

Bu evrak sadece belge niteliđi taşımakta olup evrađın içeriđi hakkında kurumların herhangi bir sorumluluđu yoktur.

- ▶ **B Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayı ve 24 Ekim 1995 tarihli**

AVRUPA BİRLİĐİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ

(23.11.1995 tarih ve L 281 sayılı Avrupa Birliđi Resmi Gazetesi, sayfa.31)

Tadil Eden yönetmelik:

	Resmi Gazete		
	No	sayfa	tarih
▶ <u>MI</u> 29 Eylül 2003 tarihli Konsey ve Avrupa Parlamentosunun 1882/2003 sayılı yönetmeliđi	L284	1	31.10.2003(AT)

► **B Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayı ve 24 Ekim 1995 tarihli**

AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ

AVRUPA PARLAMENTOSU VE AVRUPA BİRLİĞİ KONSEYİ,

Avrupa Topluluğunu Kuran Anlaşmayı ve özellikle ilgili 100a maddesini göz önünde bulundurarak,

Komisyonun teklifini¹ göz önünde bulundurarak,

Ekonomik ve Sosyal Komite'nin² görüşünü göz önünde bulundurarak,

Anlaşmanın 189b maddesinde ortaya koyulan prosedür uyarınca hareket ederek³ aşağıda sıralanan nedenlerden dolayı:

- (1) Topluluk'un amaçları, Avrupa Birliği Anlaşması tarafından tadil edildiği, Anlaşmada öngörüldüğü şekilde; İnsan Hakları ve Temel Özgürlüklerin Korunması Hakkındaki Avrupa Sözleşmesi'nde ve Üye Devletler'in anayasaları ve yasalarında tanınan temel haklar üzerinden demokrasiyi geliştirerek ve barış ve özgürlüğü koruyup güçlendirerek halklarının yaşama koşullarının sürekli iyileştirilmesini teşvik ederek, Avrupa'yı bölen engelleri gidermek için ortak eylemle ekonomik ve sosyal ilerlemeyi sağlayarak, Topluluk'a mensup Devletlerarasında daha yakın ilişkileri teşvik etmeyi içerir;
- (2) Veri işleme sistemleri insana hizmet etmek üzere tasarlanır ve böyle olmalıdır; gerçek kişilerin milliyetine veya ikametgahlarına bakmaksızın, başta kişisel mahremiyet olmak üzere, temel haklarını ve özgürlüklerini korumalıdır ve bireylerin ekonomik ve sosyal ilerlemesine, refahına ve ticari genişlemeye katkıda bulunmalıdır;
- (3) Malların, kişilerin, servislerin ve sermayenin serbest dolaşımının sağlanması hakkındaki Anlaşmanın 7a maddesi uyarınca bir iç pazarın kurulması ve işletilmesi;

¹ OJ No: C 277, 5.11.1990 syf:3 ve OJ No: C 311, 27.11.1992, syf:3

² OJ No: C 159, 17.6.1991, syf:38

³ 15 Haziran 1995 tarihli Avrupa Parlamentosu Kararı (OJ No: C 166, 3.7.1995) ve 20 Şubat 1995 tarihli Komisyon ortak görüşü (OJ No: C 93, 13.4.1995, syf:1) ; 2 Eylül 1993'de onaylanan (OJ No: C 342, 20.12.1993, syf:30) 11 Mart 1992 tarihli Avrupa Parlamentosu Görüşü (OJ No: C 94, 13.4.1992, syf:198)

yalnızca kişisel verilerin bir Üye Devletten diğere serbestçe akabilmesini değil, aynı zamanda bireylerin temel haklarının güvenceye alınmasını gerektirir;

- (4) Topluluk'a, ekonomik ve sosyal faaliyetin çeşitli alanlarında kişisel verilerin işlenmesine dönük olarak artan sıklıkta başvuru yapılmaktadır; bilgi teknolojisinde sağlanan ilerlemeler, bu tür verilerin işlenmesini ve değişimini önemli ölçüde kolaylaştırmaktadır;
- (5) Anlaşmanın 7a maddesinin anlamı kapsamında iç pazarın kurulması ve işlemeden kaynaklanan ekonomik ve sosyal entegrasyon; Üye Devletlerde ekonomik ve sosyal faaliyete özel veya kamu sıfatıyla katılan herkes arasında kişisel verilerin sınır ötesi akışında zorunlu olarak önemli bir artışa yol açacaktır. Farklı Üye Devletlerdeki teşebbüsler arasında kişisel verilerin alışverişi artmaya başlamıştır; çeşitli Üye Devletlerdeki ulusal makamlardan, iç pazarın sınırları dikkate almaksızın diğere bir Üye Devletteki bir makam adına görevlerini yerine getirebilmek veya görevlerini yapabilmek hususunda topluluk hukukuna binaen, kişisel verileri takas etmesi ve iş birliği yapması istenmektedir;
- (6) Üstelik Toplulukta yeni haberleşme ağlarının eşgüdümlü uygulanması ve bilimsel ve teknik işbirliğindeki artış, kişisel verilerin sınır ötesi akışını gerektirmekte ve kolaylaştırmaktadır;
- (7) Üye Devletlerde uygulanan kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere bireylerin hakları ve özgürlüklerinin korunma seviyesindeki farklılıklar, bir Üye Devlet toprağından diğere Üye Devlete bu tür verilerin iletilmesini engelleyebilir; bu nedenle bu fark, Topluluk seviyesindeki birtakım ekonomik faaliyetlerin takibi için bir engel oluşturabilir, rekabeti bozabilir ve Topluluk hukuku kapsamında makamların sorumluluklarını yerine getirmesini engelleyebilir; koruma seviyesindeki bu fark, çok çeşitli ulusal kanunlar, yönetmelikler ve idari hükümlerin varlığından dolayıdır;
- (8) Kişisel verilerin akışındaki engelleri kaldırmak için, bireylerin hak ve özgürlüklerinin korunma seviyesi bu tür verilerin işlenmesine ilişkin olarak tüm Üye Devletlerde eşit olmalıdır; bu amaç iç pazar için hayattır ancak özellikle Anlaşmanın 7a maddesinde belirtilen iç pazar amacına uyan tutarlı bir şekilde kişisel verilerin sınır ötesi akışının düzenlenmesini temin etmek hususunda Üye Devletlerdeki ilgili kanunlar arasında mevcut uyumsuzlukların ölçüğü göz önüne alındığında bu, Üye Devletler tarafından tek başına başarılamaz; bu yüzden bu kanunları yaklaştırmak için Topluluk eylemine gerek duyulmaktadır;
- (9) Ulusal kanunların yakınlştırılmasından kaynaklanan eşdeğer koruma dikkate alındığında, Üye Devletler, özellikle kişisel gizlilik hakkı başta olmak üzere, bireylerin özgürlükleri ve haklarının korunması gerekçesiyle, kişisel verilerin aralarında serbest dolaşımını artık engelleyemeyeceklerdir; Üye Devletlere, Direktifin uygulanması bağlamında, iş ve sosyal ortaklar tarafından da yerine getirilebilecek bir manevra alanı bırakılacaktır; bu nedenle Üye Devletler veri işleminin yasallığını yöneten genel koşulları, kendi ulusal yasalarına koyabileceklerdir. Üye Devletler bu şekilde kendi mevzuatlarıyla güncel olarak sağlanan korumayı geliştirmeye çalışacaklardır; bu

manevra alanının limitleri dâhilinde ve Topluluk kanuna uygun olarak, Direktifin uygulanmasında eşitsizlikler ortaya çıkabilir ve bu, Topluluğun yanı sıra bir Üye Devlet bünyesinde verilerin dolaşımı etkileyebilir;

- (10) Kişisel verilerin işlenmesi hakkındaki ulusal kanunların amacı, başta kişisel mahremiyet hakkı olmak üzere, hem Topluluk kanununun genel esaslarında, hem de İnsan Hakları ve Temel Özgürlüklerini Koruma hakkındaki Avrupa Sözleşmesinin 8. maddesinde tanınan temel hakları ve özgürlükleri korumaktır; bu nedenle, bu kanunların yakınlaştırılması, sağladıkları korumanın azalmasına yol açmamalı aksine, Topluluk içinde yüksek seviyeli bir korumanın sağlanması için çabalamalıdır;
- (11) Kişisel mahremiyet başta olmak üzere bireylerin haklarının ve özgürlüklerinin korunması hakkında bu Direktifte belirtilen esaslar, Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Hakkındaki 28 Ocak 1981 tarihli Avrupa Konseyi Sözleşmesinde belirtilenleri güçlendirir ve genişletir;
- (12) Koruma esasları, faaliyetleri Topluluk hukukunca yönetilen herhangi bir kişinin kişisel verilerinin tüm işlenmesine uygulanmalıdır; adres kayıtlarını tutma ve yazışma gibi özellikle şahsi veya ailevi olan aktiviteler esnasında, bir gerçek kişinin gerçekleştirdiği veri işleme, hariç tutulmalıdır;
- (13) Avrupa Topluluğunu Kuran Anlaşmanın 100a maddesi veya madde 56 (2), madde 57 kapsamında Üye Devletler üzerine düşen yükümlülükler saklı kalmak üzere; kamu güvenliği, savunma, devlet güvenliğine dair Avrupa Birliği Anlaşmasının V ve VI. Başlığında atıfta bulunulan faaliyetler ile ceza kanunları alanındaki Devlet faaliyetleri; Topluluk hukuku kapsamında değildir; Devletin güvenlik konularıyla ilişkili olduğunda, devletin ekonomik refahını güvenceye almak için gerekli olan kişisel verilerin işlenmesi, bu Direktifin kapsamında değildir;
- (14) Gerçek kişilere ilişkin ses ve görüntü verilerini yakalamak, iletmek, değiştirmek, kaydetmek, saklamak veya nakletmek için kullanılan teknolojilerin, bilgi toplumu çerçevesinde devam eden gelişmelerinin önemi dikkate alındığında, bu Direktif bu tür verileri gerektiren işlemeye uygulanmalıdır;
- (15) Bu tür verilerin işlenmesi; söz konusu kişisel verilere kolay erişime izin vermek için, yalnızca otomatik olursa veya işlenen veriler, bireylere ilişkin özel kriterlere göre yapılandırılan bir dosyalama sistemi içine alınırsa veya alınması planlanırsa, bu Direktif kapsamındadır;
- (16) Video gözetim durumlarındaki gibi, ses ve görüntü verilerinin işlenmesi; ceza hukuku alanına ilişkin Devlet faaliyetleri esnasında veya ulusal güvenlik, savunma kamu güvenliği amacıyla veya Topluluk hukuku kapsamına girmeyen diğer faaliyetler için yürütülürse bu Direktif kapsamına girmez;
- (17) Başta görsel işitsel alan olmak üzere, ilgili edebi ve sanatsal ifade amaçlarının yanı sıra gazetecilik amaçları için ses ve görüntü verilerinin işlenmesinde; Direktifin esasları, madde 9'da öngörülen hükümlere göre, sınırlı bir şekilde uygulanacaktır;
- (18) Bireylerin, bu Direktif kapsamında sağlanan korumadan yoksun kalmamalarını sağlamak için, Topluluktaki herhangi bir kişisel veri işlenmesi, Üye Devletler'den birinin

kanununa uygun olarak yerine getirilmelidir; bu bağlamda, bir Üye Devlette yerleşik bir denetleyicinin sorumluluğu altında yapılan işlem, o Devletin kanununca yönetilmelidir;

- (19) Bir Üye Devletin sınırları içindeki kuruluş, istikrarlı düzenlemeler aracılığıyla faaliyetin etkin ve reel olarak gerçekleştirilmesini sağlar. İster bir tüzel kişiliğin şubesi veya bağlı kuruluşu olsun bu tür kuruluşun yasal biçimi; bu bakımdan belirleyici bir faktör değildir; özellikle bağlı kuruluşlar aracılığıyla çeşitli Üye Devletlerin topraklarında tek bir denetleyici kuruluş kurulursa, ulusal kuralların boşluklarından yararlanmayı önlemek için, denetleyici kuruluşların her birinin, faaliyetlerine uygulanan ulusal kanunun emrettiği yükümlülükleri yerine getirmesi sağlanmalıdır;
- (20) Verilerin işlenmesinin üçüncü bir ülkede kurulan bir tüzel kişilik tarafından yapılması, bu Direktifte sağlanan bireylerin korunma biçimine engel olmamalıdır; bu durumlarda, işleme, kullanılan yöntemlerin bulunduğu Üye Devlet kanununca yönetilmelidir ve bu Direktifte sağlanan hakların, uygulamada gözetilmesini sağlayacak garantiler olmalıdır;
- (21) Bu Direktif, ülkesellik ilkeleri saklı kalmak üzere ceza konularına uygulanır;
- (22) Üye Devletler, işlemenin yasallığına dair genel koşulları, çıkardıkları yasalarda veya bu Direktif kapsamındaki tedbirleri yürürlüğe koyduklarında, daha hassas olarak tanımlayacaklardır; madde 7 ve 8 ile bağlantılı olarak özellikle madde 5, genel kurallardan bağımsız olarak Üye Devletlere, madde 8'in kapsadığı çeşitli veri kategorileri için ve belirli sektörler için, özel işleme koşulları koymaya izin verir.
- (23) Üye Devletler, hem kişisel verilerin işlenmesi hususunda bireylerin korunması hakkındaki genel kanunlar, hem de örneğin istatistik enstitülerine ilişkin olanlar gibi sektörel kanunlar yoluyla bireylerin korunmasını uygulamayı temin etmek üzere yetkilendirilmişlerdir;
- (24) Kendilerini ilgilendiren verileri işlemeye dair tüzel kişilerin korunmasına ilişkin mevzuat, bu Direktiften etkilenmez;
- (25) Korumanın esasları; bir taraftan, başta işlemenin yürütülebileceği koşullar ve denetleme makamına bildirim, teknik güvenlik ve veri kalitesi olmak üzere işlemeden sorumlu diğer kuruluşlar veya kişiler, kamu makamları, işletmeler, temsilciler üzerine yüklenen yükümlülüklerle ve diğer taraftan, bireylere verilen haklara, işlemenin konusu olan verilere, işlemenin yapıldığını bildirme, verileri danışmaya, düzeltme talep etmeye ve hatta bazı koşullarda işlemeye itiraza yansıtılmalıdır;
- (26) Koruma esasları, tespit edilmiş veya tespit edilebilir bir kişiye ilişkin herhangi bir bilgiye uygulanmalıdır; bir kişinin tespit edilebilir olup olmadığını belirlemek için, adı geçen şahsı tespit etmek için herhangi bir diğer kişi tarafından veya denetleyici tarafından kullanılacak makul tüm araçlar dikkate alınmalıdır; koruma esasları, veri öznesinin artık tespit edilebilir olmadığı bir biçimde anonimleşmiş verilere uygulanmayacaktır; madde 27'nin anlamı dahilindeki davranış kuralları, verilerin anonimleşebilmesine ve veri öznesinin tespitinin artık mümkün olmadığı bir biçimde alıkonma biçimlerine dair rehberlik sağlamak için yararlı bir araç olabilir;

- (27) Bireylerin korunması, manuel işlemenin yanı sıra verilerin otomatik işlenmesinde de uygulanmalıdır; bu korumanın kapsamı kullanılan tekniklere bağlı olarak geçerli olmamalıdır, aksi takdirde, bu ciddi bir kanun boşluklarından yararlanma riski yaratacaktır; yine de manuel işlemeye dair bu Direktif yapılandırılmamış dosyaları değil yalnızca dosyalama sistemlerini kapsar, özellikle bir dosyalama sisteminin içeriği, kişisel verilere kolay erişime olanak veren bireylere ilişkin özel kriterlere göre yapılandırılmalıdır; madde 2 (c)deki tanım doğrultusunda, kişisel verilerin yapılandırılmış bir dizisinin bileşenlerini belirlemek için farklı kriterler ve bu tür bir veri dizisine erişimi yöneten farklı kriterler, her bir Üye Devlet tarafından belirlenebilir; özel kriterlere göre yapılandırılmamış kapak sayfalarının yanı sıra dosyalar veya dosya dizileri, hiçbir koşul altında bu Direktifin kapsamına girmeyecektir;
- (28) Kişisel verilerin işlenmesi, ilgili bireyler için yasal ve adil olmalıdır; özellikle veriler uygun, ilgili olmalıdır ve işlendikleri amacı aşmamalıdır; bu tür amaçlar açık ve meşru olmalı ve verilerin toplanma zamanında belirlenmelidir; toplama sonrasındaki işleme amaçları, başlangıçta belirtilen amaçlarla uyumsuz olmamalıdır;
- (29) Tarihsel, istatistiksel veya bilimsel amaçlarla kişisel verilerin ayrıca işlenmesi, Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla önceden toplanmış verilerin amaçlarıyla uyumsuz olarak kabul edilmez, bu korunma önlemleri özellikle, herhangi bir özel bireye dair tedbirlerin veya kararların desteklenmesinde verilerin kullanımına imkan vermemelidir;
- (30) Kişisel verilerin işlenmesi, ayrıca veri öznesinin haklarının ve özgürlüklerinin çiğnenmemesi koşuluyla, yasal olması amacıyla, veri öznesinin rızasıyla yürütülmelidir veya veri öznesi hakkında bağlayıcı bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için veya gerçek veya tüzel bir kişinin meşru menfaati için veya resmi otoritenin uygulanması için veya kamu menfaatine yürütülen bir görevin yerine getirilmesi için gerekli olmalıdır; özellikle etkin rekabeti garanti ederken, ilgili menfaatler arasında bir denge sağlamak için, Üye Devletler, şirketlerin veya diğer kuruluşların olağan meşru iş faaliyetleri bağlamında kişisel verilerin kullanılabilme veya üçüncü bir şahsa açıklanma koşullarını belirleyebilirler; benzer şekilde Üye Devletler, örneğin nedenlerini belirtmeksizin ve bedelsiz olarak, hakkındaki verilerin işlenmesine itiraz etmek için bir veri öznesine izin veren hükümlere tabi olan ister siyasi yapıdaki herhangi diğer bir dernek veya vakıf veya yardım kuruluşu tarafından isterse ticari olarak yürütülen pazarlama amaçları için, kişisel verilerin üçüncü bir şahsa açıklanabilme koşullarını belirtebilirler;
- (31) Veri öznesinin yaşamı için asıl olan bir menfaati korumak için yapıldığında kişisel verilerin işlenmesi, aynı derecede yasal kabul edilmelidir;
- (32) Kamu menfaatinde veya resmi otoritenin uygulamasında yürütülen bir görevi yerine getiren denetleyicinin, bir kamu idaresi veya kamu hukuku veya bir meslek örgütü gibi özel bir kanun tarafından yönetilen başka bir tüzel veya gerçek kişi mi olacağını belirlemek ulusal mevzuata kalmaktadır;
- (33) Veri öznesi açık şekilde rıza göstermezse, temel özgürlükleri veya kişisel mahremiyeti ihlal eden yapıdaki veriler işlenmemelidir; ancak, temel özgürlüklerin yerine

getirilmesine izin verecek amaçlar için, bazı derneklerin veya vakıfların meşru faaliyetleri esnasında veya mesleki gizlilik hakkındaki yasal bir yükümlülüğe tabi kişiler tarafından bu verilerin sağlık amaçları için kullanılması durumunda; bu yasaklamaya uymama durumu açıkça belirtilmelidir;

- (34) Sağlık sigortası sistemindeki hizmetler ve yardımlar için talepleri belirtmede kullanılan prosedürlerin kalitesini ve maliyet etkinliğini temin etmek başta olmak üzere - kamu menfaati için önemli nedenlerle gerekçelendirildiğinde, önemli kamu menfaati gerekçesine dayanması durumunda; bilimsel araştırma ve hükümet istatistikleri halk sağlığı ve sosyal koruma gibi alanlarda, Üye Devletlerin verilerin hassas kategorilerini işleme yasağına uymamasına da izin verilmelidir; ancak bireylerin kişisel gizlilik ve temel haklarını korumak hususunda özel ve uygun korunma önlemlerini sağlamak, Üye Devletlerin ödevidir;
- (35) Ayrıca, resmi olarak tanınan dini derneklerle ilgili veya uluslararası kamu hukuku veya anayasa hukukunda öngörülen amaçları başarmak için resmi makamlar tarafından kişisel verilerin işlenmesi, kamu menfaatinin önemli gerekçeleri üzerine yürütülür;
- (36) Belirli Üye Devletlerde, seçim faaliyetleri esnasında demokratik sistemin işlemesi, siyasi partilerin halkın siyasi görüşü hakkındaki verileri derlemesini gerektirir, uygun korunma önlemlerinin sağlanması koşuluyla bu tür verilerin işlenmesine önemli kamu menfaati nedeniyle izin verilebilir;
- (37) Başta görsel işitsel alan olmak üzere, sanatsal ifade, edebi amaçları için veya gazetecilik amaçları için kişisel verilerin işlenmesi; özellikle, İnsan Hakları ve Temel Özgürlüklerinin Korunması hakkındaki Avrupa Sözleşmesinin 10. maddesinde garanti edildiği gibi, özellikle bilgi alma ve verme hakkı ve bilgilendirme hakkıyla bireylerin temel haklarını uzlaştırmanın gerekli olması durumunda, bu Direktifin bazı hükümlerinin koşullarından muaf tutulmaya yetki vermelidir. Bu yüzden üye Devletler, denetleme makamının yetkisi ve üçüncü ülkelere verilerin aktarılması hakkındaki tedbirlere, veri işlemenin yasallığı hakkındaki genel tedbirlere dair temel haklar arasında denge sağlama amacı için gerekli muafiyetleri ve derogasyonları belirtmelidir;
- (38) Verilerin işlenmesinin adil olması için, veri öznesi, işleme faaliyetinin varlığını öğrenecek konumda olmalıdır ve veriler ondan toplandığında, toplama koşullarını dikkate alan doğru ve tam bilgi verilmelidir;
- (39) Bazı verilerin işlenmesi, denetleyicinin veri öznesinden doğrudan toplamadığı verileri gerektirir, ayrıca, veri öznesinden veriler toplandığı esnada, ifşa beklenmese bile, veriler üçüncü bir şahsa yasal olarak ifşa edilebilir; tüm bu durumlarda, veri öznesi, veriler kaydedildiğinde veya en geç veriler ilk kez bir üçüncü şahsa ifşa edildiğinde, bilgilendirilmelidir;
- (40) Ancak, veri öznesinin önceden bilgili olması durumunda, bu yükümlülüğü uygulamak gereksizdir; ayrıca, açıklama veya kaydetme açık şekilde yasayla sağlanırsa veya veri öznesine bilgi sağlamanın imkansızlığı kanıtlanırsa veya işlemenin tarihsel, istatistiki veya bilimsel amaçlar için olması halinde gerekebilecek aşırı çabayı gerektirmesi

halinde bu tür bir yükümlülük olmayacaktır; bu bakımdan, veri öznelerinin sayısı, verilerin yaşı ve kabul edilen herhangi dengeleyici tedbirler dikkate alınmalıdır;

- (41) Her kişi, özellikle işlemenin yasallığını ve verilerin doğruluğunu onaylamak için işlenmekte olan ona ait verilere erişim hakkını kullanabilmelidir; aynı nedenlerle, her veri öznesi en azından madde 15 (1)de atıfta bulunulan otomatik kararlar durumunda, ona ilişkin verilerin otomatik işlenmesiyle ilgili mantığı bilme hakkına sahip olmalıdır; bu hak, başta yazılımı koruyan telif hakkını ve ticari sırları veya fikri mülkiyeti ters şekilde etkilememelidir; ancak bu düşünceler, veri öznesinin bilgilendirilmemesine yol açmamalıdır;
- (42) Üye Devletler, veri öznesinin menfaati için veya diğerlerinin hak ve özgürlüklerini korumak için bilgiye erişim hakkını sınırlandırabilirler; örneğin, tıbbi verilere erişimin yalnızca bir sağlık uzmanı tarafından elde edilebileceğini belirtebilirler;
- (43) Benzer şekilde denetleyicinin bazı yükümlülükleri ve bilgilendirme ve erişim hakları üzerindeki sınırlandırmalar; örneğin, düzenlenen mesleklerdeki etik ihlallerine dair kriminal soruşturmalar, takibatlar ve davaların yanı sıra bir Üye Devlet veya Birliğin ulusal güvenlik, savunma, kamu güvenliği veya önemli ekonomik veya mali menfaatlerini güvence altına almanın gerektirdiği ölçüde Üye Devletler tarafından uygulanabilir; istisnalar ve sınırlamaların listesi, kamu güvenliği, ekonomik veya mali menfaatler ve suç önlemeye ilişkin en son söz edilen üç alanda gerekli yönetmelik veya izleme, denetim görevlerini içermelidir; bu üç alandaki görevlerin listelenmesi, Devlet güvenlik veya savunma nedenleri için sınırlamaları veya istisnaların meşruiyetini etkilemez;
- (44) Üye Devletler, Topluluk hukuku gerekçesiyle, yukarıda atıfta bulunulan amaçların bazısını güvenceye almak için, verilerin kalitesi ve bireyleri bilgilendirme yükümlülüğü, erişim hakkına ilişkin bu Direktifin hükümlerine uymayabilir;
- (45) Verilerin, gerçek veya tüzel bir kişinin meşru menfaatleri veya resmi otorite, kamu menfaati gerekçesiyle yasal olarak işlenebileceği durumlarda, herhangi bir veri öznesine, yine de kendisine ait herhangi bir verinin işlenmesine itiraz etmek için özel durumuna ilişkin meşru ve mecburi gerekçelerle izin verilmelidir; bununla birlikte Üye Devletler bunun aksine ulusal hüküm koyabilirler;
- (46) Kişisel verilerin işlenmesine dair veri öznelerinin haklarının ve özgürlüklerinin korunması, hem, güvenliği sağlamak ve bu suretle herhangi bir yetkisiz işlemeyi önlemek için işlemenin kendi zamanında hem de işleme sisteminin tasarımı zamanında uygun teknik ve kurumsal tedbirlerin alınmasını gerektirir; bu tedbirlere denetleyicilerin uymasını sağlamak Üye Devletlerin ödevidir, bu tedbirler, korunacak verilerin yapısı ve işlemenin yapısındaki risklere ilişkin uygulamanın maliyetlerini ve durumunu dikkate alarak uygun güvenlik seviyesini sağlamalıdır;
- (47) Tek amacı verilerin iletilmesi olan, kişisel verileri içeren bir mesajın bir iletişim aracıyla veya elektronik posta servisiyle iletilmesi durumunda, mesajda belirtilen kişisel verilere dair denetleyici; iletim servislerini sunan kişi yerine, mesajın çıktığı kişi olarak kabul edilecektir; bununla birlikte bu tür servisleri sunanlar, normal olarak, servisin

çalışması için gerekli ek kişisel verilerin işlenmesi bakımından denetleyici olarak kabul edilecektir;

- (48) Denetleme makamını bilgilendirmeye dönük prosedürler, faaliyetin, bu Direktif kapsamında alınan ulusal tedbirlere uygun olduğunu doğrulama amacı için, herhangi bir işleme faaliyetinin amaçlarının ve ana özelliklerinin açıklanmasını sağlamak üzere tasarlanmıştır;
- (49) Uygun olmayan idari formalitelerden kaçınmak için, gerekli bildirim yükümlülüğünden muafiyetler; sınırlarını belirten bir Üye Devlet tarafından alınan bir tedbire uyumlu olması koşuluyla, işlemenin, veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkilemesinin mümkün olmadığı durumlarda, Üye Devlet tarafından koyulabilir; benzer şekilde muafiyet veya basitleştirme, denetleyici tarafından atanan bir kişinin yürütülen işlemenin veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkilemesinin olanaksız olmasını sağladığında, Üye Devletler tarafından koyulabilir; ister denetleyicinin bir çalışanı olsun veya olmasın bu tür bir veri koruma görevlisi tam bağımsızlık içinde işlevlerini yerine getirecek bir konumda olmalıdır;
- (50) Muafiyet veya basitleştirme, meşru bir menfaati kanıtlayan bir kişi veya kamu tarafından danışmaya açma ve kamuya bilgi sağlamak için ulusal yasaya göre tek amacı kayıt tutma olan işleme faaliyetleri için öngörülebilir;
- (51) Yine de bildirim yükümlülüğünden muafiyet veya basitleştirme denetleyiciyi bu Direktiften kaynaklanan diğer yükümlülüklerinin herhangi birisinden kurtarmayacaktır;
- (52) Bu bağlamda, genel olarak yetkili makamlar tarafından *olaydan sonra* doğrulama yeterli bir tedbir olarak kabul edilmelidir;
- (53) Ancak bazı işleme faaliyetlerinin, yeni teknolojilerin özel kullanımından dolayı veya bir sözleşme, hak, faydadan bireyleri kapsam dışı tutanlar gibi kendi amaçlarının kapsamı nedeniyle veri öznelerinin hak ve özgürlüklerine özel riskler yaratması olasıdır; Üye Devletler isterlerse mevzuatlarında bu tür riskleri belirtebilirler;
- (54) Toplulukta yapılan tüm işlemeye ilişkin olarak; özel riskleri ortaya çıkaran miktar çok sınırlı olmalıdır; Üye Devletler denetleme makamı veya makamla işbirliği içindeki veri koruma görevlisinin, işlenmesinden önce kontrolün yapılmasını sağlamalıdır; bu ön kontrolün ardından, ulusal yasasına göre denetleme makamı, işlemeye dair bir görüş veya bir izin verebilir; bu tür kontrol; ya ulusal parlamentonun bir tedbirin ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bir yasal tedbirin hazırlanmasıyla eş zamanlı olabilir;
- (55) Denetleyici veri öznelerinin haklarını gözetmezse, ulusal mevzuat bir yargı yolu sağlamalıdır; yasadışı işlemenin bir sonucu olarak bir kişinin maruz kalabileceği herhangi bir zarar; mücbir sebepler durumunda ya da hatanın veri öznesinin tarafında olduğunu saptadığı durumlarda; zarardan sorumlu olmadığını kanıtlarsa yükümlülükten muaf tutulacak olan denetleyici tarafından tazmin edilmelidir; yaptırımlar, bu Direktif kapsamında alınan ulusal tedbirlere uymayanın kamu veya özel hukuk tarafından yönetilen herhangi bir kişi olduğuna bakılmaksızın uygulanmalıdır;

- (56) Kişisel verilerin sınır ötesi dolaşımı, uluslararası ticaretin genişletilmesi için gereklidir, Bu Direktifle Topluluk bünyesinde garanti edilen bireylerin korunması; yeterli koruma seviyesini sağlayan üçüncü ülkelere kişisel verilerin aktarılmasını önlememelidir; üçüncü bir ülke tarafından sağlanan koruma seviyesinin yeterliliği, transfer işlemleri veya transfer işlemini çevreleyen tüm koşulların ışığında değerlendirilmelidir;
- (57) Diğer taraftan yeterli ve elverişli koruma seviyesini sağlamayan üçüncü bir ülkeye, kişisel verilerin transferi yasaklanmalıdır;
- (58) Transferin, yasayla belirlenen bir kayıttan ve meşru menfaate sahip kamu veya kişiler tarafından danışma için yapıldığı veya örneğin, sosyal güvenlik konularında yetkili servisler arasında veya gümrük veya vergi idareleri arasında verilerin uluslararası transferi durumunda, önemli kamu menfaati korumasının bunu gerektirdiği bir sözleşme veya yasal hak talebine ilişkin transferin gerektiği, veri öznesinin rızasını verdiği bazı durumlarda bu yasaktan muafiyet için önlemler alınmalıdır; bu tür bir transferin kayıttaki mevcut tüm veri kategorilerini veya verilerin tümünü gerektirmediği durumlarda ve kayıt, meşru bir menfaate sahip kişiler tarafından danışılma içinse, transfer yalnızca bu kişilerin talebi üzerine veya bunlar alıcı olacaklarsa yapılmalıdır;
- (59) Denetleyicinin, uygun korunma önlemleri sunduğu durumlarda, üçüncü bir ülkede koruma olmayışını tazmin etmek için özel önlemler alınmalıdır; ayrıca Topluluk ve bu tür üçüncü ülkeler arasındaki müzakere prosedürleri için önlem alınmalıdır;
- (60) Herhangi bir durumda, üçüncü ülkelere transferler, bu Direktif ve özellikle ilgili 8. maddesi uyarınca, yalnızca Üye Devletler tarafından kabul edilen hükümlere tam uygun şekilde gerçekleştirilebilir;
- (61) Üye Devletler ve Komisyon, kendi ilgili yetki alanları içinde, uygulanması için benimsenen ulusal hükümleri gözeterek ve bazı sektörlerde yerine getirilen işlemin özel karakteristiklerini göz önüne alarak, bu Direktifin uygulanmasını kolaylaştırmak hususunda, davranış kurallarını düzenlemeleri için ticari birlikleri ve ilgili diğer temsilci kuruluşları teşvik etmelidir;
- (62) Denetim makamına ilişkin Üye Devletlerdeki tam bağımsız olarak işlevlerini yerine getiren kuruluşlar; kişisel verilerin işlenmesine dair bireylerin korunmasında, zorunlu bir bileşendir;
- (63) Bu tür makamlar, özellikle yasal takibata kalkışma yetkisi ve bireylerden şikayet durumlarında inceleme ve müdahale yetkileri dahil olmak üzere kendi görevlerini yerine getirmek için gerekli araçlara sahip olmalıdır; bu tür makamlar, kendi yetki alanlarındaki Üye Devletlerde; işlemin şeffaflığını sağlamak için yardımcı olmalıdırlar;
- (64) Farklı Üye Devletlerdeki makamlar, Avrupa Birliği çapında, koruma kurallarının uygun şekilde gözetilmesini sağlamak için kendi görevlerini yerine getirmede birbirlerini desteklemeye ihtiyaç duyacaklardır;
- (65) Topluluk düzeyinde, kişisel verilerin işlenmesine dair Bireylerin Korunması hakkında bir Çalışma Grubu kurulmalıdır ve işlevlerini yerine getirmede tamamen bağımsız

olmalıdır; özel yapılarını dikkate alarak, Komisyona tavsiyelerde bulunmalıdır ve özellikle bu Direktif uyarınca kabul edilen ulusal kuralların homojen uygulanmasına katkı sağlamalıdır;

- (66) Bu direktif, üçüncü ülkelere verilerin transferine ilişkin olarak, 87/373/EEC⁴ sayılı Konsey kararında belirtilen şekilde bir prosedürün tesisini ve Komisyon üzerindeki uygulama yetkilerinin verilmesini gerektirir⁵;
- (67) AT Anlaşmasının madde 189 b'sinde öngörülen prosedüre uygun olarak kabul edilen eylemler için tedbirleri uygulamaya dair, Avrupa Parlamentosu, Konsey ve Komisyon arasında geçici bir anlaşma üzerine mutabakata 20 Aralık 1994 tarihinde erişilmiştir;
- (68) Bu Direktifte düzenlenen kişisel verilerin işlenmesine dair, kişisel mahremiyet hakkı başta olmak üzere; bireylerin hak ve özgürlüklerinin korunmasına dair prensiplere; özellikle, bu prensiplere dayalı özel kurallarla ilgili belirli sektörlere göre, ilave yapılabilir veya daha açık şekilde anlatılabilir;
- (69) Üye Devletlere, önceden devam eden tüm işleme faaliyetlerine, yeni ulusal kuralları kademeli şekilde uygulamak için, bu Direktifin yerini alan ulusal tedbirlerin uygulamaya girdiği yıldan itibaren üç yılı geçemeyen bir süre verilmelidir; maliyet etkin uygulanmasını kolaylaştırmak için, Direktif hükümlerinin bazılarıyla mevcut manuel dosyalama sistemlerinin uyumunu sağlamak üzere, bu Direktifin kabul edilme tarihinden 12 yıl sonra biten başka bir süre Üye Devletlere verilecektir; bu tür dosyalama sistemlerinde bulunan veriler bu genişletilmiş geçiş dönemi esnasında manuel olarak işlenir. Bu sistemler, bu işleme sırasındaki hükümlerle uyumlu hale getirilmelidir;
- (70) Bu hükümlerin yürürlüğe girmesinden önce bildirilen rıza ve ücrete dayalı sonuçlandırılan bir sözleşmenin yerine getirilmesinde gerekli herhangi bir hassas veri için, bu Direktif uyarınca alınan ulusal hükümler yürürlüğe girdikten sonra, veri öznesinin sürece devam etmesi için denetleyiciye yine izin vermesine gerek yoktur;
- (71) Bu tür düzenleme, kişisel verilerin işlenmesine dair bireylerin korunmasını ilgilendirmedeğinde, Bu Direktif, ülkede oturan tüketicilere yönelik pazarlama faaliyetlerini düzenleyen bir üye Devlet yönteminin yerini almaz;
- (72) Bu Direktif, bu Direktifte düzenlenen prensipler uygulandığında, dikkate alınması gereken resmi belgelere kamu erişim esaslarına olanak sağlar;

BU DİREKTİFİ KABUL ETMİŞTİR:

⁵ OJ No: L 97, 18.7.1987, syf:33

BÖLÜM I
GENEL HÜKÜMLER

Madde 1

Direktifin Amacı

1. Bu Direktife uygun olarak, Üye Devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır;
2. Üye Devletler 1. paragraf kapsamında sağlanan korumayla bağlantılı nedenler için Üye Devletler arasında kişisel verilerin akışını yasaklamayacak ya da engellemeyeceklerdir;

Madde 2

Tanımlar

Bu Direktifin amacı için:

- (a) “kişisel veri” fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (“veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir;
- (b) “kişisel verilerin işlenmesi (işleme)”, silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletlemeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisini kastedecektir;
- (c) “kişisel veri dosyalama sistemi (dosyalama sistemi)” ister merkezi ister merkezi olmayan ya da bir işlevsel veya coğrafi tabana dağıtılmış özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisini kastedecektir;
- (d) “denetleyici”, kişisel verilerin işleme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; işleme amaçları ve araçları ulusal veya Topluluk hukuku veya yönetmelikleriyle belirlendiğinde, denetleyici veya atanması için özel kriterler, ulusal veya topluluk hukukuyla belirlenebilir;
- (e) “işleyici”, denetleyici adına kişisel verileri işleyen bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya diğer bir kuruluşu kastedecektir;
- (f) “üçüncü şahıs”, veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici, veri öznesi dışındaki herhangi bir gerçek

veya tüzel kişi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir;

- (g) “alıcı”, ister bir üçüncü şahıs olsun ya da olmasın, verilerin açıklandığı bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; ancak, özel bir soruşturma çerçevesinde verileri alan makamlar alıcı olarak kabul edilmeyecektir;
- (h) “veri öznesinin rızası”, kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rızayı kastedecektir.

Madde 3

Kapsam

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

Madde 4

Uygulanacak ulusal kanun

1. Her bir Üye Devlet, aşağıdaki durumlarda, kişisel verilerin işlenmesi için bu Direktif uyarınca kabul ettikleri ulusal hükümleri uygulayacaklardır:
 - (a) İşleme, Üye Devletin topraklarındaki denetleyici kuruluşunun faaliyetleri bağlamında yapıldığında; aynı denetleyici, çeşitli Üye Devletlerin toprağında yerleşikse, bu kuruluşların her birinin, uygulanan ulusal mevzuatlarda öngörülen yükümlülüklerle uymasını temin edecek gerekli tedbirleri almalıdır;
 - (b) denetleyici Üye Devletin topraklarında yerleşik olmayıp, uluslararası kamu hukukuna göre ulusal hukukun uygulandığı bir yerde bulunuyorsa;
 - (c) denetleyici Topluluk topraklarında yerleşik değilse ve işleme amaçları için, kişisel veriler, bahse konu Üye devlet topraklarında konumlanan otomatik cihazları kullanırsa, bu tür cihazlar yalnızca Topluluk toprağı boyunca iletme amacı için kullanılmadıkça;
2. 1 (c) paragrafında atıfta bulunulan koşullarda, denetleyici, denetleyicinin kendisine

karşı başlatılabilecek davalara zarar vermeksizin o Üye Devlet toprağında yerleşik bir temsilci atamalıdır.

BÖLÜM II

KİŞİSEL VERİLERİN İŞLENMESİNİN YASALLIĞI HAKKINDAKİ GENEL KURALLAR

Madde 5

Üye Devletler, bu bölüm hükümlerinin sınırları kapsamında, kişisel verileri işlemenin yasal olduğu koşulları daha hassas şekilde belirleyeceklerdir.

I.KISIM

VERİ KALİTESİNE İLİŞKİN PRENSİPLER

Madde 6

1. Üye Devletler, kişisel verilerin aşağıdaki şekilde olmasını sağlayacaklardır:

- (a) adil ve yasal olarak işlenmiş;
- (b) belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlarla uyumsuz biçimde başkaca işlenmemiş. Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla; tarihsel, istatistiksel veya bilimsel amaçlar için verilerin detaylı işlenmesi; uyumsuz olarak kabul edilmeyecektir;
- (c) toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşmaz;
- (d) doğrudur ve gerektiği yerde güncel tutulur. Toplanma ve sonrasındaki işleme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemler alınmalıdır;
- (e) verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulur. Üye Devletler, tarihsel, istatistiksel veya bilimsel kullanım amacıyla daha uzun süreli depolanan kişisel veriler için uygun koruma önlemleri alacaktır.

2. 1. paragrafa uyulmasını sağlamak, denetleyicinin sorumluluğundadır. olacaktır.

II.KISIM

VERİ İŞLEMİYİ YASALLAŞTIRMA KRİTERLERİ

Madde 7

Üye Devletler, kişisel verilerin işlenebilmesini yalnızca aşağıdaki koşullar sağlanırsa sağlayacaklardır:

- (a) Veri öznesi açık, kesin ve net bir biçimde rızasını vermişse veya

- (b) İşleme, bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekliyse veya
- (c) İşleme denetleyicinin konusu olan bir yasal yükümlülüğe uyum için gerekirse, veya
- (d) İşleme, veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya
- (e) İşleme, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekliyse; veya
- (f) İşleme, bu tür menfaatlerin, madde 1 (1) kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çığnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekliyse;

III.KISIM

ÖZEL İŞLEME KATEGORİLERİ

Madde 8

Verilerin özel işleme kategorileri

1. Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır.

2.1. paragraf aşağıdaki durumlarda uygulanmayacaktır:

- (a) veri öznesinin rızasını vermesiyle 1. paragrafta atıfta bulunulan yasağın kaldırılmayacağını Üye Devlet kanunlarının belirtmesi haricinde, bu verilerin işlenmesinde veri öznesi açık rızasını vermişse; veya
 - (b) işlemenin, yeterli korunma önlemleri için sağlanan ulusal kanunla yetkilendirildiği kadarıyla, istihdam kanunu alanında, denetleyicinin yükümlülüklerini ve özel haklarını yerine getirme amacı için gerekli olduğunda; veya
 - (c) işleme, veri öznesinin rızasını vermesinin fiziksel veya yasal olarak elverişsiz olduğu durumda, diğer bir kişinin veya veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya
 - (d) işleme; veri öznelerinin rızası olmaksızın verilerin üçüncü şahıslara açıklanmadığı ve işlemenin yalnızca amaçlarıyla bağlantılı olarak düzenli iletişimde oldukları kişileri veya kuruluş mensuplarını ilgilendirmesi koşuluyla bir vakıf, dernek veya siyasi, felsefi, dini veya ticaret birliği amaçlı başka bir kar amacı gütmeyen kuruluş tarafından uygun teminatlı meşru faaliyetler esnasında yapılırsa, veya
 - (e) işleme, veri öznesi tarafından açıkça halka duyurulan verilere ilişkinse ya da kanuni hakların tesisi, yerine getirilmesi veya savunulması için gerekliyse.
2. Paragraf 1, sağlık hizmetlerinin yönetimi veya bakım veya tedavinin sağlanması,

tıbbi teşhis, önleyici tıp amaçları için veri işlemenin gerektiği yerde ve mesleki gizlilik yükümlülüğü için ulusal yetkili kuruluşlar tarafından veya eşdeğer gizlilik yükümlülüğüne tabi diğer bir kişi tarafından saptanan ulusal kanun kapsamında bir sağlık uzman öznesi tarafından bu verilerin işlendiği yerde uygulanmayacaktır.

3. uygun korunma önlemlerinin sağlanmasına tabi olarak, Üye Devletler, önemli kamu menfaati nedenleri için, ya ulusal yasa ya da denetleme makamının kararıyla paragraf 2'de belirtilenlere ek olarak muafiyetler koyabilir.

4. suçlar, adli hükümler veya güvenlik tedbirlerine ilişkin verilerin işlenmesi, yalnızca resmi makamın kontrolü altında yapılabilir veya ulusal yasa kapsamında uygun özel korunma önlemleri sağlanırsa, uygun özel korunma önlemleri sağlayan ulusal hükümler kapsamında Üye Devlet tarafından verilebilecek tadillere tabi olabilir. Ancak, adli hükümlerin tam bir kaydı yalnızca resmi makamın kontrolü altında tutulabilir.

Üye Devletler, hukuk davalarındaki kararlar veya idari müeyyidelere ilişkin verilerin de resmi makamın kontrolü altında işlenmesini sağlayabilirler.

6. 4 ve 5. paragraflar için 1. paragraftan tadiller komisyona haber verilecektir.

7. Üye Devletler, ulusal bir tespit numarası veya genel başvurunun diğer belirtecinin işlenebileceği koşulları belirleyecektir.

Madde 9

İfade özgürlüğü ve kişisel verilerin işlenmesi

Üye Devletler, kişisel verilerin ifade özgürlüğünü yöneten kurallarla kişisel gizlilik hakkını uzlaştırmak için gerekirse, yalnızca, edebi veya sanatsal açıklama amacı veya gazetecilik amaçları için kişisel verilerin işlenmesinde Kısım IV ve Kısım VI, bu Bölümün hükümlerinden muafiyetler veya derogasyonlar sağlayacaktır.

IV.KISIM

VERİ ÖZNESİNE VERİLECEK BİLGİLER

Madde 10

Veri öznesinden verilerin toplanma durumlarında bilgilendirme

Üye Devletler, önceden mevcut olması haricinde, kendine dair bilgilerin toplandığı bir veri öznesine, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri vermesini sağlamalıdır:

(a) Denetleyici ve varsa temsilcisinin kimliği;

(b) Kastedilen veri işleme amaçları;

(c) Aşağıdakiler gibi herhangi bir başka bilgi;

— verilerin alıcıları veya alıcı kategorileri,

— yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı,

- (özneyle) ilgili verileri düzeltme hakkının ve verilere erişim hakkının olması,
(denetleyici veya temsilcisi) bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilişkin adil işlemeyi garanti etmelidirler.

Madde 11

Verilerin veri öznesinden elde edilmediğinde bilgilendirme

1. Veriler veri öznesinden elde edilmediğinde, Üye Devletler, (veri öznesinin bu bilgilere) önceden sahip olması hariç, kişisel verilerin kaydının yapılması esnasında ya da üçüncü bir şahsa ifşa öngörüldüğünde, verilerin ilk ifşa zamanından önce, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri veri öznesine vermesini sağlayacaktır:

- (a) Denetleyicinin ve varsa temsilcisinin kimliği;
- (b) İşleminin amaçları;
- (c) Aşağıdakiler gibi herhangi bir başka bilgi;
 - verilerin alıcıları veya alıcı kategorileri,
 - yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı,
 - (özneyle) ilgili verileri düzeltme hakkı ve verilere (kendisinin) erişim hakkının olması,

(denetleyici veya temsilcisi) bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilişkin adil işlemeyi garanti etmelidirler.

2. Kayıt veya ifşa açıkça yasayla belirtilirse ya da aşırı bir çaba gerektirecek ya da imkansızlığı kanıtlanan verilerin sağlanması için, tarihsel veya bilimsel araştırma amaçları için veya istatistiksel amaçlar için işleme durumunda; Paragraf 1 uygulanmayacaktır. Bu durumlarda, Üye Devletler uygun korunma önlemleri sağlayacaktır.

V.KISIM

VERİ ÖZNELERİNİN VERİLERE ERİŞME HAKKI

Madde 12

Erişim hakkı

Üye Devletler, her veri öznesinin denetleyiciden (aşağıdakileri) temin etme hakkını garanti edecektir:

- (a) aşırı gecikme veya masraf olmaksızın ve makul aralıklarla, sınırlama olmaksızın:
 - kendisine dair verilerin işlenip işlenmeyeceği hususunda onay ve en azından, verilerin açıklandığı alıcı kategorileri veya alıcıları ve ilgili verilerin kategorileri, işleme amaçları hususunda bilgi,

- kaynakları hususunda herhangi bir mevcut bilginin ve işleme tabi tutulan verilerin anlaşılır biçimde ona iletilmesi,
- en azından madde 15 (1)'de atıfta bulunulan otomatik kararlar durumunda, kendisine ilişkin verilerin otomatik işlenmesiyle ilgili mantık bilgisi;
- (b) Özellikle verinin eksik veya yanlış yapısı yüzünden, bu Direktifin hükümlerine uymayan işlemede, verilerin engellenmesi veya silinmesi, uygun olarak düzeltilmesi;
- (c) Bunun imkansız olduğu gösterilmezse veya orantısız çabayı gerektirmezse, (b) bendine uygun olarak yapılan herhangi bir düzeltme, silme veya engelleme hakkında, verilerin açıklandığı üçüncü şahıslara bildirim.

VI.KISIM

MUAFİYETLER VE SINIRLAMALAR

Madde 13

Muafiyetler ve sınırlamalar

1. Bu tür bir sınırlama, aşağıdakileri sağlamak için gerekli tedbirleri oluşturduğunda, Üye Devletler, 6 (1), 10, 11 (1), 12 ve 21 maddelerinde belirtilen hak ve yükümlülüklerin kapsamını sınırlandıracak yasal tedbirleri kabul edebilirler:

- (a) ulusal güvenlik;
- (b) savunma;
- (c) kamu güvenliği;
- (d) düzenlenmiş meslekler için etik ihlallerinin veya ceza gerektiren suçların önlenmesi, incelenmesi, tespiti ve kovuşturulması;
- (e) parasal, bütçe ve vergilendirme konuları dahil olmak üzere, Avrupa Birliği'nin veya bir Üye Devletin önemli bir ekonomik veya mali menfaati;
- (f) c), (d) ve (e)'de atıfta bulunulan durumlarda, resmi makamın yürütmesiyle ara sıra da olsa bağlantılı düzenleyici fonksiyon veya izleme, denetim;
- (g) diğerlerinin hak ve özgürlüklerinin veya veri öznesinin korunması.

2. Üye Devletler, yeterli yasal korunma önlemlerine tabi olarak özellikle veriler herhangi özel bir bireye dair kararlar veya tedbirler almak için kullanılmadığında, veri öznesinin gizlilik hakkını ihlal riski açıkça yoksa, veriler yalnızca bilimsel araştırma amacı için işlendiğinde veya yalnızca istatistik yaratma amacı için gerekli dönemi aşmayan bir süre için kişisel formda tutulduğunda, madde 12'de belirtilen hakları bir yasama tedbiriyle sınırlandırabilir.

VII.KISIM

VERİ ÖZNESİNİN İTİRAZ HAKKI*Madde 14***Veri öznesinin itiraz hakkı**

Üye Devletler aşağıdaki hakları veri öznesine vereceklerdir:

- (a) En azından madde 7 (e) ve (f)'de atıfta bulunulan durumlarda, ulusal mevzuat tarafından aksinin belirtilmesi haricinde, kendisine dair verilerin işlenmesinde, özel durumuna ilişkin zorlayıcı kanuni gerekçelere her zaman itiraz etmek. Gerekçeli bir itiraz olduğunda, denetleyici tarafından başlatılan işleme, artık bu verileri kapsamayabilir;
- (b) Denetleyicinin doğrudan pazarlama amaçları için işlenmesini öngördüğü, kendine ait kişisel verilerin işlenmesine ücretsiz ve istek üzerine itiraz etme (hakkı) veya kişisel veriler üçüncü şahıslara ilk kez ifşa edilmeden veya doğrudan pazarlama amaçları için üçüncü şahıslar adına kullanılmadan önce bilgilendirilme (hakkı) ve bu tür ifşalara veya kullanımlara ücretsiz itiraz hakkının açık şekilde sunulması;

Üye Devletler, (b)'nin ilk alt paragrafında atıfta bulunulan hakkın varlığından veri öznelerinin haberdar olmasını temin etmek için gerekli tedbirleri alacaklardır.

*Madde 15***Otomatik bireysel kararlar**

1. Üye Devletler, her kişiye, işte performans, kredibilite, güvenilirlik, tutum v.b gibi kendisine ilişkin bazı kişisel yönleri değerlendirmek için yalnızca verilerin otomatik işlenmesine dayalı ve onu önemli derecede etkileyen veya ona ilişkin yasal etkiler üreten bir karara tabi kalmama hakkı verecektir.
2. Bu Direktifin diğer maddelerine tabi olarak Üye Devletler şayet karar aşağıdaki şekilde alındı veya yetki veriyorsa, 1. paragrafta atıfta bulunulan türde bir karara bir kişinin tabi olabilmesini sağlayacaklardır:
 - (a) kendi görüşünü belirtmesine izin veren düzenlemeler gibi meşru menfaatlerini güvenceye alacak uygun tedbirler olduğunda ya da veri öznesi tarafından sunulan sözleşmenin yapılması veya yerine getirilme talebinin karşılanması koşuluyla bir sözleşmenin yapılması veya yerine getirilmesi esnasında alınır veya;
 - (b) öznenin meşru menfaatlerini güvenceye alacak tedbirleri de belirten bir yasa tarafından yetkilendirilirse.

VIII.KISIM

İŞLEMENİN GİZLİLİĞİ VE GÜVENLİĞİ*Madde 16***İşlemenin gizliliği**

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

*Madde 17***İşlemenin güvenliği**

1. Üye Devletler, özellikle işlemenin bir ağ üzerinde verilerin iletilmesini gerektirdiğinde ve işlemenin tüm diğer yasa dışı biçimlerine karşı, yetkisiz açıklama veya erişim, değiştirme, kazara kayıp veya kazara veya yasa dışı tahribe karşı kişisel verileri korumak için gereken uygun teknik ve kurumsal tedbirleri, denetleyicinin uygulamasını sağlayacaklardır.

Bu tür tedbirler, uygulamalarının durum ve maliyetini dikkate alarak, korunacak verinin yapısına ve işleme tarafından sunulan risklere uygun seviyede güvenlik sağlayacaktır.

2. Üye Devletler, işleme kendi adına yürütüldüğünde, denetleyicinin yürütülecek işlemeyi yöneten teknik güvenlik tedbirlerine ve kurumsal tedbirlere dair yeterli garantiler sağlayan bir işleyiciyi seçmesini ve bu tedbirlerle uyum sağlamasını temin edecektir.

3. İşleyici vasıtasıyla işlemenin yapılması özellikle aşağıdakileri şart koşan ve işleyiciyi denetleyiciye bağlayan yasal belge veya bir sözleşme ile yönetilmelidir:

- işleyici yalnızca denetleyiciden gelen talimatlara göre hareket edecektir.
- işleyicinin yerleşik olduğu Üye Devlet kanunuyla tanımlandığı şekilde, 1. paragrafta düzenlenen yükümlülükler işleyicinin de ödevi olacaktır.

4. Paragraf 1’de atıfta bulunulan tedbirlere dair koşullara ve veri korunmasına ilişkin yasal belge veya sözleşmenin parçaları, kanıtı tutma amaçları için yazılı veya eşdeğer diğer bir biçimde olacaktır.

IX.KISIM

BİLDİRİM*Madde 18***Denetleme makamına bildirimde bulunma yükümlülüğü**

1. Üye Devletler, kısmen veya tamamen otomatik işleme faaliyeti veya tek amaç veya ilgili çeşitli amaçlara hizmet etmesi istenen bu tür bir dizi faaliyeti yürütmeden önce denetleyici ve varsa temsilcisinin, madde 28’de atıfta bulunulan denetleme

makamına bildirimde bulunmasını sağlayacaklardır.

2. Üye Devletler, yalnızca aşağıdaki durumlarda ve aşağıdaki koşullarda bildirimden muafiyeti veya bildirim basitleştirilmesini sağlayabilirler:

- veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkileyecek, işlenecek verileri muhtemelen dikkate almayan işleme faaliyeti kategorileri için, depolanacak veriler süre uzunluğu ve verilerin ifşa edileceği alıcılar veya alıcı kategorileri, veri öznesi kategorisi veya kategorileri, işlemeye tabi veri kategorileri veya veriler, işleme amaçlarını belirtirler, ve/veya;
- denetleyici, kendisini yöneten ulusal kanunla uyumlu olarak özellikle aşağıdakilerden sorumlu bir kişisel veri koruma görevlisi atar;
- bu Direktif uyarınca, alınan ulusal hükümlerin bağımsız şekilde dahili uygulamasını sağlama;
- madde 21(2)'de atıfta bulunulan bilgilendirme maddelerini içeren şekilde, denetleyici tarafından yürütülen işleme faaliyetlerinin kaydını tutma;
- böylece, veri öznelerinin hak ve özgürlüklerinin, işleme faaliyetleri tarafından olumsuz şekilde etkilenmesinin olanaksız olmasını sağlama.

3. Üye Devletler, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlamak amaçlı kanunlara veya yönetmeliklere göre tek amacı bir kayıt tutma olan işlemeye 1. paragrafın uygulanmamasını sağlayabilir.

4. Üye Devletler, madde 8(2)(d)'de atıfta bulunulan işleme faaliyetleri durumunda, bildirim basitleştirilmesini veya bildirimde bulunma yükümlülüğünden muafiyeti sağlayabilirler.

5. Üye Devletler, kişisel verileri kapsayan belirli veya tüm otomatik olmayan işleme faaliyetlerinin bildirilmesini şart koşabilirler ya da bu işleme faaliyetlerinin basitleştirilmiş bildirim tabi olmasını belirtebilirler.

Madde 19

Bildirim içerikleri

1. Üye Devletler, bildirimde verilecek bilgileri belirteceklerdir. Bunlar en azından aşağıdakileri içerecektir:

- (a) Denetleyici ve varsa temsilcisinin adı ve adresi;
- (b) İşlemenin amacı veya amaçları;
- (c) Bunlara ilişkin veri kategorileri veya verinin ve özne verisinin kategorileri veya kategorisinin tanımı;
- (d) Verilerin açıklanabileceği alıcılar veya alıcı kategorileri;
- (e) Üçüncü ülkelere önerilen veri transferleri;

(f) Veri güvenliğini sağlamak üzere madde 17 uyarınca alınan tedbirlerin uygunluğunun sağlanması için bir ön değerlendirmeye olanak sağlayan genel bir tanım;

2. Üye Devletler paragraf 1’de atıf yapılan bilgileri etkileyen herhangi bir değişikliğin denetleme makamına bildirilmesine dönük prosedürleri belirletecektir.

Madde 20

Ön kontrol

1. Üye Devletler, veri öznelerinin haklarına ve özgürlüklerine özel riskler sunması, olası işleme faaliyetlerini belirleyecektir ve bu işleme faaliyetlerinin başlatılmasından önce incelenmesini kontrol edecektir.

2. Bu tür ön kontroller, şüphe durumunda denetim makamına danışması gereken bir veri koruma görevlisi tarafından veya denetleyiciden bir bildirim alınmasını takiben denetleme makamı tarafından yerine getirilecektir.

3. Üye Devletler ya ulusal parlamentonun bir tedbiri ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bu tür bir yasama tedbirine dayalı bir tedbirin hazırlanması bağlamında, bu tür kontrolleri de yapabilir.

Madde 21

İşleme faaliyetlerinin duyurulması

1. Üye Devletler, işleme faaliyetlerinin duyurulmasını temin etmek için tedbirler alacaktır.

2. Üye Devletler, madde 18’e uygun olarak, bildirilen işleme faaliyetlerinin bir kaydının denetleme makamı tarafından tutulmasını sağlayacaktır.

Kayıt, en azından madde 19 (1) (a) (e) de listelenen bilgileri içerecektir.

Kayıt herhangi bir kişi tarafından denetlenebilir.

3. Üye Devletler, bildirim tabi olmayan işleme faaliyetlerine ilişkin olarak, Üye Devletler tarafından atanan denetleyicilerin veya diğer bir kuruluşun, talep üzerine herhangi bir kişiye uygun biçimde en azından madde 19 (1) (a) (e)de atıfta bulunulan bilgileri sağlamasını temin edecektir.

Üye Devletler ya meşru menfaat kanıtını temin edebilen herhangi bir kişi tarafından ya da genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlaması kastedilen yönetmeliklere veya yasalara göre; tek amacı bir kayıt tutulması olan işlemeye bu hükmün uygulanmamasını sağlayabilir.

BÖLÜM III

YARGI YOLLARI, SORUMLULUK VE MÜEYYİDELER

Madde 22

Yargı yolları

Yargı makamına başvurudan önce, madde 28'de atıfta bulunulan denetleme makamı öncesinde, diğerlerine ilaveten koyulabilecek hüküm için herhangi bir idari çözüme zarar vermeksizin, Üye Devletler, söz konusu işlemeye uygulanan ulusal kanun tarafından garanti edilen hakların herhangi bir ihlali için bir yargı yolunu, her kişinin hakkı olarak sağlayacaktır.

Madde 23

Sorumluluk

1. Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumsuz herhangi bir işlemenin veya yasadışı bir işleme faaliyetinin sonucu olarak zarara uğrayan herhangi bir kişinin, uğradığı zarar için denetleyiciden tazminat almaya hak kazanmasını sağlayacaktır.
2. Denetleyici, zarara yol açan olayda sorumlu olmadığını kanıtlarsa, kısmen ya da tamamen bu yükümlülükten muaf tutulabilir.

Madde 24

Müeyyideler

Üye Devletler, bu Direktifin hükümlerinin tam uygulanmasını sağlayacak uygun tedbirleri kabul edecektir ve özellikle, bu direktif uyarınca kabul edilen hükümlerin ihlali durumunda uygulanacak müeyyideleri koyacaktır.

BÖLÜM IV

KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE TRANSFERİ

Madde 25

Prensipler

1. Üye Devletler, bu Direktifin diğer hükümleri uyarınca benimsenen ulusal hükümlere uyuma zarar vermeksizin, yalnızca söz konusu üçüncü ülke yeterli koruma seviyesi sağlarsa, transfer sonrası işleme için istenen veya işlemeye tabi olan kişisel verilerin bir üçüncü ülkeye transferinin gerçekleşebilmesini sağlayacaktır.
2. Bir üçüncü ülke tarafından sağlanan koruma seviyesinin yeterliliği, veri transfer faaliyetlerinin dizisinin veya bir veri transfer faaliyetini çevreleyen tüm koşulların ışığında değerlendirilecektir. O ülkeyle uyumlu meslek kuralları ve güvenlik tedbirleri ve söz konusu üçüncü ülkedeki yürürlükte olan hem genel hem sektörel yasa hükümleri, son varış ülkesi ve menşe ülke, önerilen faaliyet veya faaliyetlerin süresi ve amacı, verilerin yapısına özel önem verilecektir.

3. Üye Devletler ve Komisyon, 2. paragrafın anlamı dahilinde yeterli koruma seviyesini bir üçüncü ülkenin sağlamadığını düşündükleri durumlarda birbirlerini bilgilendireceklerdir.
4. Komisyon, bu maddenin 2. paragrafının anlamında, bir üçüncü ülkenin yeterli koruma seviyesini sağlamadığını madde 31 (2) kapsamında sağlanan prosedüre göre tespit ederse, Üye Devletler, söz konusu üçüncü ülkeye aynı tipte verilerin herhangi bir transferini önlemek için gerekli önlemleri alacaklardır.
5. Komisyon, uygun bir zamanda, paragraf 4 uyarınca sağlanan bulgudan kaynaklanan durumu çözmek amacıyla müzakerelere başlayacaktır.
6. Komisyon, madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak; bireylerin temel haklarının ve özel yaşamlarının korunması için, özellikle paragraf 5'te atıfta bulunulan müzakerelerin sonuçlanması üzerine, giriştiği uluslararası taahhütler veya kendi yerel yasası nedeniyle, bu maddenin 2. paragrafı anlamı dahilinde üçüncü bir ülkenin yeterli bir koruma seviyesini temin etmesini isteyebilir.

Üye Devletler, Komisyonun kararıyla uyum sağlamak için gerekli tedbirleri alacaktır.

Madde 26

İstisnalar

1. Madde 25'den derogasyon (uygulama dışı tutma) yoluyla ve özel durumları yöneten iç hukukun aksini belirtmesi haricinde, Üye Devletler, aşağıdaki koşullarda madde 25 (2)'nin anlamı dahilinde yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel verilerin transfer dizisini veya transferinin yapılabilmesini sağlayacaktır:
 - (a) Veri öznesi önerilen transfer için açık şekilde rızasını vermişse veya
 - (b) Veri öznesinin talebine yanıt olarak alınan ön sözleşme tedbirlerinin uygulanması veya denetleyici ve veri öznesi arasındaki bir sözleşmenin yerine getirilmesi için transfer gerekliyse; veya
 - (c) Üçüncü bir şahıs ve denetleyici arasında veri öznesinin menfaatine sonuçlanan bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için transfer gerekliyse, veya
 - (d) Transfer; kanuni hakların tesisi, işletilmesi veya savunulması için veya önemli kamu menfaati zemininde yasal olarak gerekliyse veya zorunluysa, veya
 - (e) Veri öznesinin hayati menfaatlerinin korunması için transfer gerekirse, veya
 - (f) Özel durumda yapılan konsültasyon için kanunda öngörülen koşullar ölçüsünde, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlamak amaçlı kanunlar veya yönetmeliklere göre transfer bir kayıttan sağlanırsa.
2. Paragraf 1'e zarar vermeksizin, bir Üye Devlet, ilgili hakların işletilmesine dair ve bireylerin temel hak ve özgürlükleri ve kişisel mahremiyet hakkının korunmasına ilişkin anlam dahilinde, yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel veri transferler dizisine veya bir transferine izin verebilir, bu tür korunma önlemleri

özellikle uygun sözleşme maddelerinden kaynaklanabilir.

3. Üye Devlet, paragraf 2 uyarınca verdiği izinlerden Üye Devletleri ve Komisyonu haberdar edecektir.

Bir Üye Devlet veya Komisyon, bireylerin temel hakları ve özgürlükleri ve mahremiyetinin korunmasını gerektiren gerekçeli dayanaklara itiraz ederse, Komisyon, madde 31 (2)'de belirtilen prosedüre göre uygun tedbirleri alacaktır.

Üye Devletler Komisyonun kararına uymak için gerekli tedbirleri alacaklardır.

4. Madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak, Komisyon, bazı standart sözleşme maddelerinin paragraf 2'nin gerektirdiği şekilde yeterli teminat sunmasına karar verirse, Üye Devletler, Komisyon kararına uymak için gerekli tedbirleri alacaklardır.

BÖLÜM V

DAVRANIŞ KURALLARI

Madde 27

1. Üye Devletler ve Komisyon, çeşitli sektörlerin özel niteliklerini dikkate alarak, bu Direktif uyarınca Üye Devletler tarafından benimsenen ulusal hükümlerin doğru uygulanmasına katkı sağlamak için planlanan davranış kurallarını düzenlemeye teşvik edecektir.
2. Üye Devletler, mevcut ulusal kodları tadil etme veya genişletme niyetine sahip veya taslak ulusal kodları hazırlamış denetleyicilerin diğer kategorilerini temsil eden diğer kuruluşlar ve ticari kurumların, davranış kurallarını ulusal makamın görüşüne sunabilmesi için önlem alacaktır.

Üye Devletler, sunulan taslakların, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumlu olup olmadığını ulusal makamın belirlemesi için önlem alacaktır. Komisyon, taslağı uygun görürse, ulusal makam, kendi temsilcilerinin veya veri öznelerinin görüşlerini isteyecektir.

3. Taslak Topluluk kodları ve mevcut Topluluk kodlarının uzantıları veya düzeltmeleri, madde 29'da atıfta bulunulan çalışma grubuna sunulabilir. Bu çalışma grubu diğer şeyler arasında, sunulan taslağın, bu Direktif uyarınca kabul edilen ulusal hükümlere uygun olup olmadığını belirleyecektir. Uygun bulursa, (ulusal) makam, veri öznelerinin ve kendi temsilcilerinin görüşlerini isteyecektir. Komisyon, Çalışma Grubu tarafından onaylanmış kuralların uygun şekilde tanıtımını sağlayabilir.

BÖLÜM VI

KİŞİSEL VERİLERİN İŞLENMESİNE DAİR BİREYLERİN KORUNMASI HAKKINDAKİ ÇALIŞMA GRUBU VE DENETLEME MAKAMI

Madde 28

Denetleme makamı

1. Her bir Üye Devlet, , bu Direktif uyarınca Üye Devletler tarafından kabul edilen

hükümlerin kendi ülkesindeki uygulamasını izlemekten, bir veya daha fazla kamu makamının sorumlu olmasını sağlayacaktır.

Bu makamlar, onlara tevdi edilen işlevleri yerine getirmede tam bağımsız olarak hareket edeceklerdir.

2. Her bir Üye Devlet, kişisel verilerin işlenmesine dair bireylerin hak ve özgürlüklerinin korunmasına ilişkin idari tedbirleri veya yönetmelikleri hazırlarken, denetim makamına danışılmasını sağlayacaktır.

3. Her bir makama özellikle sağlanacaktır:

— denetim görevlerinin yerine getirilmesi için gerekli tüm bilgileri toplama yetkileri ve işleme faaliyetlerinin konusunu oluşturan verilere erişim yetkileri gibi araştırma yetkileri;

— örneğin ulusal parlamentolar veya diğer siyasi kuruluşlara konuyu havale etme veya denetleyiciye ihtar verme veya uyarma, işleme üzerinde geçici veya kesin yasaklama koyma, verilerin yok edilmesini veya silinmesini, engellenmesini emretme, bu tür görüşlerin uygun şekilde yayınlanmasını sağlama ve madde 20'e uygun olarak işleme faaliyetlerinin yerine getirilmesinden önce görüş bildirme gibi etkin müdahale yetkileri;

— Bu Direktif uyarınca kabul edilen ulusal hükümler ihlal edildiğinde veya bu ihlalleri yargı makamlarının dikkatine sunma için kanuni kovuşturmayla girişme yetkisi.

Denetleme makamının şikayetlere yol açan kararları; mahkemelerde temyiz edilebilir.

4. Her bir denetim makamı, kişisel verilerin işlenmesine dair hak ve özgürlüklerin korunmasına ilişkin o kişiyi temsil eden bir dernek veya herhangi bir kişi tarafından arzedilen iddiaları dinleyecektir.

Her bir denetim makamı, özellikle, bu Direktifin 13. maddesi uyarınca kabul edilen ulusal hükümler uygulandığında, herhangi bir kişi tarafından arz edilen veri işlemenin yasallığı hakkındaki kontroller için iddiaları dinleyecektir. Kişi, bir kontrolün yapıldığından her halükarda bilgilendirilecektir.

5. Her denetleme makamı, faaliyetleri hakkında düzenli aralıklarla bir rapor hazırlayacaktır. Rapor, kamuya açıklanacaktır.

6. Her denetleme makamı, sözkonusu işlemeye uygulanan ulusal kanun her ne olursa olsun, paragraf 3'e uygun olarak verilen yetkileri kendi Üye Devletinin toprağında uygulamaya yetkilidir. Her bir makamdaki, diğer bir Üye Devletin makamı ile yetkilerini uygulaması istenebilir.

Denetleme makamları, özellikle tüm yararlı bilgileri takas ederek, kendi görevlerini yerine getirmek için gerekli ölçüde birbirleriyle iş birliği yapacaklardır.

7. Üye Devletler, görevlerinin bitiminden sonra bile, denetleme makamının personellerinin ve mensuplarının, eriştikleri gizli bilgilere dair mesleki gizlilik görevine tabi olmalarını sağlayacaktır.

*Madde 29***Kişisel Verilerin İşlenmesine dair Bireylerin Korunması Hakkındaki Çalışma Grubu**

1. Bundan böyle “Çalışma Grubu” denilecek olan, Kişisel Verilerin İşlenmesine dair Bireylerin Korunması hakkında bir çalışma grubu, bu belgeyle kurulmaktadır.

Danışma statüsüne sahip olacak ve bağımsız olarak hareket edecektir.

2. Çalışma Grubu, Komisyon’un bir temsilcisi ve Topluluk kurumları ve kuruluşları için kurulan makamların veya makamın birer temsilcisi ve her bir Üye Devlet tarafından atanan denetleme makamı veya makamlarının birer temsilcisinden oluşacaktır.

Çalışma Grubunun her bir üyesi, temsil ettikleri makam veya makamlar, kurumlar tarafından atanacaklardır. Bir Üye Devlet birden fazla denetleme makamı atamışsa, bunlar ortak bir temsilci atayacaklardır. Aynısı, Topluluk kurum ve kuruluşları için saptanan makamlara uygulanacaktır.

3. Çalışma Grubu, denetleme makamları temsilcilerinin salt (kendi) çoğunluğuyla kararlar alacaktır.

4. Çalışma Grubu, başkanını seçer. Başkanın görev süresi iki yıl olacaktır. Başkan yeniden seçilebilecektir.

5. Çalışma Grubunun sekreteryası Komisyon tarafından sağlanacaktır.

6. Çalışma Grubu, kendi prosedür kurallarını kabul edecektir.

7. Çalışma Grubu, ya Komisyon’un talebi veya denetleme makamının bir temsilcisinin talebi üzerine veya kendi inisiyatifıyla, başkanı tarafından gündemine getirilen maddeleri ele alacaktır.

Madde 30

1. Çalışma Grubu:

(a) Bu tür tedbirlerin düzenli uygulanmasına katkı sağlamak için bu Direktif kapsamında benimsenen ulusal tedbirlerin uygulanmasını kapsayan herhangi bir sorunu inceleyecektir;

(b) Topluluktaki ve üçüncü ülkelerdeki koruma seviyesi hakkında Komisyon’a görüş verecektir;

(c) Kişisel verilerin işlenmesine dair gerçek kişilerin hak ve özgürlüklerini güvenceye alacak ek veya özel tedbirler hakkında ve bu tür hak ve özgürlükleri etkileyen diğer önerilmiş Topluluk tedbirleri hakkında, bu Direktifin herhangi bir önerilen tadili üzerinde Komisyona tavsiyede bulunacaktır;

(d) Topluluk seviyesinde hazırlanan davranış kuralları hakkında görüş verecektir.

2. Çalışma Grubu, Topluluktaki kişisel verilerin işlenmesine dair kişilerin korunmasında eşdeğerliği muhtemelen etkileyecek uyumsuzlukların Üye Devletlerin uygulamalarından ya da kanunlarından kaynaklandığını saptarsa, bu doğrultuda

Komisyon'u bilgilendirecektir.

3. Çalışma Grubu kendi insiyatifiyle, Toplulukta kişisel verilerin işlenmesine dair kişilerin korunmasına ilişkin tüm konularda tavsiyelerde bulunabilir.

4. Çalışma Grubunun fikirleri ve tavsiyeleri, madde 31'de atıfta bulunulan komiteye ve Komisyon'a iletilecektir.

5. Komisyon, görüş ve tavsiyelerine yanıt olarak aldığı önlemleri Çalışma Grubu'na bildirecektir. Bunu Avrupa Parlamentosu ve Konseyi'ne de iletilecek bir raporla yapacaktır. Rapor kamuya açık olacaktır.

6. Çalışma Grubu, Komisyon, Avrupa Parlamentosu ve Konseyi'ne iletilecek olan üçüncü ülkelerde ve topluluktaki kişisel verilerin işlenmesine dair gerçek kişilerin korunmasına dair durum hakkında bir yıllık rapor hazırlayacaktır. Rapor halka duyurulacaktır.

BÖLÜM VII

TEDBİRLERİ UYGULAYAN TOPLULUK

▼ M1

Madde 31

1. Komisyon bir komite tarafından desteklenecektir.
2. Bu maddeye atıf yapıldığında, 1999/468/EC (¹) sayılı kararın 4 ve 7. maddeleri, ilgili 8. maddenin hükümleri gözönünde bulundurularak uygulanacaktır.

1999/468/EC sayılı kararın 4(3) maddesinde belirtilen dönem, üç ay olacaktır.

3. Komite kendi prosedür kurallarını kabul edecektir.

▼ B

NİHAİ HÜKÜMLER

Madde 32

1. Üye Devletler, bu Direktifle uyum sağlamak için gerekli idari hükümleri, yasaları ve yönetmelikleri kabul edilme tarihinden itibaren en geç üç yıllık dönemin bitimine kadar yürürlüğe koyacaklardır.

Üye Devletler bu kararları kabul ettiğinde, bunlar, bu Direktife bir atıfı içerecektir veya kendi resmi yayınları dolayısıyla bu tür bir atıf eşlik edecektir. Bu tür referans yapma yöntemleri, Üye Devletler tarafından öngörülecektir.

2. Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerin yürürlüğe girdiği tarihte devam eden işlemenin; bu yürürlük tarihinden itibaren üç yıl içinde, bu hükümlerle uygun hale getirilmesini temin edeceklerdir.

Önceki alt paragraftan derogasyon yoluyla, Üye Devletler, bu Direktifin

uygulanmasına ilişkin benimsenen ulusal hükümlerin yürürlüğe koyulduğu tarihte manuel dosyalama sisteminde tutulan verilerin işlenmesinin kabul tarihinden itibaren 12 yıl içinde, bu Direktifin 6, 7 ve 8. maddelerine uyumlu hale getirilmesini sağlayabilirler. Ancak, Üye Devletler, denetleyici tarafından izlenen meşru amaçlarla uyumsuz bir biçimde depolanan veya eksik, yanlış olan verilerin engellenmesi veya silinmesi, düzeltilmesi ve elde etme hakkını, özellikle erişim hakkını yerine getirme zamanında ve talebi üzerine veri öznesine vereceklerdir.

3. Paragraf 2'den derogasyon yoluyla, Üye Devletler, uygun korunma önlemlerine tabii olarak, yalnızca, tarihsel araştırma amacıyla tutulan verilerin bu Direktifin 6, 7 ve 8. Maddesine uyumlu hale getirilmesine gerek olmadığını belirtebilirler.

4. Üye Devletler, bu Direktifle kapsanan alanda kabul ettikleri iç hukuk hükümlerinin metnini Komisyona iletacaktır.

Madde 33

Komisyon, gerekirse, tadiller için uygun önerileri raporuna ekleyerek, bu Direktifin uygulanması hakkında madde 32⁶ de atıfta bulunulan tarihin 3 yıl öncesinden başlayarak düzenli aralıklarla Avrupa Parlamentosu ve Konseye rapor sunacaktır. Rapor halka duyurulacaktır.

Komisyon, özellikle, gerçek kişilere ilişkin ses ve görüntü verilerinin işlenmesinde bu Direktifin uygulanmasını inceleyecektir ve bilgi toplumundaki ilerleme durumunun ışığında ve bilgi teknolojisindeki gelişmeleri dikkate alarak gerekeceği kanıtlanan herhangi uygun önerileri sunacaktır.

Madde 34

Bu Direktif Üye Devletlere hitap etmektedir.

⁶ Komisyona verilen uygulama yetkilerinin yerine getirilme prosedürlerini belirten 1999/468/EC sayı ve 28 Haziran 1999 tarihli Konsey Kararı (OJ L 184, 17.7.1999, sayfa:23)