerin varlığını da hesaba katmalıdır.

50. Dördüncü fıkranın (b) bendinde belirtilen kişisel verilerin başkaca amaçlarla işlenmesi, kamu yararı için arşivleme, bilimsel veya tarihsel araştırma veya istatistiksel amaçlarla, diğer güvencelerin mevcut olması koşuluyla (örneğin, verinin tanımlanabilir halinin saklanması gereken durumlar haricinde verilerin anonimleştirilmesi veya takma ad verme; meslek sırları; yukarıda belirtilen amaçlarla özellikle istatistik ve kamu arşivleri ile ilgili olarak kısıtlı erişimi ve verinin iletimini düzenleyen hükümler ve diğer teknik ve organizasyonel veri güvenliği önlemleri) elde edilen bilgilerin belirli bir bireye ilişkin kararlar veya önlemler için kullanımı dışında, uygun olarak değerlendirilir. “İstatistiksel amaçlar”, istatistiksel araştırmaların hazırlanmasını veya istatistiksel, kümelenmiş sonuçların üretilmesini ifade eder. İstatistik, belli bir nüfustaki toplu veya ortak olayları analiz etmeyi ve karakterize etmeyi amaçlar. İstatistiksel amaçlar kamu ya da özel sektör tarafından

¹¹ 1949 tarihli Cenevre Sözleşmeleri, 1977 tarihli Ek Protokolleri ve Uluslararası Kırmızı Haç ve Kırmızı Hilal Hareketleri Statüsü uygulanır.

güdülebilir¹². Verilerin “bilimsel araştırma amacıyla” işlenmesi, araştırmacılara çeşitli bilimsel alanlarda (epidemioloji, psikoloji, ekonomi, sosyoloji, dilbilim, siyaset bilimi, kriminoloji, vb.) kapsadığı tüm bireyleri aşan kalıcı ilkeler, davranış yasaları veya nedensellik kalıpları oluşturmak amacıyla bilgi sağlamayı hedefler¹³. “Tarihsel araştırma amacı” kalıtımsal araştırmaları içerir. “Kamunun yararına arşivleme amacı” ayrıca kamunun menfaatini ilgilendiren durumlarda özel hukuk kişilerinin arşivlerini de kapsayabilir.

51. İşlenmekte olan kişisel veriler elverişli, ilgili ve ölçülü olmalıdır. Ayrıca, veriler doğru olmalı ve gerekli hallerde düzenli olarak güncellenmelidir.

52. Dördüncü fıkranın (c) bendinde belirtilen işlenen verilerin “ölçülü” olması gerekliliği, öncelikle veri işlemenin işleme amacı için gerekli olanla sınırlı kalmasını gerektirir. Kişisel veri yalnızca, kişisel veri içermeyen bilgilerin işlenmesiyle amaçların makul bir şekilde yerine getirilemediği durumlarda işlenmelidir. Bu gereklilik sadece niceliği değil, aynı zamanda kişisel verilerin niteliğini de ifade eder. Yeterli ve ilgili olan ancak temel hak ve özgürlüklere orantısız bir müdahaleye yol açacak kişisel veriler, ölçüsüz olarak kabul edilmeli ve işlenmemelidir.

53. Dördüncü fıkranın (e) bendinde yer verilen kişisel verilerin depolanmasına ilişkin zaman sınırlamaları, verilerin işleme amacı gerçekleştirildikten sonra silinmesi ya da yalnızca ilgili kişinin doğrudan veya dolaylı olarak belirlenmesini önleyecek bir biçimde saklanması gerektiği anlamına gelir.

54. On birinci maddenin dördüncü fıkrasında belirtilen istisnalara, 11inci maddenin 1inci fıkrada belirtilen koşullar altında izin verilir.

Madde 6 – Özel Veri Kategorileri

55. Belirli veri türlerinin işlenmesi veya ortaya hassas bilgiler çıkaran belirli verilerin işlenmesi, menfaatlara, haklara ve özgürlüklere zarar verebilir. Bu verilerin işlenmesi örneğin, bir bireyin onurunun veya fiziksel bütünlüğünün ayırımı ya da zarar görme riskinin olduğu, ilgili kişinin cinsel yaşamı ya da cinsel yönelimi gibi en mahrem alanını ya da masumiyet karinesini etkileyebilir. Ancak Konvansiyon’un diğer koruyucu hükümlerini tamamlayan, yasalarca belirtilen uygun güvenlik önlemlerinin sağlandığı hallerde kabul edilmelidir. Konvansiyon hükümlerini tamamlayan uygun korumaların gerekliliği, 9uncu madde uyarınca ilgili kişilere verilen haklara 11inci maddeyle getirilen istisna ve kısıtlamaları dışlamaz.

56. İlgili kişiye yönelik olumsuz etkilerin önlenmesi için, tek başına veya kümülatif olarak; ilgili kişinin açık onayı; işlemle hedeflenen amaç ve araçları veya bu işlemlerin yapılmasına izin verilebilecek istisnai durumları belirten bir yasa; bir mesleki sır yükümlülüğü; risk analizini takiben alınan önlemler; belirli ve nitelikli bir organizasyonel veya teknik güvenlik önlemi (örneğin veri şifreleme) gibi özel nitelikli verilerin meşru amaçlarla işlenmesine uygun güvenlik önlemleri (örneğin, söz konusu risklere ve korunacak menfaatlara, haklara ve özgürlüklere uyarlanmış) belirlenmelidir.

¹² Bkz. Bakanlar Komitesinin (97)18 sayılı istatistiksel amaçla toplanıp işlenen kişisel verilerin korunması ile ilgili Tavsiye Kararı, Ek, 1, 30 Eylül 1997

¹³ Bakanlar Komitesinin üye devletlere (97)18 sayılı istatistiksel amaçla toplanıp işlenen kişisel verilerin korunması Tavsiye Kararıyla ilgili Açıklayıcı Bilgi Notu, 11. Ve 14. fıkra

57. Belirli veri işleme türleri, işlemin içeriğinden bağımsız olarak ilgili kişiler için özel risk taşıyabilir. Örnek olarak bireyler tarafından bırakılabilen ve kişinin veya üçüncü kişilerin sağlığı veya soyu hakkında bilgi açığa çıkarabilen genetik verilerin işlenmesi durumu gösterilebilir. Genetik veriler, bir bireyin kalıtsal veya doğum öncesi gelişim sırasında edindiği genetik özellikleri ile ilgili tüm verilerdir. İlgili bireyden alınan bir biyolojik örneğin kromozomal, DNA veya RNA analizi veya eşdeğer bilgilerin elde edilmesini sağlayan herhangi bir başka analizle ortaya çıkar. Cezai suçlar (şüpheli suçlar dahil), ceza mahkumiyetleri (ceza hukukuna dayalı ve cezai kovuşturmalar çerçevesinde) ve ilgili kişilerin hak ve özgürlükleri için uygun önlemlerin alınmasını gerektiren ilgili güvenlik önlemleri (örneğin, özgürlükten mahrum bırakma) ile ilgili verilerin işlenmesiyle benzer riskler ortaya çıkmaktadır.

58. Biyometrik verilerin (bireyin kendine özgü bir şekilde belirlenmesine veya doğrulanmasına izin veren, bir bireyin fiziksel, biyolojik veya fizyolojik özellikleriyle ilgili spesifik teknik bir işlemde kaynaklanan verilerin) işlenmesi, aynı zamanda ilgili kişiyi benzersiz bir şekilde belirlemek için kullanıldığında özel nitelikli olarak kabul edilir.

59. Görüntülerin işlenmesi durumu, verilerin özel niteliğine göre değişiklik gösterir. Görüntülerin işlenmesi, genel olarak özel nitelikli verilerin işlenmesi teşkil etmeyecektir çünkü görüntüler, yalnızca belirli bir teknik yöntemle işlendiğinde bir bireyin kesin olarak belirlenmesine veya doğrulanmasına izin veriyorsa biyometrik veri olarak tanımlanacaktır. Ayrıca görüntülerin işlenmesiyle ırk, etnik köken veya sağlık bilgisinin ortaya çıkarılması amaçlandığında (aşağıdaki noktaya bakınız), bu işlem özel nitelikli verilerin işlenmesi olarak kabul edilecektir. Aksine, bir güvenlik kamerası sistemi tarafından bir alışveriş alanına ait yalnızca güvenlik nedenleriyle işlenen görüntüler, genellikle özel nitelikli verilerin işlenmesi olarak değerlendirilmez.

60. Özel nitelikli verilerin işlenmesi, işleme sonucu ortaya çıkan belirli bilgiler sebebiyle ilgili kişilerin haklarını olumsuz yönde etkileme potansiyeline sahiptir. Soyadların işlenmesi birçok durumda bireyler için herhangi bir risk (örneğin, ortak maaş bordrosu amacı) içermese de bu gibi işlemler bazı durumlarda, örneğin amaç, bireylerin isimlerinin dilsel kökenlerinden yola çıkarak etnik kökenlerini veya dini inançlarını ortaya koymak olduğunda özel nitelikli veri teşkil edebilir. Sağlık bilgileri, bir bireyin fiziksel veya zihinsel sağlığı ve hasta veya sağlıklı olma durumu ile ilgili geçmişe, şimdiye ve geleceğe ilişkin bilgileri içerir. Kalın gözlüklü, kırık bacaklı, yanık tenli veya sağlığına ilişkin diğer görülebilir ayırt edici özelliklere sahip kişilerin görüntülerinin işlenmesi, yalnızca, işleme resimlerden elde edilebilecek sağlık bilgisine dayandığında özel nitelikli verilerin işlenmesi olarak kabul edilebilir.

61. Özel nitelikli verilerin istatistiksel bir amaç için işlenmesi gerektiğinde veriler, ilgili kişinin kimliği belirlenemeyecek şekilde toplanmalıdır. Kimlik belirten veriler olmadan özel nitelikli verilerin toplanması, Madde 6 kapsamında güvence altındadır. İstatistiksel amaçlar için özel nitelikli verilerin kimlik belirlenebilir biçimde toplanmasının meşru bir ihtiyaç olduğu durumlarda (örneğin bir tekrar veya dikey bir anket gerçekleştirildiğinde) uygun önlemler alınmalıdır¹⁴.

Madde 7 – Veri Güvenliği

62. Veri sorumlusu ve uygulanabildiği durumlarda veri işleyen aşağıdakileri dikkate alarak her işlem için hem teknik hem de organizasyonel nitelikte özel güvenlik önlemleri almalıdır:

¹⁴ Bkz. Bakanlar Komitesinin (97)18 sayılı Tavsiye Kararı, a.g.e.

birey için olası olumsuz sonuçlar, kişisel verilerin niteliği, işlenmiş kişisel verilerin hacmi, işleme için kullanılan teknik mimarinin saldırıya açıklık derecesi, verilere erişimi kısıtlama ihtiyacı, uzun süreli saklama ile ilgili şartlar vb.

63. Güvenlik önlemleri, veri işleme alanındaki veri güvenliği yöntem ve tekniklerinin mevcut durumunu göz önünde bulundurmalıdır. Bunların maliyetleri, potansiyel risklerin ciddiyeti ve olasılığı ile orantılı olmalıdır. Güvenlik önlemleri gözden geçirilmeli ve gerektiğinde güncellenmelidir.

64. Güvenlik önlemleri birtakım riskleri önlemeyi amaçlarken, 2nci fıkra bireyin temel hak ve özgürlüklerine ciddi şekilde müdahale edebilecek bir veri ihlali yaşanması durumu için özel bir yükümlülük içerir. Örneğin, mesleki sır kapsamında olan veya finansal, itibar veya fiziksel zarar veya küçük düşürmeyle sonuçlanabilecek verilerin açıklanması “ciddi” bir müdahale olarak kabul edilebilir.

65. Böyle bir veri ihlali meydana geldiğinde veri sorumlusunun, 11inci maddenin 1inci fıkrasında öngörülen istisnaya tabi olarak, ilgili gözetim otoritelerine, konu olan olayla ilgili haber vermesi gerekmektedir. Veri sorumlusu ayrıca ihlale ve olası sonuçlarına karşı alınan ve/veya önerilen önlemleri de gözetim otoritelerine bildirmelidir.

66. Veri sorumlusu tarafından gözetim otoritelerine yapılan bildirim, diğer ek bildirimleri engellemez. Örneğin, veri sorumlusu, özellikle veri ihlalinin bireylerin hak ve özgürlükleri, örneğin ayrımcılık, kimlik hırsızlığı veya dolandırıcılık, maddi kayıp, itibarın zarar görmesi, mesleki gizlilik veya diğer önemli ekonomik veya sosyal dezavantajlar sebebiyle korunan verilerin gizliliğinin kaybı gibi önemli bir riskle sonuçlanabileceği durumlarda, ilgili kişilere bildirme ve bunlara ihlalin olumsuz etkilerinin azaltılması için temas noktaları ve olası önlemler konusunda yeterli ve anlamlı bilgiler sağlamak ihtiyacı duyulabilir. Veri sorumlusunun ilgili kişiyi veri ihlali konusunda kendiliğinden bilgilendirmediği durumlarda ihlalin olası olumsuz etkilerini göz önünde bulunduran gözetim otoritesinin veri sorumlusundan bunu talep etmesi gerekir. Bilgisayar sistemleri güvenliğinden sorumlu olanlar gibi diğer ilgili makamlara bildirimde bulunulması da istenebilir.

Madde 8 – İşlemenin Şeffaflığı

67. Veri sorumlusunun, adil işlemeyi sağlamak amacıyla veri işlerken şeffaf olmasını ve ilgili kişilerin bu veri işleme bağlamında haklarını anlayarak tam olarak kullanmalarını sağlamak gerekmektedir.

68. Bazı temel bilgilerin, veri sorumlusu tarafından ilgili kişilere doğrudan veya dolaylı olarak (ilgili kişi üzerinden değil, üçüncü kişi aracılığıyla) veri toplanırken, on birinci maddenin 1inci fıkrası doğrultusundaki olası istisnalara tabi olarak, proaktif bir şekilde zorunlu olarak verilmesi gerekmektedir. Veri sorumlusunun (veya ortak veri sorumlularının) adı ve adresi, veri işlemenin yasal dayanağı ve amaçları, işlenen veri kategorileri ve alıcılar ile hakların kullanımının yolları hakkında bilgiler ilgili kişiye adil ve etkin bir şekilde sunulduğu sürece uygun bir biçimde (bir web sitesi, kişisel cihazlardaki teknolojik araçlar vb. aracılığıyla) sağlanabilir. Sunulan bilgiler kolayca erişilebilir, okunaklı, anlaşılabilir ve ilgili kişilere uyarlanmış olmalıdır (örneğin, gerektiğinde çocukların anlayabileceği bir dilde). Adil veri işlemeyi sağlamak veya bu amaç için faydalı olan, saklama süresi veya veri işlemenin altında yatan nedenler veya başka bir Tarafa veya Taraf olmayan (söz konusu Taraf olmayanların belirli bir düzeyde veri koruma sağlayıp sağlamadığı veya veri sorumlusunun

böyle bir uygun veri koruma düzeyini sağlamak için aldığı önlemler dahil) bir alıcıya veri aktarımı gibi her ilave bilgi de sağlanacaktır.

69. Veri sorumlusunun, ilgili kişinin zaten bildiği; işlemin yasalarca açıkça belirtildiği ve verinin üçüncü kişiler aracılığıyla dolaylı olarak toplandığı; ilgili kişi doğrudan belirlenemediği için veya veri sorumlusunun ilgili kişiyle iletişime geçme imkanı olmadığı ya da bunun orantısız çaba gerektirdiği veya imkansız olduğu durumlarda bilgi sağlanması gerekli değildir. Bu imkansızlık hem yasal bir nitelikte (örneğin bir cezai soruşturma bağlamında) hem de pratik nitelikte olabilir (örneğin, bir veri sorumlusu yalnızca fotoğraf işlerken ve ilgili kişilerin adlarını ve iletişim bilgilerini bilmediğinde).

70. Veri sorumlusu, ilgili kişileri toplu olarak (bir web sitesinde veya genel duyuru suretiyle) veya bireysel olarak bilgilendirmek için uygun, makul ve düşük maliyetli herhangi bir yöntemi kullanabilir. İşleme başlarken bunu yapmak mümkün değilse, daha sonraki bir aşamada, örneğin veri sorumlusu herhangi bir yeni nedenle dolayı ilgili kişi ile temasa geçtiğinde yapılabilir.

Madde 9 – İlgili Kişinin Hakları

71. Bu madde, her bireyin kendisiyle ilgili kişisel verilerin işlenmesi konusunda kullanması gereken hakları listelemektedir. Konvansiyon'un Tarafları, yasal mevzuatları dahilinde, her bir ilgili kişinin tüm bu hakları yasal ve pratik olarak yeterli ve etkili yollarla birlikte kullanabilmesini sağlayacaktır.

72. Bu haklar aşağıdakileri içermektedir:

- Herkesin, kendisinin görüşleri dikkate alınmadan tamamen otomatik yollarla veri işlenmesi sonucunda kendisini esaslı bir şekilde etkileyen bir karara tabi olmama hakkı (*a bendi*);
- Herkesin kendileriyle ilgili işlenen bir verinin onayını isteme ve verilere makul aralıklarla ve aşırı gecikme veya harcama olmadan erişme hakkı (*b bendi*);
- Talep halinde, herkesin, sonuçlarının kendilerine uygulandığı veri işleme faaliyetlerinin gerekçesini öğrenme hakkı (*c bendi*);
- Veri sorumlusu, ilgili kişilerin çıkarlarını veya temel hak ve özgürlüklerini geçersiz kılan işlem için meşru bir zemin göstermediği sürece, ilgili kişilerin kendi durumlarıyla ilgili gerekçelerle, kendileriyle ilgili kişisel verilerin işlenmesine itiraz etme hakkı (*d bendi*);
- Kişisel verilerin eksik, yanlış veya hukuka aykırı olarak işlenmiş olması hâlinde bunların düzeltilmesini veya silinmesini isteme; (*e bendi*);
- Önceki haklardan herhangi birine uyulmadığı takdirde, herkesin bir başvuru yolundan yararlanma hakkı (*f bendi*);
- Herkesin bir gözetim otoritesinden yardım alma hakkı (*g bendi*).

73. Bu hakların diğer haklarla ve meşru menfaatlerle uyumlu olması gerekmektedir. On birinci maddeye uyarınca bu haklar, kanunla ve demokratik bir toplumda gerekli ve orantılı bir önlem oluşturması halinde sınırlandırılabilir. Örneğin, kişisel verileri silme hakkı, veri sorumlusunun tabi olduğu yasa ile işlemeyi gerektiren yasal bir zorunluluğa uyulması, kamu yararına yürütülen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin tatbikinde gerçekleştirilen bir görevin yerine getirilmesi için işlemin gerekli olduğu ölçüde kısıtlanabilir.

74. Konvansiyon, bir ilgili kişinin kimden onay, iletişim, düzeltme, vb. alabileceğini veya görüşlerine itiraz edebileceğini ya da görüşlerini ifade edebileceğini belirtmese de, çoğu

durumda bu veri sorumlusu veya onun adına veri işleyen olacaktır. İstisnai durumlarda, erişim, düzeltme ve silme haklarını kullanma yöntemleri gözetim otoritesinin aracılığını içerebilir. Sağlık verileriyle ilgili olarak, haklar, doğrudan erişimden farklı bir şekilde de kullanılabilir. Örneğin, ilgili kişinin menfaatine olduğu hallerde bir sağlık uzmanının yardımıyla, özellikle de verileri anlamalarına yardımcı olmak veya ilgili kişinin psikolojik durumunun bilgi verirken uygun şekilde göz önünde bulundurulmasını sağlamak için ve tabii deontolojik ilkeler doğrultusunda haklar kullanılabilir.

75. *a bendi.* Tamamen otomatik yollarla alınan bir kararın konusunu oluşturan bir bireyin, kendi görüşünü ve argümanlarını anlamlı bir şekilde ileri sürerek böyle bir karara itiraz etme hakkı vardır. Özellikle, ilgili kişi, otomatik yollarla alınan bir kararda kullanılmadan önce kişisel verilerin olası yanlışlığını, kendi özel durumuna uygulanacak profilin alakasız olduğunu veya kararın sonucunu etkileyebilecek diğer faktörleri ortaya koyma fırsatına sahip olmalıdır. Bu, özellikle, bireylerin, sosyal haklarının kısıtlanmasına veya reddedilmesine neden olan algoritmik akıl yürütmenin uygulanmasıyla damgalanmaları veya kredi kapasitelerinin yalnızca bir yazılım tarafından değerlendirildiğini gördükleri durumlardır. Ancak, otomatik yollarla alınan karar, veri sorumlusunun tabi olduğu bir yasa ile izin verilmiş ise ve aynı zamanda ilgili kişinin haklarını, özgürlüklerini ve meşru çıkarlarını korumak için uygun önlemleri ortaya koyuyor ise ilgili kişi bu hakkı kullanamaz.

76. *b bendi.* İlgili kişinin, kişisel verilerinin işlenmesi hakkında bilgi sahibi olmaya hakkı vardır. Erişim hakkı prensip olarak ücretsiz olmalıdır. Bununla birlikte, (b) bendinin ifadesi, veri sorumlusunun belirli şartlarda; taleplerin aşırı olduğu ve birden fazla süreci kapsadığı durumlarda makul bir ücret talep etmesine engel olmadığını belirtmektedir. Böyle bir ücret istisnai ve her halükarda makul olmalı ve ilgili kişilerin haklarını kullanmalarını engellememeli veya caydırmamalıdır. Ayrıca, veri sorumlusu veya veri işleyen, özellikle tekrarlayan nitelikleri nedeniyle açıkça temelsiz veya aşırı isteklere cevap vermeyi reddedebilir. Veri sorumlusu böyle durumlarda, reddin sebebini açıklayabiliyor olmalıdır. Erişim hakkının adil bir şekilde kullanılmasını sağlamak iletişimin “anlaşılabilir” olması, içeriğe olduğu kadar standartlaştırılmış dijital iletişim biçimi için de geçerlidir.

77. *c bendi.* İlgili kişilere, profil oluşturma da dahil olmak üzere, otomatik yollarla alınan kararlar için algoritmaların kullanılmasını içeren işlemlerde, bu işlemlerin altında yatan sebepleri ve işlemlerin olası amaçlarını bilme hakkı verilmelidir. Örneğin, kredi puanlaması durumunda, ilgili kişilere, yalnızca kararın kendisi hakkında bilgi vermek yerine verilerinin işlenmesini destekleyen ve “evet” veya “hayır” kararıyla sonuçlanan mantığı bilme hakkı verilmelidir. Bu unsurların anlaşılması, itiraz hakkı ve yetkili bir makama şikayette bulunma hakkı gibi diğer temel koruma önlemlerinin etkin bir şekilde kullanılmasına önemli derecede katkıda bulunur.

78. *d bendi.* İtiraz etme hakkı nezdinde veri sorumlusunun, ilgili kişilerin menfaatlerini, haklarını veya özgürlüklerini olumsuz etkileyen veya geçersiz kılan veri işleme faaliyeti için meşru bir temeli olabilir. Örneğin kamu güvenliği veya yasal taleplerin oluşturulması, kullanılması ve savunulması için veri işlemenin devamının gerekmesi veri işlemeyi haklı kılan meşru zeminler olarak kabul edilebilir. Bu durumun olay bazında değerlendiriliyor olması gerekir ve işleme devam ederken böyle zorlayıcı meşru gerekçelerin gösterilmemesi yasadışı olarak kabul edilebilir. İtiraz etme hakkı düzeltme veya silme hakkından farklı ve ayrı bir şekilde kullanılmaktadır (*e bendi*).

79. Pazarlama amacıyla veri işlenmesine itiraz, itiraz kapsamındaki kişisel verilerin koşulsuz olarak silinmesi veya ortadan kaldırılması ile sonuçlanmalıdır

80. İtiraz hakkı, bir kanun ile sınırlandırılabilir. Buna örnek olarak cezai suçların soruşturulması veya kovuşturulması verilebilir. Durumun niteliğine göre, ilgili kişi, dayandığı işlemin yasallığına itiraz edebilir. Veri işleminin geçerli bir rızaya dayandığı hallerde ilgili kişi, itiraz hakkını kullanmak yerine rızasını geri çekme hakkını kullanabilir. İlgili kişi rızasını geri çekebilir ve dolayısıyla rızanın geri çekilmesiyle ilgili olarak mevzuattan doğabilecek veri sorumlusunun tazmini gibi bir sorumluluk söz konusu olacaktır. Benzer şekilde, veri işleminin bir sözleşmeye dayanması durumunda, ilgili kişi sözleşmeyi iptal etmek için gerekli aksiyonları alabilir.

81. *e bendi*. Düzeltme veya silme, gerekçeli ise ücretsiz olmalıdır. (e) bendinde belirtilen ilkeye uygun olarak elde edilen düzeltme ve silme işlemleri, imkansız olmadıkça veya orantısız çaba gerektirmedikçe, orijinal bilgilerin alıcılarının dikkatine sunulmalıdır.

82. *g bendi*, ilgili kişinin Konvansiyon tarafından sağlanan haklarını kullanmasında gözetim otoritesinden yardım alma hakkı sağlayarak bu haklarının etkili korunmasını sağlamayı amaçlar. İlgili kişinin başka bir Tarafın ülkesinde ikamet ettiği hallerde, bu Tarafın tayin ettiği otoritenin aracılığıyla talebini sunabilir. Yardım talebi, söz konusu veri işleminin tanımlanmasına izin verecek kadar yeterli bilgi içermelidir. Bu hak, 11inci maddeye göre sınırlandırılabilir veya derdest bir adli sürecin menfaatlerini korumak için uyarlanabilir.

83. Madde 11 paragraf 1'de belirtilen koşullar altında 9uncu maddeye getirilebilecek sınırlı istisnalara izin verilir.

Madde 10 – Ek Yükümlülükler

84. Kişisel verilerin korunması hakkının etkili olmasını sağlamak için, veri sorumlusuna ve uygulanabilir olduğu durumlarda veri işleyen(ler) e ilave yükümlülükler getirilmiştir.

85. Birinci paragrafta göre, veri sorumlusunun yeterli veri korumasını sağlama yükümlülüğü, veri işleminin yürürlükteki mevzuata uygun olduğunu doğrulama ve ortaya koyma sorumluluğuyla bağlantılıdır. Tasarım aşaması da dahil olmak üzere Konvansiyon'da belirtilen veri işleminin tüm aşamalarında uygulanacak olan veri koruma ilkeleri, ilgili kişileri korumayı ve onların güvenlerini arttırmayı amaçlar. Uyumluluğu sağlamak için veri işleyen ve veri sorumlusunun alması gereken önlemler arasında çalışanların eğitilmesi; uygun bildirim prosedürlerinin hazırlanması (örneğin verilerin sistemden silinmesi gereken zamanı belirten bildirim prosedürü); işlemeye yetkilendirmenin söz konusu olduğu hallerde Konvansiyon'un uygulanması için özel sözleşmesel hükümlerin oluşturulması; uyumluluğun doğrulanması ve ortaya konması için iç prosedürlerin oluşturulması yer almaktadır.

86. On birinci maddenin üçüncü paragrafına göre, bir Tarafın 15inci madde kapsamında gözetim otoritesinin yetkilerini, ulusal güvenlik ve savunma amaçlı işleme faaliyetlerine atıfta bulunarak sınırlandırmayı tercih etmesi durumunda veri sorumlusu, söz konusu istisna kapsamına giren faaliyetler için böyle bir gözetim otoritesine veri koruma gereklilikleriyle uyumlu olduğunu ortaya koyma yükümlülüğü altında değildir.

87. Veri sorumlusu tarafından bu tür bir uyumluluğun doğrulanması ve ortaya konması sürecinin yürütülmesini kolaylaştırmak için alınabilecek olası bir güvence, görevini yerine getirmek için gerekli imkanlara sahip bir "veri koruma görevlisinin" belirlenmesidir. Gözetim otoritesine atamaya ilişkin bilgi verilmesi gereken bu tür bir veri koruma görevlisi, veri sorumlusunun bünyesinden veya dışarıdan olabilir.

88. İkinci paragraf, bir veri işleme faaliyeti gerçekleştirmeden önce veri sorumlusunun, işlemenin ilgili kişilerin hakları ve temel özgürlükleri üzerindeki potansiyel etkisini incelemesi gerektiğini netleştirmektedir. Bu incelemeler aşırı formaliteler olmadan yapılabilir. Bu durumda orantılılık ilkesinin, amaçlanan işlemenin genel esasları da göz önünde bulundurularak, dikkate alınması gerekecektir. Veri işleyenin de veri sorumlusuna ek olarak sürece dahil olduğu durumlarda risk incelemesi yapması gerekmektedir. Güvenlik uzmanları ve tasarımcılar da dahil olmak üzere BT sistem geliştiricileri, kullanıcılar ve hukuk uzmanları ile birlikte risk inceleme sürecine yardımcı olabilirler.

89. Üçüncü paragraf, etkili bir koruma seviyesini daha iyi bir şekilde sağlayabilmek için, veri sorumlularının ve uygulanabilir olduğu ölçüde veri işleyenlerin, teknik ve idari tedbirler yoluyla veri işleme operasyonlarına veri koruma gerekliliklerini, ideali sistem mimarisi ve tasarımı aşamasında olmak üzere mümkün olan en kısa zamanda entegre etmelerini düzenlemektedir. Veri koruma gerekliliklerinin yerine getirilmeleri yalnızca verilerin işlenmesinde kullanılan teknolojiyle değil aynı zamanda ilgili iş ve yönetim süreçleriyle sağlanmalıdır. Uygulanacak mevzuata uyumu kolaylaştıran, kullanımı kolay işlevler oluşturulmalıdır. Örneğin, mümkün ve ilgili olan hallerde ilgili kişilerin kendi verilerine güvenli çevrimiçi erişim imkanı sunulmalıdır. İlgili kişilerin kendi verilerini kendi seçtikleri başka bir sağlayıcıya taşınmasını veya verileri kendilerinde tutmalarını sağlamak için kullanımı kolay araçlar da söz konusu olmalıdır (veri taşınabilirliği araçları). Varsayılan ayarlar için teknik gereklilikleri ayarlarken, uygulamaların ve yazılımların kullanımının ilgili kişilerin haklarını ihlal etmemesi ve özellikle meşru amaca ulaşmak için gerekenden fazla verinin işlenmesinde kaçınılması için veri sorumluları ve veri işleyenler gizlilik dostu standart yapılandırmaları seçmelidir (varsayılan veri koruma). Örneğin, sosyal ağlar, varsayılan olarak gönderi veya resimlerin tüm internette değil yalnızca sınırlı ve seçili çevrelerle paylaşılacak şekilde yapılandırılmalıdır.

90. Dördüncü paragraf, Tarafların, ilgili kişilerin menfaatleri, hakları ve temel özgürlükleri için riskleri göz önünde bulundurarak 1, 2 ve 3. paragraflarda listelenen ek yükümlülükleri belirlemelerine izin vermektedir. Bu tür bir adaptasyon, işlenen verilerin niteliği ve hacmi, veri işlemenin niteliği, kapsamı ve amaçları ve bazı durumlarda işleme yapan işletmenin büyüklüğü göz önünde bulundurularak yapılmalıdır. Örneğin, ticari faaliyetleri çerçevesinde ve başka amaçlar için tekrar kullanmadan, yalnızca müşterilerinden elde ettiği hassas olmayan kişisel bilgileri işleyen küçük ve orta ölçekli işletmelerin (KOBİ'ler) nezdinde aşırı maliyetler gerektirmeyecek şekilde yükümlülükler düzenlenmelidir. İlgili kişi için herhangi bir risk içermeyen işlemler gibi belirli veri işleme kategorileri, bu maddede öngörülen bazı ek yükümlülüklerden muaf dahi tutulabilir.

Madde 11 – İstisnalar ve Kısıtlamalar

91. İstisnaların kanunla öngörülmesi, temel hak ve özgürlüklerin özüne saygı duyması ve 11inci maddenin (a) ve (b) bentleri temelinde demokratik toplumda gereklilik şartına uygun olması şartıyla sınırlı sayıda hüküm (madde 5 paragraf 4, madde 7 paragraf 2, madde 8 paragraf 1 ve madde 9) dışında II. Bölüm hükümlerinde istisnalar kabul edilmez. “Demokratik bir toplumda gerekli” olan bir önlem, meşru bir amaç izlemeli ve daha az müdahaleci araçlarla sağlanamayan önemli bir sosyal ihtiyacı karşılamalıdır. Böyle bir önlem ayrıca, sürdürülmekte olan meşru amaçla orantılı ve ulusal otoritelerin hukuka uygunluğu ortaya koyabilmek için getirdiği nedenlerle ilgili ve yeterli olmalıdır. Böyle bir önlem, yeterince ayrıntılı olması gereken, erişilebilir ve öngörülebilir bir yasa ile belirlenmelidir.

92. Tüm kişisel veri işleme faaliyetleri, ilgili kişilere ilişkin olarak hukuka uygun, adil ve şeffaf olmalıdır ve sadece kişisel veriler sadece belirli amaçlar için işlenmelidir. Bu durum kendiliğinden kolluk birimlerinin soruşturma veya görüntülü izleme gibi faaliyetlerini engellemez. Bu tür faaliyetler, kanunlarla belirlendiği ve ilgili kişilerin meşru çıkarları göz önünde bulundurularak demokratik bir toplumda gerekli ve orantılı bir önlem teşkil ettiği sürece; ulusal güvenlik ve kamu güvenliğine yönelik tehditlerin önlenmesi ve korunması da dahil, suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması ve cezaların infazı amacıyla yapılabilir.

93. Bu istisnaların gerekliliği her olay bazında ve ilk paragrafın (a) ve (b) bentlerinde detaylandırılan genel kamu menfaati için temel hedefler ışığında incelenmelidir. (a) bendi, istisna gerektirebilecek devletin veya uluslararası organizasyonun genel kamu menfaatine yönelik bazı hedeflerini listelemektedir.

94. “Ulusal güvenlik” kavramı, Avrupa İnsan Hakları Mahkemesi'nin ilgili içtihat hukuku temelinde yorumlanmalıdır¹⁵.

95. “Önemli ekonomik ve finansal çıkarlar” terimi, özellikle vergi tahsilâtını ve döviz denetimini kapsar. Bu bentte “cezai suçların önlenmesi, soruşturulması ve kovuşturulması ve cezanın infazı” terimi, cezai kovuşturma ve buna ilişkin yaptırımların uygulanmasını içerir. “Genel kamu yararının diğer temel amaçları” terimi, diğerlerinin yanı sıra, düzenlenmiş meslekler için etik ihlallerin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması ile medeni hukuk iddialarının uygulanmasını kapsar.

96. (b) bendi, ilgili kişinin kendisi veya üçüncü taraflar gibi özel tarafların, basın özgürlüğü, akademik, sanatsal ve edebi ifade özgürlüğü, bilgi alma ve verme hakkı, yazışma ve iletişimin gizliliği, ticari sır ve yasal olarak korunan diğer sırlar dahil olmak üzere temel hak ve özgürlükleri (örneğin ilgili kişi kayıp olduğu için hayati çıkarları tehdit altında ise) ile ilgilidir. Bu bent özellikle görsel-işitsel alandaki, haber arşivlerindeki ve basın kütüphanelerindeki kişisel verilerin işlenmesi için uygulanmalıdır. Her demokratik toplumda ifade özgürlüğü hakkının önemini dikkate almak için, gazetecilik gibi özgürlükle ilgili kavramların geniş bir şekilde yorumlanması gerekmektedir.

97. İkinci paragraf, ilgili kişilerin temel hak ve özgürlüklerine aykırılık riski taşımayan ve arşivleme amacıyla yapılan, kamu yararı, bilimsel ya da tarihsel araştırma veya istatistiksel amaçlarla yapılan belirli veri işlemleriyle ilgili 8 ve 9uncu maddelerde belirtilen hükümlerin kısıtlanması olasılığına imkan vermektedir. İstatistik çalışmaları için verilerin, uygun veri koruma önlemlerinin mevcut olması şartıyla kamuya açık veya özel alanlarda, bu verilerin kümülatif formatta yayınlanması, yukarıdaki duruma örnek teşkil edebilir (bkz. paragraf 50).

98. Ulusal güvenlik ve savunma amaçlı işleme faaliyetleriyle ilgili olarak 4üncü maddenin 3üncü paragrafında, 14üncü maddenin 5 ve 6ncı paragraflarında ve 15inci maddenin 2nci paragrafının (a), (b), (c) ve (d) bentlerinde bulunan istisnalar, inceleme ve gözetim mekanizmalarının bağımsızlığına ve etkinliğine halel getirmez¹⁶.

¹⁵ İlgili içtihat hukuku, özellikle devlet güvenliğinin ve anayasal demokrasinin korunmasını, ve bunların yanı sıra casusluk, terörizm, terörü destekleme ve ayrımcılıktan korunmayı da içerir. Ulusal güvenliğin tehlikede olduğu durumlarda, sınırsız yetkiye karşı koruma sağlanmalıdır. Avrupa İnsan Hakları Mahkemesinin ilgili kararlarını Mahkeme'nin internet sitesinde (hudoc.echr.coe.int) bulabilirsiniz.

¹⁶ Avrupa Konseyi üyesi olan Taraflar için bu şartlar, Avrupa İnsan Hakları Mahkemesinin AİHS'nin 8. maddesi uyarınca içtihat hukuku ile geliştirilmiştir (bkz. AİHM, Roma Zakharov / Rusya (Başvuru No. 47143/06), 4 Aralık 2015, paragraf 233; Szabó ve Vissy / Macaristan (Başvuru No. 37138/14), 12 Ocak 2016, paragraflar 75 vd.).

Madde 12 – Yaptırımlar ve Başvuru Yolları

99. Konvansiyon'un etkin bir veri koruma düzeyi sağlaması için veri sorumlusu ve veri işleyenin görevleri ve ilgili kişilerin hakları, Tarafların ilgili yaptırım ve çözümlerle ilgili mevzuatlarına yansıtılmalıdır.

100. Bu adli ve adli olmayan yaptırımların niteliğinin (medeni, idari, cezai) belirlenmesi her bir Tarafa bırakılmıştır. Bu yaptırımlar etkili, orantılı ve caydırıcı olmalıdır. Aynı durum çözüm yolları için de geçerlidir: bu yöntemlerin tanımlanması Taraflara bırakılmakla beraber ilgili kişilerin bir karar veya uygulamaya kanun yoluyla itiraz etme imkânı olmalıdır. Kanun yolları dışında da ilgili kişilere çözüm yolları sunulmalıdır. İşlemeden kaynaklanan maddi ve manevi zararlar için parasal tazminat ve toplu davalar da dikkate alınmalıdır.

Madde 13 – Genişletilmiş Koruma

101. İşbu madde Avrupa İnsan Hakları Sözleşmesi'nin 53üncü maddesi ile benzer bir temele dayanmaktadır. Konvansiyon, tüm Tarafların kabul etmeye hazır olduğu veri koruma mevzuatı ilkelerine karşılık gelmektedir. Metin, bu ilkelerin, Taraflarca üzerine daha gelişmiş bir koruma sistemi kurulabilecek bir temel oluşturduğunu ifade etmektedir. Dolayısıyla "daha fazla koruyucu önlem" ifadesi Konvansiyon'un hali hazırda gerektirdiği koruma standartlarından daha az olmamak üzere daha yüksek bir korumayı ifade etmektedir.

Bölüm 3 – Kişisel Verilerin Sınır Ötesi Akışı¹⁷

Madde 14 – Kişisel Verilerin Sınır Ötesi Akışı

102. Bu maddenin amacı, kişisel verilerin işlenmesine ilişkin olarak bireylerin uygun seviyede korunmasını güvence altına almak kaydıyla (önsözde belirtildiği üzere) sınırlar önemli olmaksızın bilginin serbest akışının kolaylaştırılmasıdır. Kişisel verilerin, bir başka devletin veya uluslararası organizasyonun yetkisine tabi bir alıcıya ifşa edildiği veya erişilebilir kılındığı hallerde sınır ötesi veri aktarımı gerçekleşmiş olmaktadır.

103. Sınır ötesi akış rejiminin amacı, öncelikle bir Tarafın yetki alanında işlenen (örneğin orada toplanan veya depolanan veriler) ve daha sonra Konvansiyon'a Taraf olmayan bir devletin yetkisi altında olan bir yerde işlenen kişisel verilerin uygun güvenlik önlemleriyle işlenmeye devam etmesini sağlamaktır. Önemli olan, bir Tarafın yetkisi dahilinde işlenen verilerin, Konvansiyon'un ilgili veri koruma ilkeleri tarafından her zaman korunmaya devam etmesidir. Çok çeşitli koruma sistemleri söz konusu olabilmekle beraber sağlanan koruma, insan haklarının küreselleşmeden ve sınır ötesi veri akışlarından etkilenmemesini güvence altına alacak nitelikte olmalıdır.

104. Yurt içerisindeki akışlar alıcı Tarafın veri koruma rejimi kapsamında olduğu için 14üncü madde, yurt içerisinde aktarımlara değil, sadece yurt dışına aktarımlara uygulanır.

105. *Birinci paragraf*, Konvansiyon'un Tarafları arasında gerçekleştirilen aktarımları kapsamaktadır. Veri aktarımı, "sadece kişisel verilerin korunması amacıyla" yasaklanamaz veya özel izne tabi tutulamaz. Bununla birlikte, Konvansiyon, ulusal güvenlik, savunma, kamu güvenliği ve (devlet sırlarının korunması dahil) diğer kamu menfaatleri gibi başka

¹⁷ Değişiklik Protokolü'nün yürürlüğe girmesinden itibaren, gözetim otoriteleri ve sınır ötesi akışlara ilişkin Ek Protokol (ETS No. 181), değişik Konvansiyon'un ayrılmaz bir parçası olarak değerlendirilecektir.

amaçlarla bir Tarafın başka bir Tarafa kişisel veri aktarımını sınırlandırma özgürlüğünü kısıtlamaz.

106. Birinci paragraftaki hükmün gerekçesi, Konvansiyon'da belirtilen veri koruma hükümlerinin ortak temelini kabul etmiş tüm Tarafların, uygun olduğu düşünülen ve bu nedenle kural olarak verilerin özgür dolaşımına izin veren bir koruma düzeyi sunmasıdır. Bununla birlikte, kişisel verilerin bu serbest dolaşımının Konvansiyon uygulanmaması sonucu doğuracak gerçek ve ciddi bir risk teşkil ettiği istisnai durumlar olabilmektedir. Bir istisna olarak, bu hüküm dar yorumlanmalıdır ve Taraflar, riskin farazi veya düşük olduğu hallerde bu hükme dayanamayacaktır. Bu nedenle, bir Taraf, işbu istisnayı ancak belirli bir durumda, verileri başka bir Tarafa aktarımın, Konvansiyon kapsamında bu verilere sağlanan korumaları önemli ölçüde etkileyebileceği ve bu olasılığın yüksek olduğu konusunda açık ve güvenilir bir delil olması durumunda ileri sürebilecektir. Konvansiyon uyarınca sağlanan bazı korumaların diğer Tarafça artık garanti edilmediği durumlar (örneğin, gözetim otoritesinin işlevlerini etkin bir şekilde yerine getiremediğinden) veya başka bir Tarafa transfer edilen verilerin uygun bir koruma düzeyi sağlanmadan ikincil olarak aktarılmasının (ileri aktarım) muhtemel olması, bu duruma örnek oluşturmaktadır. Uluslararası hukukta tanınan bir başka istisna, Tarafların daha detaylı bir entegrasyon gözetim bölgesel (ekonomik) kuruluşlara dahil olan devletlerin paylaştığı uyumlaştırılmış veri koruma standartlarına tabi oldukları durumunda ortaya çıkmaktadır.

107. Bu durum, diğerlerinin yanında, AB üye ülkeleri arasında geçerlidir. Bununla birlikte, Genel Verileri Koruma Regülasyonu (AB) 2016/679'da açıkça belirtildiği üzere, üçüncü bir ülkenin Konvansiyon 108'e ve onun uygulanmasına katılımı, AB'nin uluslararası transfer rejimini uygularken, özellikle üçüncü ülkenin yeterli düzeyde koruma sağlayıp sağlamadığı değerlendirilirken (ve bu şekilde bu kişisel verilerin serbest akışına izin verilirken) önemli bir faktör olacaktır.

108. İkinci paragraf kural olarak "Konvansiyon hükümleri temelinde uygun bir koruma seviyesinin güvence altına alınmasını" sağlama yükümlülüğü getirmektedir. Aynı zamanda dördüncü paragraf uyarınca Taraflar, meşruluğun ortaya konması şartı ile, kanunla öngörölmüş olması ve bu tür transferlerin demokratik bir toplumda gerekli ve orantılı bir ölçüt teşkil etmesi (c bendi) durumunda "başta önemli kamu menfaatleri olmak üzere meşru menfaatleri ileri sürerek" uygun bir veri koruma seviyesi olması bile verileri aktarabilirler. Böylece kişisel veriler, 11inci maddenin 1 ve üçüncü paragraflarında listelenenlere benzer gerekçelerle aktarılabilir. Her halükarda Taraflar, veri koruması amacıyla veya başka nedenlerle veri transferini Taraf olmayan taraflara sınırlandırmak hususunda Konvansiyon kapsamında özgürlerdir.

109. İkinci paragraf, kişisel verilerin bir Tarafın yetkisi altında olmayan bir alıcıya aktarımını düzenlemektedir. Ulusal sınırlar dışına gerçekleştirilecek herhangi bir kişisel veri aktarımında, uygun bir koruma seviyesi garanti altına alınmalıdır. Alıcının Konvansiyon'a Taraf olmadığı durumlarda Konvansiyon, veri koruma seviyesinin gerçek anlamıyla uygun olmasını sağlamak için; kanun ile veya usulüne uygun olarak uygulanan geçici veya onaylanmış standartlaştırılmış güvenceler olmak üzere iki mekanizma kurar.

110. İkinci ve üçüncü paragraflar, kanuni veya standartlaştırılmış güvenceler ile sağlanan tüm uygun koruma biçimlerine uygulanır. Kanun, işbu Konvansiyon'da belirtilen ilgili veri koruma unsurlarını içermelidir. Koruma seviyesi her aktarım veya aktarım kategorisi için değerlendirilmelidir. Veri türü; verilerin aktarıldığı işlemlerin amaçları ve süresi; nihai varış ülkesi tarafından hukukun üstünlüğüne saygı duyulması; söz konusu devlette veya kuruluşta

geçerli olan genel ve sektörel yasal kurallar; ve orada uygulanan mesleki ve güvenlik kuralları gibi aktarımın çeşitli unsurları incelenmelidir.

111. Geçici veya onaylanmış standartlaştırılmış güvencelerin içeriği, veri korumasının ilgili unsurlarını içermelidir. Ayrıca sözleşmesel hükümler, örneğin, ilgili kişiye, esasa ilişkin koruma standartlarına uyumu sağlamakla yükümlü olan ve veri aktarımından sorumlu olan bir irtibat kişi sağlanmasına imkan verir şekilde düzenlenebilir. İlgili kişi, bu kişi ile veri işlemesi veya aktarımları ile ilgili olarak herhangi bir zamanda ve hiçbir ücret ödmeden iletişim kurabilir ve uygun olduğunda haklarını kullanma konusunda yardım alabilecektir.

112. Koruma seviyesinin uygun olup olmadığına ilişkin değerlendirme yapılırken spesifik aktarımla ilgili oldukları sürece Konvansiyon ilkeleri ve ilgili kişinin düzenlemelere aykırılık durumunda menfaatlerini nasıl savunabildiği göz önünde bulundurulmalı ve bu durumların alıcı devlette veya organizasyonda ne ölçüde karşılandıkları dikkate alınmalıdır. İlgili kişilerin haklarının uygulanabilirliği ve kişisel verileri aktarılan ilgili kişilere etkin idari ve adli çare sağlanması değerlendirmede dikkate alınmalıdır. Benzer şekilde, bu değerlendirme tüm devlet veya kuruluş için yapılabilen, böylece bu varış noktasına yapılacak tüm veri aktarımlarına izin verilebilecektir.

113. *Dördüncü paragraf*, Tarafların uygun bir koruma seviyesi talep etme ilkesini uygulamalarına ve böyle bir koruma sağlamayan bir alıcıya veri aktarılmasına izin vermesine imkan vermektedir. Bu istisnalara yalnızca sınırlı durumlarda izin verilmektedir: ilgili kişinin rızası veya özel çıkarları ile ve/veya mevzuatın öngördüğü ve üstün gelen meşru menfaatin olması ve/veya aktarımın ifade özgürlüğü için demokratik bir toplumda gerekli ve orantılı bir önlem teşkil ettiği durumlar. Bu tür istisnalar, gereklilik ve orantılılık ilkeleriyle uygun olmalıdır.

114. Beşinci paragraf tamamlayıcı bir koruma sağlamaktadır: yetkili gözetim otoritesine, paragraf 3(b)'de belirtilen verilerin aktarımları ve talep üzerine 4(b) ve 4(c) ile ilgili tüm bilgilerin sağlanması gerekmektedir. Otorite, bu aktarımların şartları ve gerekçeleri ile ilgili bilgi talep etmeye yetkili olmalıdır. On birinci maddenin üçüncü paragrafında yer alan şartlar dahilinde 14üncü maddenin 5inci paragrafına istisna getirilmesine izin verilmektedir.

115. Altıncı paragraf uyarınca gözetim otoritesinin, alınan önlemlerin etkinliğini veya üstün gelen meşru menfaatlerin varlığının gösterilmesini talep etmekle ve ilgili kişilerin temel hak ve özgürlüklerini korumak için gerekli olması halinde aktarımı yasaklamakla, askıya almakla veya şartlar getirmekle yetkili kılınmalıdır. On birinci maddenin üçüncü paragrafında yer alan şartlar dahilinde 14üncü maddenin 6ncı paragrafına bazı istisnalar getirilmesine izin verilmektedir.

116. Artan veri akışı ve buna ilişkin olarak kişisel verilerin korunmasının artırılması konusundaki ihtiyaç, aynı zamanda yetkili gözetim otoriteleri arasında uluslararası işbirliğinde de bir artış gerektirmektedir.

Bölüm 4 – Gözetim Otoriteleri¹⁸

Madde 15 – Gözetim Otoriteleri

¹⁸ Değişiklik Protokolünün yürürlüğe girmesinden itibaren, gözetim otoriteleri ve Verilerin Yurt dışına aktarılmasına ilişkin Ek Protokol (ETS No. 181), Sözleşmenin ayrılmaz bir parçası olarak kabul edilecektir.

117. İşbu madde, Tarafların, kişisel verilerin işlenmesiyle ilgili olarak bireylerin hak ve özgürlüklerinin korunmasına katkıda bulunan bir veya birden fazla bağımsız ve tarafsız kamu gözetim otoritesi belirlemelerini gerektirerek, bireylerin etkin korunmasını sağlamayı amaçlamaktadır. Bu otoriteler tek bir komiser veya bir üniversite organı olabilir. Veri koruma gözetim otoritelerinin uygun çareler sunabilmeleri için, etkili yetki ve işlevlere sahip olmalı ve gerçek anlamda bir bağımsızlık ile görevlerini yerine getirebilmelidir. Bu otoriteler, demokratik bir toplumda veri koruma gözetim sisteminin temel bir bileşenidir. On birinci maddenin 3üncü paragrafı uygulandığı sürece, ulusal güvenlik ve savunma amaçlı işleme faaliyetlerinin bağımsız ve etkin bir şekilde incelenmesi için diğer uygun mekanizmalar Taraflarca sağlanabilecektir.

118. *Birinci paragraf*, farklı yasal sistemlerin (örneğin federal devletlerdeki) belirli koşullarının yerine getirilmesi için birden fazla otoritenin gerekli olabileceğini netleştirmektedir. Faaliyetleri belirli bir sektörle (elektronik iletişim sektörü, sağlık sektörü, kamu sektörü vb.) sınırlı spesifik gözetim otoritelerinin de belirlenmesi mümkündür. Bu durum aynı zamanda ifade özgürlüğü hakkıyla kişisel verilerin korunması hakkının uzlaştırılması gerektiğinde gazetecilik amaçlı kişisel verilerin işlenmesi için de geçerlidir. Gözetim otoritelerinin, hızlı ve etkili hareket edebilmesi için gerekli altyapıya ve finansal, teknik ve insan kaynaklarına (avukatlar, BT uzmanları) sahip olması gerekmektedir. Kaynakların yeterliliği göz önünde bulundurulmalıdır. On birinci maddenin 4üncü paragrafı, ulusal güvenlik ve savunma amaçları için işleme faaliyetleri nezdinde gözetim otoritelerinin yetkilerinde istisnaların belirlenmesine izin vermektedir (bu istisnaların geçerli olduğu durumlarda, bu maddenin diğer paragrafları uygulanabilir veya ilgili olmayabilecektir). Ancak bu durum, inceleme ve gözetim mekanizmalarının bağımsızlığına ve etkililiğine ilişkin gereklilikleri halletmez¹⁹.

119. Taraflar, otoritelerin görevlerini yerine getirmelerine ilişkin nasıl düzenleneceğine dair belirli bir takdir yetkisine sahiptir. Bununla birlikte 11inci maddenin 3 üncü paragrafı uyarınca istisnalara tabi olma ihtimali ile birlikte otoriteler, ikinci paragrafta göre, en azından soruşturma ve müdahale yetkisi ve Konvansiyon'un hükümlerinin ihlali ile ilgili karar verme yetkisine haiz olmalıdır. Karar verme yetkisi, para cezaları dahil olmak üzere idari yaptırım uygulanmasını içerebilecektir. İlgili Tarafın yasal sisteminin idari yaptırımlara imkan vermediği durumlarda, 2nci paragraf, yaptırımın yetkili gözetim otoritesi tarafından önerilmesi ve yetkili ulusal mahkemece uygulanması şeklinde uygulanabilir. Her halükarda uygulanan yaptırımların etkili, orantılı ve caydırıcı olması gerekmektedir.

120. Otorite, 11inci maddenin 3 üncü paragrafı uyarınca istisnalara tabi olma ihtimali ile birlikte, veri sorumlusu ve veri işleyenden kişisel verilerin işlenmesi ile ilgili bilgi isteme ve bu bilgileri elde etme gibi soruşturma yetkilerine haiz olur. On beşinci madde uyarınca, bu tür bir bilginin, özellikle gözetim otoritesine guncu maddede öngörülen haklarını kullanmak isteyen bir ilgili kişi ulaştığı zaman erişilebilir kılınması gerekir. İlgili kişi bu durumda 11inci maddenin 3 üncü paragrafındaki istisnalara tabidir.

121. Gözetim otoritesinin 1inci paragrafta öngörülen müdahale yetkisi, Tarafların mevzuatında çeşitli şekillerde yer alabilir. Örneğin, otorite, resen veya ilgili kişinin bu hakları bizzat kullanamaması halinde veri sorumlusunun doğruyu yansıtmayan veya hukuka aykırı olarak işlediği verileri düzeltmesini, silmesini veya imha etmesini zorunlu kılma yetkisine sahip olabilir. Gerekli bilgileri makul bir süre içinde iletmek istemeyen veri sorumlularına karşı inceleme başlatabilme ve yaptırım uygulayabilme yetkisi de, müdahale yetkisinin

¹⁹ Dipnot 14'e bakınız.

özellikle etkili bir görünümü olacaktır. Bu yetki aynı zamanda veri işleme operasyonlarının uygulamaya alınmasından önce görüş bildirme (işlemenin ilgili kişilerin temel hak ve özgürlüklerine dikkate değer risk teşkil ettiği durumlarda, gözetim otoritesine süreçlerin tasarımının en erken aşamasından itibaren veri sorumluları tarafından danışılması gerekir), veya vakaları ilgili yetkili makamlara sevk etme imkanını içerebilir.

122. Ayrıca, 4üncü paragraf uyarınca, her ilgili kişi, gözetim otoritesinden, kişisel veri işleme konusundaki hak ve özgürlükleri ile ilgili bir talebinin soruşturulmasını isteme imkanına sahip olmalıdır. Bu durum, 9 ve 12nci maddeler uyarınca yerinde bir çözüm hakkının sağlanmasına yardımcı olmaktadır. Bu görevin yerine getirilmesi için gerekli kaynakların sağlanması gerekmektedir. Mevcut kaynaklarına göre gözetim otoritelerine ilgili kişilerin talep ve şikayetlerini ele alma önceliklerini belirleme imkanı verilmelidir.

123. Taraflar, gözetim otoritesine, herhangi bir veri koruma kuralı ihlaline ilişkin olarak, 11inci maddenin 3 üncü paragrafı uyarınca istisnalara tabi olma ihtimali ile birlikte, yasal işlemlerde bulunma ya da bu ihlali adli makamların dikkatine sunma yetkisi vermelidir. Bu yetki, bireyin korunma hakkının ihlal edildiğinin meydana çıkmasını sağlayabilecek soruşturma yürütme yetkisinden kaynaklanmaktadır. Taraflar otoritenin karar almasını sağlayarak bu yetkiyi otoriteye verme yükümlülüklerini yerine getirebilirler.

124. Bir idari kararın yasal etki yaratması durumunda, etkilenen her kişi yürürlükteki ulusal mevzuata uygun olarak etkili bir yargı yoluna başvurma hakkına sahip olmalıdır.

125. İkinci paragrafın (2) bendi, gözetim otoritelerinin farkındalık yaratma rolüyle ilgilenir. Bu bağlamda gözetim otoritesinin proaktif olarak faaliyetlerinin, işlevlerinin ve yetkilerinin görünürlüğünü sağlaması özellikle önemlidir. Bu amaçla, gözetim otoritesi kamuyu periyodik raporlar aracılığıyla bilgilendirmelidir (bkz. Paragraf 131). Ayrıca görüşlerini yayınlayabilir, veri koruma kurallarının doğru bir şekilde uygulanmasına ilişkin genel öneriler düzenleyebilir veya diğer iletişim araçlarını kullanabilir. Bunların yanı sıra, bireylere ve veri sorumlularına ve veri işleyenlere, veri koruma konusundaki hak ve yükümlülükleri hakkında bilgi sağlamalıdır. Veri koruma konularında farkındalık yaratırken otoritelerin, bu amaç için uyarlanmış yollarla çocuklara ve özel olarak korunması gereken bireylere özellikle hitap etmeleri için özenli olmaları gerekmektedir.

126. Üçüncü paragraf ile öngörüldüğü üzere, gözetim otoriteleri, uygulanabilir yerel mevzuata uygun olarak, kişisel verilerin işlenmesini düzenleyen yasal veya idari düzenlemeler hakkında görüş bildirme hakkına sahiptir. Bireysel düzenlemelerin değil, yalnızca genel düzenlemelerin bu görüş bildirme yetkisi çerçevesinde olması amaçlanmaktadır.

127. Üçüncü paragrafta öngörülen bu görüş bildirmeye ek olarak, örneğin davranış kuralları veya teknik normlar gibi kişisel veri işleme ile ilgili diğer düzenlemeler hazırlanırken de otoriteden görüş bildirmesi istenebilecektir.

128. On beşinci madde, başka yetkilerin gözetim otoritelerine tahsis edilmesini engellemektedir.

129. Beşinci paragraf, gözetim otoritelerinin işlevlerini tam bir bağımsızlık ile kullanmadıkları sürece, temel hak ve özgürlükleri etkili bir şekilde koruyamayacaklarını açıklamaktadır. Otoritenin oluşumu da dahil olmak üzere bir dizi unsur, gözetim otoritesinin işlevlerini yerine getirmedeki bağımsızlığını korumaya katkıda bulunur. Bu unsurlar şu

şekildedir: üyelerini atama yöntemi; işlevlerinin süresi ve bırakma koşulları; uygun olmayan kısıtlamalara tabi olmaksızın ilgili toplantılara katılma imkânı; teknik veya diğer uzmanlara danışması veya dışarıdan danışmanlık alması; otoriteye yeterli kaynak bulunması; kendi personelini işe alma imkânı veya ister doğrudan ister dolaylı olsun dış müdahaleye maruz kalmadan karar alması.

130. Talimat alma ya da kabul etme yasağı, gözetim otoritesi olarak görevlerin yerine getirilmesi hallerini kapsamaktadır. Bu durum, gözetim otoritelerinin kendi bağımsız takdirlerini kullandıkları sürece gerekli gördükleri hallerde uzmanlaşmış tavsiyeler talep etmelerini engellemez.

131. Yedinci paragraf ile gözetim otoritelerinin çalışmalarında ve faaliyetlerinde şeffaflığı gözetmeleri, örneğin, diğerlerinin yanı sıra, uygulamaya yönelik faaliyetleriyle ilgili bilgileri içeren yıllık faaliyet raporlarını yayınlamaları gerektiği düzenlenmiştir.

132. Bu bağımsızlığa hanel getirmemekle birlikte, 9uncu paragrafta öngörüldüğü üzere, gözetim otoritelerin kararlarına mahkemeler nezdinde hukuk devleti ilkesine uygun olarak itiraz edilmesi mümkün olmalıdır.

133. Ayrıca, gözetim otoritelerinin yargıya taşıma ve icrasını isteme hususunda yasal kapasiteye sahip olmaları gerekir, ancak bir gözetim otoritesinin müdahale etmesi (ya da etmemesi), durumdan etkilenen bir kimsenin yargı yoluna başvurmasını engellememelidir (bkz. Paragraf 124).

134. On beşinci maddenin 10uncu paragrafı, gözetim otoritelerinin, adli kapasiteleri içerisinde hareket ederken bağımsız kuruluşlar tarafından yürütülen işleme faaliyetleriyle ilgili olarak yetkili olamayacağını belirtmektedir. Gözetim yetkilerindeki bu muafiyet kesinlikle ulusal mevzuata uygun olarak, gerçek anlamda adli faaliyetlerle sınırlı kalmalıdır.

Bölüm 5 – İş Birliği ve Karşılıklı Yardımlaşma

Madde 16 – Gözetim Otoritelerinin Belirlenmesi

135. Bölüm 5 (Madde 16-21), çeşitli otoriteleri aracılığıyla, Konvansiyon uyarınca uygulanan veri koruma mevzuatını yürürlüğe koyan Taraflar arasında, işbirliği ve karşılıklı yardım konusunda bir dizi hüküm içermektedir. Bu hükümler, 20nci maddede belirtilen durumlar dışında emredicidir. On altıncı madde uyarınca Taraflar, bir veya daha fazla yetkili otorite belirleyecek ve iletişim bilgilerini ve eğer varsa maddi ve bölgesel yetkilerini Avrupa Konseyi Genel Sekreteri'ne iletceklerdir. Bunu takip eden maddeler, işbirliği ve karşılıklı yardım için ayrıntılı bir çerçeve sağlamaktadır.

136. Taraflar arasındaki işbirliği genellikle 15inci madde uyarınca kurulan gözetim otoriteleri tarafından gerçekleştirilirken, bir Tarafın 16ncı maddenin hükümlerini uygulamak üzere başka bir otorite tayin etmesi yasaklanmamaktadır.

137. İşbirliği ve genel yardım bir olay öncesi kontrolleri için olduğu kadar olay sonrası kontrolleri (örneğin, belirli bir veri denetleyicisinin faaliyetlerini doğrulamak için) için de söz konusu olmaktadır. Paylaşılan bilgiler mevzuata veya vakaya ilişkin nitelikte olabilir.

Madde 17 – İş Birliği Biçimleri

138. On yedinci madde uyarınca, 15inci maddede düzenlenen gözetim otoriteleri, görevlerini yerine getirmeleri ve yetkilerini kullanabilmeleri için gerekli olduğu derecede birbirleriyle işbirliği yaparlar. On yedinci maddenin gözetim otoritelerinin işbirliğini “görevlerinin yerine getirilmesi ve yetkilerin kullanılması” için gerekli olanla sınırlaması ve gözetim otoritesinin işbirliği yapabilmesinin ancak yetkileri ile sınırlı olması dikkate alındığında işbu düzenleme, bir Tarafın 1inci maddenin 3üncü paragrafı kullanarak 15inci maddenin 2nci paragrafının (a) ve (b) bentleri uyarınca gözetim otoritesinin yetkilerini sınırlandırdığı hallerde uygulanmayacaktır.

139. İşbirliği çeşitli biçimlerde olabilir; veri koruma yasalarının karşılıklı yardım yoluyla uygulanması gibi bazı “ağır” biçimlerde olabileceği gibi, farkındalık yaratma, eğitim, personel değişimi gibi bazı “hafif” biçimlerde de olabilir.

140. Muhtemel işbirliği faaliyetleri listesi sınırlı sayıda değildir. İlk olarak, gözetim otoriteleri, özellikle ilgili ve faydalı bilgileri paylaşarak birbirlerine karşılıklı yardım sağlayacaktır. Bu bilgi iki katmanlı olabilir: kişisel veriler dahil olmak üzere gizli bilgilerin yanı sıra “veri korumaya ilişkin mevzuatı ve idari uygulamaları hakkında bilgi ve belgeler” (normalde herhangi bir sorun gündeme getirmeyen bu bilgiler serbestçe değiştirilebilir ve kamuya açıklanabilir).

141. Kişisel veriler söz konusu olduğunda, bu veriler ancak işbirliği için gerekiyorsa, yani değişim olmadığı durumda işbirliği etkisiz hale gelecekse veya ilgili kişi bu hususta “açık, özel, serbest ve aydınlatılmış rıza” verdiyse değiştirilebilir. Her durumda, kişisel verilerin aktarımı Konvansiyon’un özellikle 2nci Bölüm düzenlemeleri (ayrıca reddetme ile ilgili olan 20öncü maddeye bakılması gerekir) olmak üzere hükümlerine uymak zorundadır.

142. İlgili ve faydalı bilgilerin sağlanmasının yanı sıra, işbirliğinin hedefleri arasında ortak eylemler ile birlikte koordineli araştırmaların veya müdahalelerin gerçekleştirilmesi de bulunmaktadır. Uygulanabilir prosedürler için gözetim otoriteleri, idari, medeni veya ceza usul kanunları veya kendi yetki alanlarının bağlı olduğu devletler üstü veya uluslararası taahhütler gibi uygulanabilir yerel mevzuata atıfta bulunacaktır.

143. Üçüncü paragraf gözetim otoritelerinin ağını düzenlemektedir. Bu ağ, işbirliği sürecinin yüksek bir seviyeye çıkarılması, dolayısıyla kişisel verilerin korunmasının etkinliğine katkıda bulunulması için bir araç niteliğindedir. Konvansiyon’un “ağ” kavramını tekil bir biçimde ifade ettiğine dikkat etmek gerekir. Bu hüküm, Tarafların gözetim otoritelerinin diğer ilgili ağlara katılımını engellememektedir.

Madde 18 – İlgili Kişilere Yardım

144. Birinci paragraf, Konvansiyon’a Taraf devlette veya üçüncü bir ülkede bulunan ilgili kişilerin, ikamet ettikleri yer ya da uyruğu ne olursa olsun, 9uncu maddede tanınan haklarını kullanabilmelerini sağlamaktadır.

145. İkinci paragraf uyarınca ilgili kişinin Konvansiyon Tarafı olan başka bir ülkede ikamet ettiği durumda, haklarını ya doğrudan ilgili verilerin işlendiği ülkede ya da görevlendirilmiş gözetim otoritesi aracılığı ile ileri sürebilir.

146. Ayrıca, yurtdışında ikamet eden ilgili kişiler de kendi ülkelerindeki diplomatik veya konsolosluk temsilcilerinin yardımlarıyla haklarını kullanma fırsatına sahip olabilirler.

147. Üçüncü paraf, prosedürü hızlandırmak için taleplerin mümkün olduğunca spesifik olması gerektiğini belirtmektedir.

Madde 19 – Güvenceler

148. Bu madde, gözetim otoritelerine, diğer Tarafların gözetim otoritelerine ve yurt dışında yaşayan ilgili kişilere karşı aynı gizlilik yükümlülüğünü yerine getirme borcu yüklemektedir.

149. İlgili kişi adına bir gözetim otoritesinden yardım, ancak bu ilgili kişinin bir talebine cevap olarak sağlanabilmektedir. Otorite ilgili kişiden bir talep almış olmalı ve ilgili kişi adına bağımsız olarak hareket etmemelidir. Bu hüküm, karşılıklı yardımın dayanağı olan karşılıklı güven için temel bir öneme sahiptir.

Madde 20 – Taleplerin Reddi

150. Bu madde, Tarafların işbirliği ve karşılıklı yardım taleplerine uyma zorunluluğunu belirtir. Uymayı reddetme gerekçeleri tüketici bir şekilde sıralanmıştır.

151. (c) bendinde kullanılan “uyum” terimi geniş yorumlanmalı ve yalnızca talebin cevabını değil, aynı zamanda talepten önceki durumu de kapsayacak şekilde anlaşılmalıdır. Örneğin; bilgi talep edilen otorite, talep edilen bilgilerin sadece bir bireyin haklarına ve temel özgürlüklerine zararlı olabileceği ihtimalinde değil aynı zamanda, bilginin talep edilmesinin kendisinin de ilgili kişinin temel hak ve özgürlüklerini zarar verebileceğini göz önünde bulundurarak talebi reddedebilir. Bunun yanı sıra otorite, ulusal mevzuat hükümleri uyarınca diğer kamu düzeni çıkarlarının korunması için ayrıca yükümlülük altında olabilmektedir (kolluk soruşturmasının gizliliğin sağlanması için gibi). Bu şekilde, bir gözetim otoritesi, bir talebe cevaben bazı bilgi veya belgeleri eksik bırakmak zorunda kalabilmektedir.

Madde 21 – Giderler ve Prosedürler

152. Bu maddenin hükümleri diğer uluslararası belgelerde bulunan hükümlerle benzer niteliktedir.

153. Bu maddenin üçüncü paragrafı, Taraflar arasında kullanılacak prosedür, formatlar ve dilin kararlaştırılmasını sağlar. Bu paragrafın metni herhangi bir resmi prosedür gerektirmemekle birlikte belirli durumlara özgü olabilecek idari düzenlemelere izin vermektedir. Ayrıca, Tarafların bu tür düzenlemeleri gerçekleştirme yetkisini gözetim otoritelerine bırakmaları tavsiye edilmektedir. İşbirliği ve yardım biçimleri de olaya göre değişkenlik gösterebilmektedir. Özel nitelikli tıbbi bilgiye erişim talebiyle bir nüfus sayımı kaydındaki girişlerle ilgili rutin soruların farklı gereksinimlere sahip olacağı açıktır.

Bölüm 6 – Konvansiyon Komitesi

Madde 22 – Komitenin Oluşumu

154. 22, 23 ve 24üncü maddelerin amacı, Konvansiyon’un etkili bir şekilde uygulanmasını kolaylaştırmak ve gerektiğinde kusursuzlaştırmaktır. Konvansiyon Komitesi, Konvansiyon’a uygun olarak uygulanan veri koruma yasalarını yürürlüğe koyan Tarafların bir başka işbirliği aracı niteliğindedir.

155. Konvansiyon Komitesi, tüm Tarafların ulusal denetleme makamlarından veya hükümetten gelen temsilcilerinden oluşmaktadır.

156. Konvansiyon Komitesi'nin niteliği ve takip edilen olası prosedür, Avrupa Konseyi çerçevesinde yapılan diğer sözleşmelerin hükümleri uyarınca oluşturulmuş olanlar ile benzerlik gösterebilir.

157. Konvansiyon sürekli gelişen bir konuyu ele aldığından, Konvansiyon'un pratikte uygulaması (23üncü maddenin (a) bendi) ve anlamıyla (23üncü maddenin (d) bendi) ilgili soruların ortaya çıkması beklenebilecektir.

158. Konvansiyon Komitesi Usul Kuralları, Tarafların oy kullanma hakkı ve bu hakkın kullanım şekillerine ilişkin hükümler içerir ve değişiklik yapan Protokol'e eklenmiştir.

159. Usul Kurallarında yapılacak herhangi bir değişiklik, Konvansiyon'un 25inci maddesinin uygulandığı oy hakkı ve ilgili usuller üzerindeki değişikliklerin haricinde, üçte iki çoğunluğa tabidir.

160. Katılım üzerine AB, Konvansiyon kapsamında kişisel verilerin korunmasına ilişkin olarak AB ile üye ülkeleri arasındaki yetki dağılımını açıklayan bir açıklama yapacaktır. Daha sonra AB, Genel Sekreter'e, yetkilerin dağılımındaki önemli değişiklikler hakkında bilgi verecektir.

161. 25inci maddeye göre Konvansiyon Komitesi, Konvansiyon'da değişiklik önerme ve bir Taraf veya Bakanlar Komitesi tarafından formüle edilmiş değişiklik önerilerini inceleme hakkına sahiptir (23üncü maddenin (b) ve (c) bentleri).

162. Konvansiyon tarafından belirlenen veri koruma ilkelerinin uygulanmasını garanti altına almak için Konvansiyon Komitesi'nin; bir aday tarafından katılım için sağlanan veri koruma seviyesinin değerlendirmesini hazırlarken (23üncü maddenin (e) bendi) ya da Taraflarca Konvansiyon'un uygulanmasını periyodik olarak gözden geçirirken (23üncü maddenin (h) bendi) Konvansiyon'a uygunluğun değerlendirilmesinde kilit bir rolü olacaktır. Konvansiyon Komitesi ayrıca, talep edilir ise, bir devlet veya uluslararası organizasyonun veri koruma düzeninin Konvansiyon'a uygunluğunu değerlendirme yetkisine sahip olacaktır (23üncü maddenin (f) bendi).

163. Sözleşme ile uyum düzeyine dair bu tür görüşlerin sağlanmasında Konvansiyon Komitesi, Usul Kurallarında belirtilen adil, şeffaf ve halka açık bir prosedür temelinde çalışacaktır.

164. Ayrıca, Konvansiyon Komitesi veri aktarımı için standart güvenlik modellerini onaylayabilir (23üncü maddenin (g) bendi).

165. Son olarak, Konvansiyon Komitesi Taraflar arasında ortaya çıkan sorunları ve zorlukları çözmeye yardımcı olabilecektir (23üncü maddenin (i) bendi). Anlaşmazlıkların söz konusu olduğu durumlarda, Konvansiyon Komitesi müzakere veya başka dostane yollarla bir çözüm arayacaktır.

Bölüm 7 – Değişiklikler

Madde 25 – Değişiklikler

166. Bu Konvansiyon'un orijinal metnini kabul eden Bakanlar Komitesi, değişiklikleri onaylama konusunda da yetkilidir.

167. Birinci paragraf uyarınca değişiklik girişimi, Bakanlar Komitesi'nin kendisi, Konvansiyon Komitesi veya bir Taraf (Avrupa Konseyi'ne üye olan/olmayan bir taraf olabilir) tarafından başlatılabilmektedir.

168. Konvansiyon Komitesi'nden kaynaklanmayan herhangi bir değişiklik önerisi, üçüncü paragraf uyarınca Konvansiyon Komitesi'ne görüşü için sunulmalıdır.

169. Kural olarak herhangi bir değişiklik, bütün Tarafların Avrupa Konseyi Genel Sekreteri'ne kabullerini bildirdikleri tarihten otuz gün sonra yürürlüğe girecektir. Ancak, Bakanlar Komitesi, bazı durumlarda, Konvansiyon Komitesi'ne danıştıktan sonra, bir Tarafın Genel Sekreter'e itirazını bildirmediği sürece, bu değişikliklerin üç yıllık bir süre zarfının ardından yürürlüğe girmesine karar verebilir. Bu prosedürün amacı, bütün Tarafların rızası ilkesini korurken, küçük ve teknik değişikliklere uygulanması amaçlanan değişikliklerin yürürlüğe girmesini hızlandırmaktır.

Bölüm 8 – Son Hükümler

Madde 26 – Yürürlüğe Giriş

170. Geniş bir coğrafi kapsam esas alındığından 2nci paragraf Konvansiyon'un yürürlüğe girmesi için Avrupa Konseyi üyesi beş devletin Konvansiyon'u onaylaması gerektiğini belirtmektedir.

171. Sözleşme, Avrupa Birliği tarafından imzaya açılmıştır²⁰.

Madde 27 – Üye Olmayan Devletlerin veya Uluslararası Organizasyonların Katılımı

172. İlk başta OECD ve bazı Avrupa devleti olmayan ülkelerle yakın işbirliği içinde geliştirilen Konvansiyon, hükümleri uyarınca dünyadaki herhangi bir devlete de açıktır. Konvansiyon Komitesi'ne, bu uyumu değerlendirme ve Bakanlar Komitesi için adayın veri koruma düzeyine ilişkin bir görüş hazırlama görevi verilmiştir.

173. Veri akışlarının sınırlanmayan niteliği göz önüne alındığında, ülkelerin ve dünyanın her yerinden uluslararası organizasyonların katılımı aranmaktadır. Konvansiyon'u kabul edebilecek uluslararası organizasyonlar, sadece uluslararası kamu hukuku kurallarına göre yönetilen kuruluşlar olarak tanımlananlardan oluşmaktadır.

Madde 28 – Ülkesel Hükümler

174. Konvansiyon'un Tarafların yetkisi altındaki veya bir Tarafın taahhüt edebileceği deniz aşırı bölgelere uygulanması, deniz aşırı ülkelerin veri işleme operasyonlarında maliyet ve iş gücü veya alternatif gece ve gündüz veri işleme imkanının kullanılabilmesi nedenleriyle kullanıldığı dikkate alındığında, pratik önem taşımaktadır.

²⁰ 15 Haziran 1999 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından onaylanan Konvansiyon'daki değişiklikler, Protokolün yürürlüğe girmesinden itibaren amaçlarını yitirmektedir.

Madde 29 – Çekinceler

175. Bu Konvansiyon’da yer alan kurallar, etkili veri koruması için en temel ve gerekli unsurları oluşturmaktadır. Bu sebeple Konvansiyon, hükümleri için hiçbir çekinceye izin verilmemektedir; dahası belirli maddelerde izin verilen istisnalar ve kısıtlamalar dikkate alındığında Konvansiyon’un makul derecede esnek olduğu sonucuna ulaşmak mümkündür.

Madde 30 – Fesih

176. Konvansiyon’un herhangi bir tarafı herhangi bir zamanda Konvansiyon’u feshedebilir.

Madde 31 – Bildirimler

177. Bu hükümler, Avrupa Konseyi’nin diğer sözleşmelerinde yer alan nihai hükümlerle uyum içerisindedir.