İSTANBUL BİLGİ ÜNİVERSİTESİ
BİLİŞİM VE TEKNOLOJİ HUKUKU ENSTİTÜSÜ

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü olarak kişisel verilerin korunması alanındaki önemli bir Avrupa Birliği Hukuku düzenlemesi olan "**Suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı ile ilgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı yerine geçen 27 Nisan 2016 tarihli (AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ"*** isimli direktifin Türkçe tercümesini bilgilerinize sunarız.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitümüzün çalışmalarını https://itlaw.bilgi.edu.tr adresinden takip edebilirsiniz.

* Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ 04.05.2016 L 119.

L 119/89

Suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı ile ilgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı yerine geçen

27 Nisan 2016 tarihli

(AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ

AVRUPA PARLAMENTOSU VE AVRUPA BİRLİĞİ KONSEYİ,

Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'yı ve bu Antlaşma'nın özellikle 16'ncı maddesinin 2'nci fıkrasını göz önünde tutarak,

Avrupa Komisyonu'nun önerisini göz önünde tutarak,

Taslak yasama tasarrufunun ulusal parlamentolara gönderilmesini müteakip,

Bölgeler Komitesi'nin görüşünü dikkate alarak[1],

Olağan yasama usulüne uyarınca hareket ederek[2],

Aşağıdaki gerekçelerle:

(1) Kişisel verilerinin işlenmesi ile ilgili olarak gerçek kişilerin korunması temel bir haktır. Avrupa Birliği Temel Haklar Bildirgesi'nin ("**Bildirge**") 8'inci maddesinin 1'inci fıkrası ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın ("**TFEU**" ["**ABİA**"]) 16'ncı maddesinin 1'inci fıkrası uyarınca kişilere kendisiyle ilgili kişisel verilerin korunması hakkı tanınmıştır.

(2) Gerçek kişilerin kişisel verilerinin işlenmesi ile ilgili ilkeler ve koruma kuralları, onların temel hak ve özgürlüklerine özellikle kişisel verilerinin korunmasına ilişkin haklarına, uyrukları veya ikametgahları neresi olursa olsun saygı göstermelidir. İşbu Direktif özgürlük, güvenlik ve adalet alanının sağlanmasına katkıda bulunulmasını amaçlamaktadır.

[1] OJ C 391, 18.12.2012, s. 127.
[2] 12 Mart 2014 tarihli Avrupa Parlamentosu'nun Görüşü (henüz Resmi Gazete'de yayımlanmamıştır) ve Konsey'in 8 Nisan 2016 tarihli ilk mütalaası (henüz Resmi Gazete'de yayımlanmamıştır). 14 Nisan 2016 tarihli Avrupa Parlamentosu Görüşü.

(3) Hızlı teknolojik gelişmeler ve küreselleşme kişisel verilerin korunması için yeni zorlukları beraberinde getirmiştir. Kişisel verilerin toplanması ve paylaşılmasının kapsamı önemli ölçüde artmıştır. Teknoloji, suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı gibi faaliyetlerin sürdürülmesi için daha önce görülmemiş kapsamda kişisel verilerin işlenmesi imkanını tanımaktadır.

(4) Kişisel verilerin yüksek düzeyde korunması sağlanırken, suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla, Birlik içindeki kamu güvenliğine yönelik tehditlerin önlenmesi ve bu tehditlere karşı konulması ve bu tür kişisel verilerin üçüncü ülkelere ve uluslararası kuruluşlara aktarılması dahil olmak üzere, yetkili makamlar arasında verilerin serbest dolaşımı kolaylaştırılmalıdır. İlgili gelişmeler, Birlik'teki kişisel verilerin korunması için güçlü yaptırımlarla desteklenen, kuvvetli ve daha tutarlı bir çerçeve oluşturulmasını gerektirmektedir.

(5) Avrupa Parlamentosu ve Konsey'in 95/46/AT sayılı Direktifi[3] Üye Devletler'de hem kamu hem de özel sektördeki tüm kişisel verilerin işlenmesini kapsar. Ancak, cezai konularda adli ve kolluk iş birliği alanlarındaki faaliyetler gibi Topluluk hukuku kapsamı dışında kalan bir faaliyet sırasında kişisel verilerin işlenmesini kapsamaz.

(6) 2008/977/Aİİ[4] sayılı Konsey Çerçeve Kararı, cezai konularda adli ve kolluk iş birliği alanlarını kapsar. Bu Çerçeve Kararı'nın uygulanmasının kapsamı, Üye Devletler arasında aktarılan veya erişilebilen kişisel verilerin işlenmesiyle sınırlıdır.

(7) Gerçek kişilerin kişisel verilerinin sürekli ve yüksek düzeyde korunmasının sağlanması ve kişisel verilerin Üye Devletler'in yetkili makamları arasında alışverişinin kolaylaşması, cezai konularda adli ve kolluk iş birliğinin sağlanması için büyük önemi haizdir. Bu maksatla, kişisel verilerin, kamu güvenliğine yönelik tehditlerin önlenmesi ve bu tehditlere karşı konulması dahil, yetkili makamlarca suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla işlenmesiyle ilgili gerçek kişilerin hak ve özgürlüklerinin korunmasının düzeyi tüm Üye Devletler'de aynı olmalıdır. Birlik genelinde kişisel verilerin etkin bir şekilde

[3] 95/46/AT sayılı ve 24 Ekim 1995 tarihli kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki Avrupa Parlamentosu ve Konsey Direktifi (OJ L 281, 23.11.1995, s. 31).
[4] 27 Kasım 2008 tarihli ve 2008/977/Aİİ sayılı suç işlenmesinde kolluk ve adli iş birliği çerçevesinde işlenen kişisel verilerin korunmasına ilişkin Konsey Çerçeve Kararı (OJ L 350, 30.12.2008, s. 60).

korunması, Üye Devletler'deki kişisel verilerin korunmasına ilişkin kurallara uyumu gözlemleyen ve sağlayan eşdeğer yetkiler yanında veri sahiplerinin haklarının ve kişisel verileri işleyenlerin yükümlülüklerinin güçlendirilmesini de gerektirmektedir.

(8) ABİA'nın 16'ncı maddesinin 2'nci fıkrası, Avrupa Parlamentosu ve Konsey'e kişisel verilerin işlenmesi ile ilgili olarak gerçek kişilerin korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kuralların belirlenmesini buyurmaktadır.

(9) Buna dayanarak, Avrupa Parlamentosu ve Konsey'in 2016/679 (AB) sayılı Regülasyonu,[5] kişisel verilerinin işlenmesi ile ilgili olarak gerçek kişilerin korunması ve kişisel verilerin Birlik içinde serbest dolaşımının sağlanması için genel hükümler belirlemektedir.

(10) Lizbon Anlaşması'nı kabul eden devletler arası görüşmenin nihai tasarrufa eklenmiş olduğu, cezai konularda adli ve kolluk iş birliği alanlarındaki kişisel verilerin korunması hakkındaki 21 sayılı Bildiri'de, ABİA'nın 16'ıncı maddesi uyarınca cezai konularda adli ve kolluk iş birliğinin sağlanması ile ilgili alanlarda kişisel verilerin korunması ve verilerin serbest dolaşımının sağlanması hakkında bu alanların kendine özgü niteliğinden kaynaklı olarak özel hükümlerin belirlenmesinin gerekli olduğu kabul edilmiştir.

(11) Bu nedenle, bahsi geçen alanların, kişisel verilerin yetkili makamlar tarafından suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla, kamu güvenliğine yönelik tehditlerin önlenmesi ve bu tehditlere karşı konulması da dahil olmak üzere işlenmesi ile ilgili olarak gerçek kişilerin korunmasına ilişkin, bu faaliyetlerin kendine özgü doğasına saygı duyan, özel kuralların belirlendiği bir direktif ile düzenlenmesinin uygun olacağına karar verilmiştir. Bu gibi yetkili makamlar, yalnızca adli makamlar, polis ve diğer kolluk kuvvetleri gibi kamu makamlarını değil, aynı zamanda Üye Devlet hukukunun işbu Direktif'in amaçları doğrultusunda kamu otoritesini ve kamu güçlerini kullanma yetkisine sahip başka herhangi bir kurum veya kuruluşu içerebilir. Bu tür bir kurumun veya kuruluşun, kişisel verileri işbu Direktif amaçları dışında işlemesi halinde, 2016/679 (AB) sayılı Regülasyon uygulanacaktır. Bu nedenle, 2016/679 (AB) sayılı Regülasyon, bir kurumun veya kuruluşun kişisel verileri farklı amaçlarla topladığı ve ayrıca tabi olduğu yasal yükümlülüğe uymak için daha fazla veri işlediği hallerde uygulanmaktadır. Örneğin, finansal kurumlar, soruşturmanın

[5] Avrupa Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/679 (AB) sayılı, 95/46/AT sayılı Direktif'in yerine geçen, kişisel verilerin işlenmesi ile ilgili olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin Tüzüğü (Avrupa Birliği Genel Veri Koruma Tüzüğü) (Resmi Gazete'nin 1'inci sayfasından ulaşılabilir).

tespiti veya ceza suçlarının kovuşturulması amacıyla kendileri tarafından işlenen belirli kişisel verileri saklamakta ve bu kişisel verileri yalnızca belirli hallerde ve Üye Devlet hukukuna uygun olarak yetkili ulusal makamlarla paylaşmaktadır. İlgili makamlar adına İşbu Direktif kapsamında kişisel veri işleyen bir kurum veya kuruluş, bir sözleşmeyle veya diğer bir hukuki tasarrufla ve işbu Direktif'e göre veri işleyenlere uygulanacak hükümlere bağlı olmakta, işbu Direktif'in kapsamı dışındaki veri işleyenin kişisel verileri işlemesinde 2016/679 (AB) sayılı Regülasyon uygulanmamaktadır.

(12) Polis veya diğer kolluk kuvvetleri tarafından yürütülen faaliyetler esas olarak, bir olayın suç olup olmadığı konusunda önceden bilgi sahibi olunmayan polis faaliyetleri de dahil olmak üzere, cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması ile ilgilidir. Bu tür faaliyetler, yetkinin, gösterilerde, büyük çaplı spor etkinliklerinde ve ayaklanmalardaki polis faaliyetleri gibi zorlayıcı önlemler alarak kullanılmasını da içermektedir. Ayrıca, hukuken güvence altına alınan, gerektiğinde cezai bir suç teşkil edebilecek olan kamu yararı ve kamu güvenliği tehditlerine karşı korunmak ve bu tehditleri önlemek gerektiğinde polis ve diğer kolluk makamlarına verilen bir görev olarak hukukun ve düzenin korunmasını da içermektedir. Üye Devletler yetkili makamlara, kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması amacıyla yapılması zorunlu olmayan başka görevler de verebilir, kişisel verilerin işlenmesi bu başka amaçlar için işlenmesi, Birlik hukuku kapsamında olduğu sürece, 2016/679 (AB) sayılı Regülasyon kapsamındadır.

(13) İşbu Direktif uyarınca cezai bir suç, Avrupa Birliği Adalet Divanı ("**Adalet Divanı**") tarafından yorumlandığı şekliyle müstakil bir Birlik hukuku kavramı olmalıdır.

(14) İşbu Direktif, kişisel verilerin Birlik hukuku kapsamı dışında kalan bir faaliyet sırasında işlenmesini kapsamadığından, ulusal güvenlikle ilgili faaliyetler, ulusal güvenlik meseleleriyle ilgili teşkilat ve birimlerin faaliyetleri ve Üye Devletler tarafından Avrupa Birliği Antlaşması'nın ("**TEU**" ["**ABA**"]) Başlık 5'in ikinci bölümünde yer alan faaliyetlerin yürütülmesi kapsamında kişisel veri işlenmesi işbu Direktif'in kapsamına giren faaliyetler olarak değerlendirilmemelidir.

(15) İşbu Direktif, Birlik genelinde gerçek kişiler için yasal olarak icra edilebilir haklar aracılığıyla aynı düzeyde koruma ve yetkili makamlar arasında kişisel verilerin alışverişini engelleyici sapmaların önlenmesini sağlamak için, kamu güvenliğine yönelik tehditlerin önlenmesi ve karşı

konulması dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla işlenen kişisel verilerin korunması ve serbest dolaşımı için uyumlaştırılmış kurallar öngörmelidir. Üye Devletler'in kanunlarının yaklaşımı, sağladıkları kişisel veri korumasının azalmasına neden olmamalı, aksine Birlik içerisinde yüksek düzeyde veri korumasının sağlanmasını amaçlamalıdır. Üye Devletler'i, veri sahiplerinin hak ve özgürlüklerinin kişisel verilerin yetkili makamlarca işlenmesi ile ilgili olarak korunmasına yönelik işbu Direktif'te belirtilenden daha yüksek güvenlik önlemlerini almaktan engellememelidir.

(16) İşbu Direktif, resmi belgelerin kamuya açıklığı ilkesine halel getirmemektedir. 2016/679 (AB) sayılı Regülasyon uyarınca, bir resmi makam ya da bir kamu kurumu veya özel kuruluş tarafından düzenlenen resmi belgelerde kamu yararı için gerçekleştirilen bir görevin yerine getirilmesine ilişkin kişisel veriler, resmi makamın veya kuruluşun, resmi belgelerin kamuya açıklığı ile kişisel verilerin korunması hakkının uyumlu olması için tabi olduğu Birlik veya Üye Devlet hukuku uyarınca bu makam veya kuruluş tarafından açıklanabilir.

(17) İşbu Direktif tarafından sağlanan koruma, kişisel verilerin işlenmesi ile ilgili olarak, gerçek kişiler için uyruk veya ikametgah fark etmeksizin uygulanır.

(18) Ciddi bir sahtekarlık riskinin doğmasının önlenmesi için gerçek kişilerin korunması teknoloji bakımından tarafsız olmalı ve kullanılan tekniklere bağlı olmamalıdır. Gerçek kişilerin korunması, kişisel verilerin elle işlenmesi yanında kişisel verilerin bir kayıt sisteminde yer aldığı veya yer almasının tasarlandığı durumlarda, kişisel verilerin otomatik yollarla işlenmesine de uygulanmalıdır. Kapak sayfalarının yanı sıra belli kriterlere göre yapılandırılmamış dosyalar veya dosya kümeleri de işbu Direktif kapsamında yer almamaktadır.

(19) Avrupa Parlamentosu'nun ve Konsey'in 45/2001 (AT)[6] sayılı Regülasyonu, kişisel verilerin Birlik kurumları, kuruluşları, ofisleri, teşkilatları tarafından işlenmesi kapsamında uygulanır. Kişisel verilerin bu şekilde işlenmesine uygulanabilir 45/2001 (AT) sayılı Regülasyon ve diğer hukuki Birlik tasarrufları, 2016/679 (AB) sayılı Regülasyon'da belirlenen ilke ve kurallara uygun hale getirilmelidir.

[6] 18 Aralık 2000 tarihli ve 45/2001 sayılı kişisel verilerin Topluluk kurum ve kuruluşları tarafından işlenmesi ve bu verilerin serbest dolaşımı hakkında kişilerin korunmasına ilişkin Avrupa Parlamentosu ve Avrupa Konseyi'nin Tüzüğü (AB) (OJ L 8, 12.1.2001, s. 1).

(20) İşbu Direktif, Üye Devletler'in, özellikle cezai işlemlere ilişkin adli karar veya kayıtlarda yer alan kişisel veriler olmak üzere, kişisel verilerin mahkeme ve diğer adli makamlar tarafından işlenmesiyle ilgili olarak ceza muhakemesi usulü ile ilgili ulusal kurallarında işleme operasyonlarını ve işleme usulünü belirlemesini engellemez.

(21) Veri koruma ilkeleri, belirli veya belirlenebilir bir gerçek kişiye ilişkin herhangi bir bilgi için uygulanır. Bir gerçek kişinin belirlenip belirlenemeyeceğini tespit etmek için, arasında seçme gibi muhtemel tüm araçlar veri sorumlusu veya gerçek kişiyi doğrudan veya dolaylı olarak tespit edecek başka bir kişi tarafından hesaba katılmalıdır. Gerçek kişiyi belirlemek için kullanılması muhtemel araçları tespit ederken, işleme zamanındaki mevcut teknoloji ve teknolojik gelişmeler göz önünde bulundurularak, tespit için harcanacak giderler ve süre gibi tüm objektif etmenler hesaba katılmalıdır. Bu nedenle, veri koruma ilkeleri, anonim bilgilere, belirli veya belirlenebilir bir gerçek kişiyle bağlantılı olmayan bilgilere veya veri sahibi artık belirlenemeyecek bir şekilde anonim hale getirilmiş kişisel verilere uygulanmaz.

(22) Vergi ve gümrük makamları, mali soruşturma birimleri, bağımsız idari makamlar veya pazarların güvenliğinin düzenlenmesi ve gözetiminden sorumlu finansal pazar makamları gibi kişisel verilerin resmi görevlerinin yerine getirilmesi için yasal bir yükümlülük uyarınca aktarıldığı resmi makamlar, Birlik veya Üye Devlet hukukuna göre belirli bir talebin kamu yararına yerine getirilmesi için gerekli olan kişisel verileri alıyorsa, veri aktarılan taraf olarak değerlendirilmemelidir. Resmi makamlarca iletilen açıklama talepleri her zaman yazılı, gerekçeli ve arızi olmalı ve bir kaıyt sisteminin bütününe ilişkin olmamalı veya kayıt sistemlerinin birbirine bağlanmasına yol açmamalıdır. Kişisel verilerin bu resmi makamlarca işlenmesi, işlemenin amaçlarına göre uygulanabilir veri koruma kurallarına uygun olmalıdır.

(23) Genetik veriler, gerçek bir kişinin fizyolojisi veya sağlığı hakkında özgün bilgiler veren ve özellikle kromozomal, deoksiribonükleik asit (DNA) veya ribonükleik asit (RNA) analizi olmak üzere ilgili gerçek kişiden alınan biyolojik bir örneğin analizi sonucunda veya eşdeğer bilginin elde edilmesini sağlayan başka bir unsurun analizinden elde edilen, kalıtsal veya edinilmiş genetik özelliklerine ilişkin kişisel veri olarak belirtilmelidir. Karmaşıklığı ve hassasiyeti dikkate alındığında, genetik verilerin veri sorumlusu tarafından çeşitli amaçlar doğrultusunda hatalı ve mükerrer kullanılması riski mevcuttur. Genetik özelliklere dayalı herhangi bir ayrımcılık, kural olarak yasaklanmalıdır.

(24) Sağlıkla ilgili kişisel veriler, bir veri sahibinin geçmiş, şimdi veya gelecekteki fiziksel veya zihinsel sağlık düzeyi ile ilgili bilgileri ortaya koyan sağlık durumuna ilişkin tüm verileri içermelidir. Bu, gerçek kişi hakkında sağlık hizmetleri için kayıt sırasında toplanan bilgileri veya Avrupa Parlamentosu ve Konsey'in 2011/24/AB sayılı Regülasyonu'nda[7] sağlık hizmetlerine ilişkin hükümle belirtildiği şekliyle gerçek kişiyi sağlık amaçlarıyla eşsiz olarak belirlemek için atanan bir sayı, sembol veya belirtiyi; biyolojik numune ve genetik veri dahil olmak üzere bir vücut bölümünün veya vücut parçasının test edilmesinden veya incelenmesinden elde edilen bilgileri; ve veri sahibinin, kaynağından, örneğin bir doktor veya başka bir sağlık uzmanından, bir hastaneden, bir tıbbi cihazdan veya in vitro diagnostik testten, bağımsız olarak örneğin bir hastalığa, engele, engelliğe, hastalık riskine, tıbbi geçmişe, klinik tedaviye veya fizyolojik veya biyomedikal duruma ilişkin herhangi bir bilgiyi içermektedir.

(25) Tüm Üye Devletler, Uluslararası Kriminal Polis Teşkilatı'na (Interpol) bağlıdır. Interpol, görevini yerini getirmek için, uluslararası suçları önlemek ve bunlarla mücadelede yetkili makamlara yardımcı olmak amacıyla kişisel verileri toplamakta, saklamakta ve paylaşmaktadır. Bu nedenle, Birlik ve Interpol arasındaki iş birliğini kişisel verilerin otomatik olarak işlenmesiyle ilgili temel hak ve özgürlüklere uyulmasını sağlarken kişisel verilerin verimli alışverişini teşvik ederek güçlendirmek uygundur. Kişisel verilerin Birlik'ten Interpol'e ve Interpol'e üye gönderen ülkelere aktarıldığı durumlarda, işbu Direktif, özellikle uluslararası veri aktarımlarıyla ilgili hükümleri, uygulanmalıdır. İşbu Direktif, 2005/69/Aİİ sayılı Konsey Ortak Tutumu'nda[8] ve 2007/533/Aİİ sayılı Konsey Kararı'nda[9] belirtilen özel hükümlere halel getirmemelidir.

(26) İlgili gerçek kişilere ilişkin her türlü kişisel veri işleme faaliyeti hukuka uygun, adil ve şeffaf olmalı ve sadece hukuken belirlenmiş özel amaçlar doğrultusunda gerçekleştirilmelidir. Tek başına bu durum kolluk ve adli yargı makamlarının gizli soruşturma veya kamera kaydı gibi faaliyetleri yürütmesini engellemez. Bu tür faaliyetler, yasayla öngörüldüğü ve ilgili kişinin meşru menfaatleri bakımından demokratik bir toplumda gerekli ve ölçülü bir önlem olduğu müddetçe, kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da

[7] Avrupa Parlamentosu ve Konsey'in hasta haklarının sınır ötesi sağlık hizmetlerinde uygulanmasına ilişkin 9 Mart 2011 tarihli ve 2011/24/AB sayılı Direktifi (OJ L 88, 4.4.2011, s. 45).
[8] 24 Ocak 2005 tarihli ve 2005/69/JHA sayılı Interpol ile belirli verilerin alışverişine ilişkin Konsey Ortak Tutumu (OJ L 27, 29.1.2005, s. 61).
[9] 12 Haziran 2007 tarihli ve 2007/533/JHA sayılı İkinci nesil Schengen Bilgi Sistemi'nin (SIS II) kurulmasına, işletilmesine ve kullanılmasına ilişkin Konsey Kararı (OJ L 205, 7.8.2007, s. 63).

cezaların infazı amacıyla yapılabilir. Adil işleme veri koruma ilkesi, Bildirge'nin 47'nci maddesinde ve Avrupa İnsan Hakları Sözleşmesi'nin 6'ncı maddesinde (AİHS) tanımlanan adil yargılanma hakkından ayrı bir kavramdır. Gerçek kişiler, kişisel verilerinin işlenmesiyle ilgili risklerin, kuralların, güvencelerin ve hakların neler olduğunun ve haklarını nasıl kullanacağının bilincinde olmalıdır. Özellikle, kişisel verilerin işlendiği özel amaçlar, açık ve meşru olmalı ve kişisel verilerin toplanması esnasında belirlenmelidir. Kişisel veriler işlendikleri amaçlara uygun ve bu amaçlarla ilgili olmalıdır. Özellikle, toplanan kişisel verilerin işlendikleri amacı aşar biçimde işlenmemesi ve işlendikleri amaç için gerekenden daha uzun süre saklanmaması sağlanmalıdır. Kişisel veriler, yalnızca işlemenin amacı başka yollarla makul şekilde yerine getirilemediğinde işlenmelidir. Bunu sağlamak için, veriler gerekenden daha uzun süre tutulmamalı, silme veya periyodik inceleme için veri sorumlusu tarafından zaman periyotları belirlenmelidir. Üye Devletler, kamu yararı, bilimsel, istatistiksel veya tarihsel kullanımda arşivlemek için daha uzun süre depolanan kişisel veriler için uygun güvenlik önlemlerini almalıdır.

(27) Cezai suçların önlenmesi, soruşturulması ve kovuşturulması için, yetkili makamların, belirli cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması bağlamında toplanan kişisel verileri, bu bağlamın ötesinde, suç faaliyetlerini daha iyi anlamak ve tespit edilen farklı cezai suçlar arasında bağlantılar kurmak için işlemesi gereklidir.

(28) Veri işleme faaliyetinin güvenliğinin sağlanması ve işbu Direktif'i ihlal edecek veri işlemenin önlenmesi için, kişisel veriler, kişisel verilere ve veri işleme faaliyeti için kullanılan ekipmanlara yetkisiz erişim ya da yetkisiz kullanımı önlemek dahil olmak üzere yeterli güvenlik ve mahremiyet seviyesini temin edecek ve mevcut en gelişmiş teknolojiyi ve korunacak kişisel verilerin riskleri ve niteliğine ilişkin uygulamanın maliyetini dikkate alacak şekilde işlenmelidir.

(29) Kişisel veriler bu Direktif kapsamında belirli, açık ve meşru amaçlarla toplanmalıdır ve kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amaçlarıyla çelişecek biçimde işlenmemelidir. Kişisel verilerin aynı ya da farklı veri sorumlusu tarafından toplanma amacından farklı işbu Direktif'in kapsamında başka bir amaçla işlendiği hallerde, söz konusu veri işleme faaliyetine, uygulanacak hukuka uygun ve söz konusu diğer amaç için gerekli ve ölçülü olduğu takdirde izin verilmelidir.

(30) Verilerin doğruluğu ilkesi, ilgili veri işlemenin niteliği ve amacı göz önüne alınarak uygulanmalıdır. Özellikle adli işlemlerde, kişisel veri içeren ifadeler gerçek kişilerin öznel algılarına dayalıdır ve her zaman doğrulanabilir değildir. Bu nedenle, doğruluk gerekliliği ifadenin doğruluğu ile değil, sadece belirli bir ifadenin verilmiş olmasıyla ilgili olmalıdır.

(31) Suça ilişkin meselelerde adli ve kolluk iş birliği alanlarındaki veri işleme faaliyetlerinde farklı kategorilerdeki veri sahiplerine ait kişisel verilerin işlenmesi doğaldır. Bu nedenle, farklı kategorilerdeki veri sahiplerine ait kişisel veriler arasında mümkün olduğu ölçüde şu gibi ayrımlar yapılmalıdır: şüpheliler; cezai bir suçtan hüküm giymiş kişiler; mağdurlar ve tanıklar gibi diğer taraflar; alakalı bilgi veya irtibata sahip kişiler; şüpheli ve hükümlülerin ortakları. Bu, Adalet Divanı ve Avrupa İnsan Hakları Mahkemesi içtihadı tarafından yorumlandığı üzere Bildirge ve AİHS tarafından korunan masumiyet karinesinin uygulanmasına engel teşkil etmeyecektir.

(32) Yetkili makamlar doğru olmayan, eksik veya güncelliğini yitirmiş kişisel verilerin aktarılmamasını ve bunlara erişilmemesini sağlamalıdır. Yetkili makamlar gerçek kişilerin korunmasını sağlamak için, kişisel verilerin doğruluğu, tamlığı ya da güncelliği ve aktarılan veya erişilen kişisel verilerin güvenilirliği hususunda gerekli bilgileri tüm veri aktarımlarında, mümkün olduğunca, eklemelidir.

(33) İşbu Direktif'in, Üye Devlet hukukuna, bir hukuki dayanağa veya bir yasama önlemine atıf yapması, ilgili Üye Devlet'in anayasal düzeni uyarınca doğan gerekliliklere halel getirmediği sürece, her zaman parlamento tarafından kabul edilecek bir hukuki tasarruf gerektirmemektedir. Ancak, bu Üye Devlet hukuku, hukuki dayanak veya yasama önlemi, Adalet Divanı ve Avrupa İnsan Hakları Mahkemesi içtihadı gereğince açık ve net ve uygulaması ona tabi olanlar için öngörülebilir olmalıdır. İşbu Direktif kapsamında kişisel verilerin işlenmesini düzenleyen Üye Devlet, en azından hedefleri, işlenecek kişisel verileri, veri işlemenin amaçlarını ve kişisel verilerin bütünlüğünün ve mahremiyetinin korunmasında izlenecek usulleri ve yok edilmesine yönelik prosedürleri belirlemeli ve böylece istismar ve keyfiyet riskine karşı yeterli korumayı sağlamalıdır.

(34) Kişisel verilerin, yetkili makamlarca, kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amaçlarıyla işlenmesi, kişisel veriler veya

kişisel veri kümeleri üzerinde bu amaçlarla, otomatik yollarla veya başka türlü gerçekleştirilen toplama, kayıt, organizasyon, yapılanma, depolama, uyarlama veya değiştirme, geri alma, danışma, kullanım, hizalama veya kombinasyon, kısıtlama, silme veya imha etme gibi herhangi bir faaliyet veya faaliyet kümesini kapsamalıdır. Özellikle, işbu Direktif'te yer alan kurallar, kişisel verilerin işbu Direktif'e tabi olmayan bir alıcıya işbu Direktif'in amaçları doğrultusunda iletilmesinde uygulanmalıdır. Bu alıcı, gerçek veya tüzel kişiyi, resmi makamı, teşkilatı veya kişisel verilerin yetkili makam tarafından hukuka uygun olarak aktarıldığı diğer herhangi bir kuruluşu kapsamalıdır. Kişisel verilerin başlangıçta yetkili bir makam tarafından işbu Direktif'in amaçlarından biri için toplandığı durumlarda, bu verilerin işbu Direktif'in amaçları dışındaki amaçlar için işlenmesinde, bu işlemeye Birlik veya Üye Devlet hukuku tarafında yetki verildiği hallerde, 2016/679 (AB) sayılı Regülasyon uygulanmalıdır. Özellikle, kişisel verilerin işbu Direktif'in kapsamı dışındaki amaçlar için aktarılmasında 2016/679 (AB) sayılı Regülasyon kuralları uygulanmalıdır. Kişisel verilerin yetkili makam olmayan ya da işbu Direktif'in kastettiği anlamda öyle hareket etmeyen ve yetkili bir makam tarafından hukuka uygun kendisine aktarıldığı bir alıcı tarafından işlenmesi durumunda 2016/679 (AB) sayılı Regülasyon kuralları uygulanmalıdır. İşbu Direktif'i uygularken, Üye Devletler ayrıca, burada düzenlenen şartlara tabi olarak, 2016/679 (AB) sayılı Regülasyon kurallarının uygulanacağı daha öte halleri de belirtebilir olmalıdır.

(35) İşbu Direktif kapsamındaki veri işleme faaliyetinin hukuka uygun olması için, bu işleme, Birlik ya da Üye Devlet hukukuna dayalı yetkili bir makam tarafından kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amaçlarıyla kamu yararına gerçekleştirilecek bir görevin ifası için gerekli olmalıdır. Bu faaliyetler veri sahibinin hayati çıkarlarının korunmasını da kapsamalıdır. Cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması görevlerinin ifasının hukuken yetkili makamlara verilmesi, bu makamların gerçek kişilere yönelik taleplerine gerçek kişilerce uyulmasını zorunlu tutmasını ve buyurmasını sağlamaktadır. Böyle bir durumda, 2016/679 (AB) sayılı Regülasyon'da tanımlandığı üzere, veri sahibinin rızası kişisel verilerin yetkili makamlar tarafından işlenmesi için hukuki dayanak oluşturmamalıdır. Bir hukuki yükümlülüğe uyması gerektiği hallerde, veri sahibinin hakiki anlamda ve özgür bir seçim hakkı yoktur ki bu nedenle veri sahibinin tepkisi arzusunun özgürce ortaya konulmuş bir belirtisi olarak değerlendirilemeyecektir. Bu durum Üye Devletler'in, kanun ile, ceza soruşturmalarında DNA testleri ya da cezaların uygulanması kapsamında elektronik takip cihazlarının gözetimi gibi, veri sahibinin kişisel verilerinin işbu

Direktif'teki amaçlarla işlenmesine izin vermesini mümkün kılmasını sağlamasını engellememelidir.

(36) Birlik veya Üye Devlet hukukunun uygulanabilir olduğu veri aktaran yetkili makam, kişisel verilerin işlenmesinde iletim kodlarının kullanılması gibi özel durumlara uygulanabilir belirli şartlar öngördüğünde, Üye Devletler, veri aktaran yetkili makamın bu verilerin alıcısını bu şartlar ve bunlara uyulması gerekliliği hakkında bilgilendirmesini sağlamalıdır. Bu şartlar, örneğin kişisel verilerin başkalarına aktarılmasına ya da alıcıya aktarılma amaçlarından farklı amaçlarla kullanılmasına ya da bilgi edinme hakkının sınırlandığı hallerde veri aktaran yetkili makamın onayı olmadan veri sahibinin bilgilendirilmemesine yönelik bir yasak içerebilir. Bu yükümlülükler ayrıca veri aktaran yetkili makam tarafından üçüncü ülkelerde yer alan alıcılara ya da uluslararası kuruluşlara yönelik aktarımlarda da uygulanmalıdır. Üye Devletler, veri aktaran yetkili makamın bu şartları diğer Üye Devletler'de yer alan alıcılara veya bu yetkili makamın Üye Devlet'i içindeki benzer veri aktarımlarına uygulanabilir olanlardan başka ABİA Başlık 5'in 4'üncü ve 5'inci bölümleri uyarınca kurulmuş olan teşkilat, ofis ve kurumlara uygulamamasını temin etmelidir.

(37) Niteliği gereği özellikle temel hak ve özgürlükler açısından hassas olan kişisel veriler, işlendikleri bağlam temel hak ve özgürlüklere yönelik önemli riskler doğurabileceği için özel koruma gerektirmektedir. Bu kişisel veriler ırksal ve etnik kökeni ortaya koyan kişisel verileri de içermekte olup, işbu Direktif'te 'ırksal köken' ifadesinin kullanımı, Birlik'in farklı insan ırklarının varlığını ortaya koymaya çalışan teorileri kabulünü ima etmemektedir. Bu gibi kişisel veriler veri sahiplerinin kanun tarafından belirlenen hak ve özgürlüklerine yönelik uygun güvencelere tabi değilse işlenmemeli, ancak kanun tarafından yetki verilen hallerde işlenebilmelidir, böyle bir kanun ile öngörülmediği hallerde ise veri işleme veri sahibi ya da başka bir kişinin hayati çıkarlarını korumak için gerekli olduğu veya veri sahibi tarafından alenileştirildiği hallerde işlenebilecektir. Veri sahibinin hak ve özgürlüklerine yönelik uygun güvenlik tedbirleri söz konusu verileri sadece ilgili gerçek kişiye ait diğer verilerle bağlantılı olarak toplama imkanını, toplanan verileri yeterli seviyede güvende tutma imkanını, yetkili makamın çalışanlarının veriye erişimine dair daha sıkı kuralları ve söz konusu verilerin iletiminin yasaklanmasını içerebilir. Bu verilerin işlenmesine, özellikle veri sahibi kendisine yönelik müdahale teşkil eden veri işleme faaliyetine açık bir biçimde rıza gösterdiği hallerde de ancak kanun ile izin verilmelidir. Ancak, veri sahibinin rızası söz konusu hassas verilerin yetkili makam tarafından işlenmesinde tek başına bir hukuki dayanak oluşturmamalıdır.

(38) Veri sahibi münhasıran otomatik sistemler vasıtasıyla veri işlemeye dayalı ve olumsuz hukuki etkiler doğuran ya da kendisini önemli biçimde etkileyen kendisine ait kişisel özelliklere yönelik kararlara tabi olmama hakkına sahip olmalıdır. Her halükârda bu işleme, veri sahibine belirli bilgilerin sağlanması ve insan müdahalesi elde etme hakkı dahil, özellikle kendi bakış açısını ifade etme, bu değerlendirme neticesinde alınan karara yönelik bir açıklama elde etme veya söz konusu karara itiraz etme dahil olmak üzere uygun güvencelere tabi olmalıdır. Niteliği gereği temel hak ve özgürlükler açısından hassas olan kişisel verilere yönelik gerçek kişiler arasında ayrımcılığa sebep olacak profilleme faaliyetleri Bildirge'nin 21'inci ve 52'nci maddelerinde yer alan şartlar kapsamında yasaklanmış olmalıdır.

(39) Veri sahibinin haklarını kullanabilmesine imkân sağlamak amacıyla, veri sahibini bilgilendirme, veri sorumlusunun internet sitesindekiler dahil olmak üzere veri sahibi tarafından kolayca erişilebilir ve açık ve yalın bir dil kullanılmak suretiyle kolayca anlaşılabilir olmalıdır. Söz konusu bilgilendirme çocuklar gibi savunmasız konumdaki insanların ihtiyaçlarına yönelik olarak uyarlanmalıdır.

(40) Veri sahiplerinin işbu Direktif uyarınca kabul edilen hükümler kapsamındaki haklarının kullanılmasını kolaylaştırmak amacıyla talep mekanizmaları ve eğer uygulanabilirse, ücretsiz elde etme, özellikle kişisel verilere erişim, düzeltilmesini isteme ve silme dahil olmak üzere yöntemler sunulmalıdır. Veri sorumlusu, veri sahiplerinin haklarına işbu Direktif doğrultusunda sınırlamalar getirmiş olmadığı takdirde, veri sahiplerinin taleplerine gecikmeksizin yanıt verme yükümlülüğünde olmalıdır. Dahası, talepler açıkça mesnetsiz veya ölçüsüz ise, örneğin veri sahibi gerekçesiz ve sürekli olarak bilgi talebinde bulunuyorsa veya veri sahibi bilgi alma hakkını talepte bulunurken örneğin yanlış ya da aldatıcı bilgiler vermek suretiyle, istismar ediyorsa veri sorumlusu makul bir ücret talep etme ya da talebi karşılamama hakkına sahip olmalıdır.

(41) Veri sorumlusunun veri sahibinin kimliğini doğrulama amacıyla ilave bilgi sağlanmasını talep ettiği hallerde, söz konusu bilgi sadece bu belirli amaç için işlenmelidir ve söz konusu amacın yerine getirilmesi için gerekenden daha fazla bir süre için muhafaza edilmemelidir.

(42) Veri sahibine en azından şu bilgiler sağlanmalıdır: veri sorumlusunun kimliği, veri işleme faaliyetinin varlığı, veri işlemenin amaçları, şikayette bulunma hakkı ve veri sorumlusundan

kişisel verilere erişme, düzeltilmesini isteme veya silme talebinde bulunma hakkının varlığı. Bu bilgilendirme yetkili makamın internet sitesinde yapılabilecektir. İlaveten, özel durumlarda ve haklarının kullanımını sağlamak amacıyla, veri sahibi veri işlemenin hukuki dayanağına ve verilerin ne kadar süreliğine muhafaza edileceğine dair ve verilerin işlendiği özel durumlar göz önüne alınarak daha fazla bilgi sağlanması gerekmesi halinde veri sahibi açısından adil veri işlemenin temin edilmesi amacıyla bilgilendirilmelidir.

(43) Bir gerçek kişi kendisine ait toplanan verilere erişme hakkına sahip olmalı ve bu hakkı veri işleme faaliyetinin hukuka uygunluğunu teyit etmek ve farkında olmak amacıyla kolayca ve makul aralıklarla kullanabilmelidir. Dolayısıyla bütün veri sahipleri verilerin işlenme amaçlarını, verilerin işlendiği zaman dilimini ve üçüncü ülkelerde yer alanlar dahil olmak üzere verilerin alıcılarını bilme ve buna dair iletiler alma hakkına sahip olmalıdır. Bu iletilerin kişisel verilerin kaynağına yönelik bilgi içermesi halinde, bu bilgiler, özellikle de gizli kaynaklar söz konusu olduğunda, gerçek kişilerin kimliğini ortaya çıkarmamalıdır. Bu hak ile uyumun sağlanması için, veri sahibinin söz konusu veriye yönelik anlaşılabilir bir biçimde özete sahip olması gerekir. Bu, veri sahibinin söz konusu verilere yönelik farkındalığa sahip olması ve verilerin doğru olduğunu ve işbu Direktif ile uyumlu biçimde işlendiğini teyit edebilmesine imkân tanınması demektir; böylece veri sahibi kendisine işbu Direktif ile tanınan haklarını kullanabilecektir. Bu gibi bir özet, veri işleme faaliyetine tabi olan kişisel verilerin bir kopyası şeklinde sunulabilir.

(44) Üye Devletler; cezai suçların resmi ya da hukuki araştırmasının, soruşturmasının veya usul işlemlerinin engellenmesine ve; cezaya tabi suçların engellenmesinin, soruşturulmasının, tespitinin veya kovuşturmasının yahut cezaların etkilenmesine mani olmak, kamu veya ulusal güvenliğin korunması veya başkalarının hak ve özgürlüklerinin korunması amacıyla, bu gibi önlemler ilgili gerçek kişinin temel hakları ve meşru menfaatleri açısından demokratik bir toplumda gerekli ve orantılı önlemler teşkil ettiği müddetçe, veri sahiplerine bilgi verilmesini geciktiren, tamamen ya da kısmen sınırlayan adli önlemleri kabul edebilecektir. Veri sorumlusu her bir olayı somut ve tekil olarak ele alarak, erişme hakkının kısmen ya da tamamen sınırlandırılıp sınırlandırılmayacağını değerlendirmelidir.

(45) Erişim talebinin reddi ya da sınırlandırılmasına yönelik her türlü karar prensip olarak veri sahibine yazılı olarak bildirilmeli ve ilgili kararın dayandığı olgusal veya hukuki sebebi içermelidir.

(46) Adalet Divanı ve Avrupa İnsan Hakları Mahkemesi içtihadında yorumlandığı üzere veri sahibinin haklarına yönelik tüm sınırlamalar Bildirge ve AİHS ile uyum içerisinde olmalıdır ve özellikle buradaki hak ve özgürlüklerin ruhuna uygun olmalıdır.

(47) Bir gerçek kişi, özellikle gerçek olgulara dayandığı hallerde, kendisi hakkında doğru olmayan kişisel verileri düzelttirme ve söz konusu verilerin işlenmesi işbu Direktif'i ihlal ettiği hallerde silme hakkına sahip olmalıdır. Öte yandan, düzeltme hakkı örneğin bir tanık ifadesini, etkilememelidir. Bir gerçek kişi ayrıca kişisel verinin doğruluğuna itiraz ettiği veya doğru olup olmadığının kesin olarak saptanamadığı veya kişisel verilerin delil amacıyla tutulması gerektiği hallerde veri işlemenin sınırlandırılması hakkına da sahip olmalıdır. Özellikle, belirli bir olayda verilerin silinmesinin veri sahibinin meşru menfaatini etkileyeceğini düşündürecek haklı gerekçeler varsa kişisel verilerin silinmesi yerine veri işleme sınırlandırılmalıdır. Böyle bir durumda, sınırlanan veri sadece silmeyi engelleyen amaçla işlenmelidir. Kişisel verilerin işlenmesini sınırlandırmaya yönelik yöntemler, diğerlerinin yanında, seçili veriyi örneğin arşivleme amaçlarıyla başka bir işleme sistemine taşıma veya seçili veriyi erişimden kaldırmayı içerebilir. Otomatik kayıt sistemlerinde veri işlemenin sınırlandırılması prensip olarak teknik araçlarla sağlanmalıdır. Kişisel verilerin işlenmesinin sınırlandırıldığı sistem içerisinde açık bir biçimde belirtilmelidir. Kişisel verilerin bu düzeltilmesi veya silinmesi veya veri işlemenin sınırlandırılması verilerin açıklandığı alıcılara ve doğru olmayan verilerin ortaya çıktığı yetkili makamlara iletilmelidir. Veri sorumluları söz konusu verilerin daha fazla yayılmasından da kaçınmalıdır.

(48) Veri sorumlusunun veri sahibini bilgi edinme hakkı, kişisel verilere erişme veya düzeltilmesini ya da silinmesini isteme hakkı veya veri işlemenin sınırlandırılmasından mahrum bıraktığı hallerde veri sahibi ulusal denetleyici makamdan veri işlemenin hukuka uygunluğunu teyit etmesini isteyebilmelidir. Veri sahibi bu hakkına dair bilgilendirilmelidir. Denetleyici makamın veri sahibinin adına hareket ettiği hallerde, veri sahibi en azından tüm gerekli doğrulama veya incelemelerin denetleyici makam tarafından gerçekleştirildiğine dair denetleyici makam tarafından bilgilendirilmelidir. Denetleyici makam veri sahibini ayrıca yargı yoluna başvurma hakkı konusunda da bilgilendirmelidir.

(49) Kişisel verilerin bir cezai soruşturma ya da ceza işlemleri esnasında işlendiği hallerde, Üye Devletler bilgi alma hakkı, kişisel verilere erişim ya da kişisel verilerin düzeltilmesi veya silinmesi

hakkının ve veri işlemenin sınırlanmasının adli yargılama hususundaki ulusal kurallar ile uyum içerisinde yürütülmesini sağlayabilmelidir.

(50) Veri sorumlusunun, veri sorumlusu tarafından gerçekleştirilen ya da veri sorumlusu adına gerçekleştirilen tüm kişisel veri işleme faaliyetlerinden kaynaklanan sorumluluğu ve yükümlülüğü belirlenmelidir. Özellikle, veri sorumlusu uygun ve etkin önlemleri alma yükümlülüğünde olmalı ve veri işleme faaliyetlerinin işbu Direktif ile uyum içerisinde olduğunu kanıtlayabilmelidir. Bu gibi önlemler veri işlemenin niteliğini, kapsamını, bağlamını ve amaçlarını, ayrıca gerçek kişilerin hak ve özgürlüklerine yönelik riskleri göz önüne almalıdır. Veri sorumlusu tarafından alınan önlemler çocuklar gibi savunmasız gerçek kişilere ait kişisel verilerin ele alınmasına yönelik özel önlemlerin belirlenmesi ve uygulamasını da içermelidir.

(51) Özellikle veri işlemenin ayrımcılığa, kimlik hırsızlığına veya dolandırıcılığa, maddi zarara, itibarın zarar görmesine, meslek sırrı olarak korunan verilerin gizliliğinin kaybolmasına, maskelemenin izinsiz geri çevrilmesine veya diğer önemli ekonomik veya sosyal dezavantajlara yol açabileceği; veri sahiplerinin hak ve özgürlüklerinden veya kişisel verileri üzerinde kontrol sahibi olmaktan mahrum bırakılabileceği; ırk veya etnik köken, siyasi görüş, din veya felsefi inanç veya sendika üyeliğini ortaya koyan kişisel verilerin işlendiği; bir kişiyi münhasıran tanımlamak için genetik verilerin veya biyometrik verilerin işlendiği veya sağlığa ilişkin verilerin ya da cinsel yaşam ve cinsel yönelim veya cezai mahkumiyet ve suçlar veya ilgili güvenlik önlemleriyle ilgili verilerin işlendiği; kişisel profillerin oluşturulması veya kullanılması için özellikle işyerinde performans, ekonomik durum, sağlık, kişisel tercihler veya ilgi alanları, güvenilirlik veya davranış, konum veya hareketlerle ilgili hususların analiz edilmesi ve öngörülmesi gibi kişisel hususların değerlendirildiği; savunmasız gerçek kişilerin, özellikle de çocukların kişisel verilerinin işlendiği; veya veri işlemenin yüksek oranda kişisel veri içerdiği ve çok sayıda veri sahibini etkilediği durumlarda fiziksel, maddi veya maddi olmayan zararlara yol açabilecek veri işleme faaliyeti dolayısıyla gerçek kişilerin hak ve özgürlükleri üzerinde değişen olasılık ve önemde risk doğabilir.

(52) Riskin olasılığı ve ciddiyeti, işlemenin niteliği, kapsamı, içeriği ve amaçları dikkate alınarak belirlenmelidir. Risk, veri işleme faaliyetlerinin yüksek bir risk içerip içermediği tespit edilerek objektif bir değerlendirme çerçevesinde ölçülmelidir. Yüksek risk, veri sahiplerinin hak ve özgürlüklerine halel getirebilecek risktir.

(53) Kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin hak ve özgürlüklerinin korunması, işbu Direktif'in şartlarının yerine getirilmesini sağlamak için uygun teknik ve organizasyonel önlemlerin alınmasını gerektirir. Bu tür önlemlerin uygulanması yalnızca ekonomik hususlara bağlı olmamalıdır. İşbu Direktif'e uyulduğunu gösterebilmek adına veri sorumlusu, iç politika düzenlemelidir ve özellikle tasarımdan itibaren ve başlangıçtan itibaren veri koruma ilkelerine uygun önlemleri almalıdır. Veri sorumlusunun işbu Direktif uyarınca veri koruma etki değerlendirmesi yaptığı hallerde, sonuçlar bu önlem ve usuller geliştirilirken dikkate alınmalıdır. Önlemler, diğerlerinin yanı sıra en kısa zamanda maskelemenin kullanılmasından oluşmalıdır. Maskelemenin işbu Direktif'in amaçları doğrultusunda kullanılması, özellikle özgürlük, güvenlik ve adalet alanında kişisel verilerin serbest akışını kolaylaştıracak bir araç olarak hizmet edebilir.

(54) Denetim makamlarının izlemesi ve önlemleriyle ilgili olarak veri sorumlusu ve veri işleyenlerin sorumluluklarının ve yükümlülüklerinin yanı sıra veri sahiplerinin hak ve özgürlüklerinin korunması, işbu Direktif'te belirtilen veri sorumlusunun, diğer veri sorumlularıyla ortak olarak işlemenin amaçlarını ve araçlarını belirlediği veya veri sorumlusu adına bir veri işleme faaliyetinin gerçekleştirildiği durumlar dahil olmak üzere sorumlulukların açıkça belirtilmesini gerektirir.

(55) Bir veri işleyen tarafından veri işlemesinin gerçekleştirilmesi, veri işleyeni veri sorumlusuna bağlayan bir sözleşmeyi içeren ve özellikle veri işleyenin yalnızca veri sorumlusunun talimatlarına göre hareket etmesini şart koşan bir hukuki tasarrufa tabi olmalıdır. Veri işleyen, tasarımdan itibaren ve başlangıçtan itibaren veri koruma ilkesini dikkate almalıdır.

(56) İşbu Direktif'e uyulduğunu göstermek adına, veri sorumlusu veya veri işleyen, kendi sorumluluğu altındaki tüm veri işleme faaliyeti kategorilerine ilişkin kayıtları tutmalıdır. Veri sorumlusu ve veri işleyenlerin her biri, denetim makamı ile iş birliği yapmak ve veri işleme faaliyetlerinin izlenmesine hizmet etmesi adına bu kayıtları talep üzerine hazır bulundurmak zorundadır. Otomatik olmayan yollarla kişisel veri işleyen veri sorumlusu veya veri işleyen, veri işlemenin yasallığını göstermek, öz izlemeyi sağlamak ve veri bütünlüğünü ve veri güvenliğini sağlamak adına log kayıtları veya diğer kayıt biçimleri gibi etkili yöntemlere sahip olmalıdır.

(57) Log kayıtları, en azından toplama, değiştirme, danışma, aktarım dahil ifşa etme, birleştirme veya silme gibi otomatik veri işleme sistemlerinde yapılan işlemler için tutulmalıdır. Kişisel verilere

erişen veya ifşa eden kişinin kimliği kayıt altına alınmalı ve bu kimlik belirlemesinden veri işleme faaliyetinin gerekçesinin belirlenmesi mümkün olmalıdır. Log kayıtları yalnızca veri işlemenin ve öz izlemenin hukukiliğinin tasdik edilmesi, veri bütünlüğünün ve veri güvenliğinin ve cezai işlemlerin sağlanması adına kullanılmalıdır. Öz izleme ayrıca yetkili makamların iç disiplin soruşturmalarını da içermektedir.

(58) Veri işleme faaliyetinin, niteliği, kapsamı veya amaçları nedeniyle veri sahiplerinin hak ve özgürlükleri için yüksek risk oluşturabileceği durumlarda veri sorumlusu tarafından, özellikle kişisel verilerin korunmasını sağlamak ve işbu Direktif'e uygunluğu göstermek için öngörülen önlem, koruma ve mekanizmaları içeren bir veri koruma etki değerlendirmesi yapılmalıdır. Etki değerlendirmeleri, münferit olayları değil veri işleme faaliyetlerinin ilgili sistem ve süreçlerini kapsamalıdır.

(59) Veri sahiplerinin hak ve özgürlüklerinin etkin bir şekilde korunmasını sağlamak adına, veri sorumlusu veya veri işleyen, bazı durumlarda veri işlemeden önce denetim makamına danışmalıdır.

(60) Güvenliği sağlamak ve işbu Direktif'i ihlal eden veri işleme faaliyetlerini engellemek adına, veri sorumlusu ve veri işleyen veri işlemenin doğasında olan riskleri değerlendirmeli ve şifreleme gibi bu riskleri azaltacak önlemleri almalıdır. Bu tür önlemler, mahremiyet dahil uygun bir güvenlik seviyesi sağlamalı ve teknolojinin durumunu, riske ilişkin uygulama maliyetlerini ve korunacak kişisel verilerin niteliğini dikkate almalıdır. Veri güvenliği riskleri değerlendirilirken, kişisel verilerin yanlışlıkla veya hukuka aykırı imha edilmesi, kaybedilmesi, değiştirilmesi veya izinsiz ifşa edilmesi veya özellikle fiziksel, maddi veya gayrı maddi hasara yol açacak şekilde iletilen, saklanan veya başka bir şekilde işlenen kişisel verilere erişilmesi gibi veri işlemeden kaynaklanan risklerin dikkate alınması gerekmektedir. Veri sorumlusu ve veri işleyen, kişisel veri işleme faaliyetinin yetkisiz kişiler tarafından yürütülmemesini sağlamalıdır.

(61) Kişisel veri ihlali, uygun bir şekilde ve zamanında bildirilmemesi halinde, gerçek kişilerin kendi kişisel verileri üzerindeki kontrolü kaybetme, haklarının sınırlanması, ayrımcılık, kimlik hırsızlığı ve sahtecilik, maddi hasar, maskelemenin izinsiz olarak geri çevrilmesi, itibar kaybı, mesleki sır olarak korunan kişisel verinin gizliliğinin kaybedilmesi veya ilgili gerçek kişinin uğrayacağı diğer önemli ekonomik veya sosyal dezavantajlar gibi fiziksel, maddi veya gayrı maddi hasarlara yol açılır. Bu nedenle, veri sorumlusu kişisel bir veri ihlali gerçekleştiğinin

farkına varır varmaz, hesap verebilirlik ilkesine uygun olarak, kişisel veri ihlalinin gerçek kişilerin hak ve özgürlükleri üzerinde bir risk yaratmadığını katlayamadığı sürece, veri sorumlusu kişisel veri ihlalini, gecikmeksizin ve mümkünse durumdan haberdar olduktan sonra en geç 72 saat içinde denetim makamına bildirmelidir. Bu tür bir bildirimin 72 saat içinde yapılamaması durumunda, gecikme nedenleri ile birlikte bildirim yapılmalıdır ve bilgi daha fazla bir gecikme olmadan aşamalar halinde sağlanabilir.

(62) Kişisel veri ihlalinin gerçek kişilerin hak ve özgürlükleri üzerinde yüksek bir risk oluşturmasının muhtemel olduğu durumlarda, gerekli tedbirleri alabilmeleri için gerçek kişiler gecikmeksizin bilgilendirilmelidir. İletişim, kişisel veri ihlalinin niteliğini tanımlamalı ve olası olumsuz etkileri azaltmak adına ilgili gerçek kişi için öneriler içermelidir. Veri sahipleriyle yapılan iletişim, denetleyici makam ile yakın iş birliği içinde ve bu makam veya diğer ilgili makamlar tarafından verilen rehberliğe uygun olarak, mümkün olan en kısa sürede yapılmalıdır. Örneğin, ani bir zarar riskini azaltma ihtiyacı, veri sahipleriyle hızlı bir şekilde iletişim kurulmasını gerektirir; buna karşın, devam eden veya benzeri veri ihlallerine karşı uygun önlemlerin uygulanması ihtiyacı iletişim için daha fazla zaman gerektirebilir. Resmi veya yasal tahkikatlar, soruşturmalar veya prosedürlerin engellenmesinden kaçınılması, suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazına halel gelmesinden kaçınılması, kamu güvenliğini korumak, ulusal güvenliği korumak veya başkalarının hak ve özgürlüklerini korumak gibi faaliyetler, veri ihlali hakkında ilgili gerçek kişiler ile yapılacak iletişimin ertelenmesi veya kısıtlanması halinde gerçekleştirilemez, istisnai durumlarda bu iletişim ihmal edilebilir.

(63) Bir Üye Devlet'in yargı yetkisini kullanırken mahkemeleri ve diğer bağımsız yargı makamlarını muaf tutmaya karar vermesi durumu hariç olmak üzere, veri sorumlusu, işbu Direktif uyarınca kabul edilen hükümler ile iç uyumu denetlemesinde kendisine yardımcı olacak bir kişi belirlemelidir. Bu kişi, veri sorumlusunun mevcut personelinin veri koruma alanında uzman bilgisi edinmek için veri koruma hukuku ve uygulamasında özel eğitim almış bir üyesi olabilir. Gerekli uzman bilgisi seviyesi, özellikle yürütülen veri işleme faaliyetine ve veri sorumlusu tarafından işlenen kişisel veriler için gereken korumaya göre belirlenmelidir. Bu kişi, görevini, yarı zamanlı veya tam zamanlı olarak gerçekleştirilebilir. Bir veri koruma görevlisi, örneğin merkezi birimlerdeki ortak kaynakların söz konusu olduğunda, organizasyon yapıları ve büyüklükleri dikkate alınarak birkaç veri sorumlusu tarafından ortak olarak atanabilir. Bu kişi ayrıca ilgili veri sorumlularının yapısı içerisinde farklı pozisyonlara atanabilir. Bu kişi, veri

sorumlusuna ve kişisel veri işleyen çalışanlara, ilgili veri işleme yükümlülüklerini yerine getirip getirmediklerini bildirerek ve onlara tavsiyelerde bulunarak yardım etmelidir. Bu tür veri koruma görevlileri, vazife ve görevlerini Üye Devlet hukukuna uygun olarak bağımsız bir şekilde yerine getirebilecek konumda olmalıdırlar.

(64) Üye Devletler, üçüncü bir ülkeye veya bir uluslararası kuruluşa aktarım, yalnızca kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı için gerekli olduğunda gerçekleştirilmelidir ve üçüncü bir ülke veya uluslararası kuruluştaki veri sorumlusu işbu Direktif kapsamında yetkili bir makamdır. Veri işleyenlere açıkça veri sorumluları adına aktarımda bulunma talimatı verildiği durumlar haricinde, aktarım yalnızca veri sorumlusu olarak hareket eden yetkili makamlar tarafından gerçekleştirilmelidir. Bu tür bir aktarım, Komisyon'un, söz konusu üçüncü ülke veya uluslararası kuruluşun, uygun korumaların sağlandığı veya belirli durumlar için istisnaların geçerli olduğu durumlarda yeterli düzeyde koruma sağladığına karar vermesi durumunda gerçekleşebilir. Kişisel verilerin Birlik'ten veri sorumlularına, veri işleyenlere veya üçüncü ülkelerdeki veya uluslararası kuruluşlardaki diğer alıcılara aktarıldığı durumlarda, kişisel verilerin üçüncü ülke ya da uluslararası kuruluş tarafından aynı ya da başka bir üçüncü ülke ya da uluslararası kuruluştaki veri sorumlularına ya da veri işleyenlere ileriye yönelik aktarılması durumları dahil olmak üzere işbu Direktif tarafından Birlik adına gerçek kişiler için sağlanan korunma seviyelerine zarar verilmemelidir.

(65) Kişisel verilerin bir Üye Devlet'ten üçüncü ülkelere veya uluslararası kuruluşlara aktarılması durumunda, böyle bir aktarım kural olarak, yalnızca verinin elde edildiği Üye Devlet'in aktarıma izin vermesinden sonra gerçekleştirilmelidir. Etkin kolluk iş birliğinin çıkarları, bir Üye Devlet'in veya üçüncü bir ülkenin kamu güvenliğine veya bir Üye Devlet'in temel çıkarlarına yönelik bir tehdidin niteliği, önceden izin almayı imkânsız kılacak kadar acil olduğu durumlarda, yetkili makamın, ilgili kişisel bir bilgiyi, önceden bir izin almadan, ilgili üçüncü ülkeye veya ilgili uluslararası kuruma aktarabilmesini gerektirir. Üye Devletler, aktarımla ilgili her türlü özel koşulun üçüncü ülkelere veya uluslararası organizasyonlara iletilmesini sağlamalıdır. Kişisel verilerin ileriye yönelik aktarımları, asıl aktarımı gerçekleştiren yetkili makamın önceden vereceği izne tabi olmalıdır. İleriye yönelik bir aktarımın onaylanması talebine karar verirken, asıl aktarımı gerçekleştiren yetkili makam, suçun ciddiyeti, asıl aktarılan verinin tabi olduğu özel koşulları ve amacını, cezanın uygulanmasının niteliği ve kişisel verilerin ileriye yönelik

aktarılacağı üçüncü ülke veya uluslararası kuruluştaki kişisel veri korunması düzeyi dahil olmak üzere tüm ilgili faktörleri dikkate almalıdır. Asıl aktarımı gerçekleştiren yetkili makam, ileriye yönelik aktarımı belirli koşullara tabi tutabilmelidir. Bu özel koşullar, örneğin işleme kurallarında tanımlanabilir.

(66) Komisyon, Birlik genelinde etki doğuracak şekilde, bazı üçüncü ülkelerin, bir bölgenin veya bir üçüncü ülke içindeki belirli bir veya daha fazla bölümün veya uluslararası bir organizasyonun, yeterli düzeyde veri koruması sunduğuna karar verebilmelidir, böylelikle, bu düzeyde bir koruma sağladığı düşünülen üçüncü ülkeler veya uluslararası kuruluşlarla ilgili Birlik genelinde hukuki belirlilik ve yeknesaklık sağlanır. Bu gibi durumlarda, kişisel verilerin bu ülkelere aktarımı, verinin elde edildiği başka bir Üye Devlet'in aktarım için izin vermesinin zorunlu olduğu durum haricinde, özel bir izin alma zorunluluğu olmaksızın gerçekleşebilmelidir.

(67) Birlik'in üzerinde kurulduğu temel değerler, özellikle de insan haklarının korunması doğrultusunda, Komisyon, üçüncü bir ülke veya üçüncü bir ülke içindeki bir bölge ya da belirli bir bölümü değerlendirirken, bu üçüncü ülkenin, hukukun üstünlüğüne, adalete erişimin yanı sıra uluslararası insan hakları norm ve standartlarına ve kamu güvenliği, savunma ve ulusal güvenlik ile ilgili mevzuata ve kamu düzeni ve ceza hukuku dahil olmak üzere genel ve özel yasalara uyup uymadığına dikkat etmelidir. Üçüncü bir ülke içindeki bir bölge veya belirli bir bölüm ile ilgili olarak bir yeterlilik kararı kabul edilirken, belirli işleme faaliyetleri ve üçüncü ülkede yürürlükte olan geçerli yasal standartların ve mevzuatın kapsamı gibi açık ve nesnel kriterler dikkate alınmalıdır. Üçüncü ülke, özellikle verinin bir veya birkaç belirli bölümde işlendiği durumlarda, özellikle Birlik içinde sağlanan ile eşdeğer düzeyde yeterli seviyede koruma sağlayan garantiler sunmalıdır. Özellikle, üçüncü ülke, etkili bağımsız veri koruma denetimi sağlamalı ve Üye Devletler'in veri koruma makamlarıyla iş birliği mekanizmaları sağlamalıdır ve veri sahiplerine etkin ve uygulanabilir haklar ve etkili idari ve adli çözümler sunulmalıdır.

(68) Üçüncü ülke veya uluslararası kuruluşun verdiği uluslararası taahhütler dışında, Komisyon, özellikle kişisel verilerin korunmasına ilişkin olarak üçüncü ülkelerin veya uluslararası kuruluşların çok taraflı veya bölgesel sistemlere katılımından kaynaklanan yükümlülükleri ve bunun yanında bu yükümlülükleri uygulamasını dikkate almalıdır. Özellikle üçüncü ülkenin, Kişisel Verilerin Otomatik İşlenmesi ve Bireylerin Korunması Hakkında 28 Ocak 1981 tarihli Avrupa Konseyi Antlaşması ile Ek Protokolü'ne katılımı dikkate alınmalıdır. Komisyon,

üçüncü ülkelerdeki veya uluslararası kuruluşlardaki koruma düzeyini değerlendirirken, 2016/679 (AB) sayılı Regülasyon ile kurulan Avrupa Veri Koruma Kurulu'na ("**Kurul**") danışmalıdır. Komisyon ayrıca, 2016/679 (AB) sayılı Regülasyon'un 45'inci maddesi uyarınca kabul edilen ilgili herhangi bir Komisyon yeterlilik kararını da dikkate almalıdır.

(69) Komisyon, üçüncü bir ülkede, bir bölgedeki veya üçüncü bir ülke içindeki belirli bir bölümdeki veya bir uluslararası kuruluştaki koruma düzeyine ilişkin kararların işleyişini izlemelidir. Yeterlilik kararlarında Komisyon, bunların işleyişleri için bir periyodik gözden geçirme mekanizması oluşturmalıdır. Bu periyodik gözden geçirme, söz konusu üçüncü ülke veya uluslararası kuruluşa danışılarak gerçekleştirilmelidir ve üçüncü ülke veya uluslararası kuruluştaki tüm ilgili gelişmeler dikkate alınmalıdır.

(70) Komisyon ayrıca, üçüncü bir ülke, bir bölge veya bir üçüncü ülke içindeki belirli bir bölüm veya uluslararası bir organizasyonun artık yeterli düzeyde veri koruması sağlamadığını fark edebilmelidir. Sonuç olarak, belirli durumlar için uygun koruma önlemleri ve istisnalara tabi aktarımlara ilişkin işbu Direktif'te yer alan şartlar yerine getirilmedikçe, kişisel verilerin söz konusu üçüncü ülke veya uluslararası kuruluşa aktarılması yasaklanmalıdır. Komisyon ile bu üçüncü ülkeler veya uluslararası kuruluşlar arasındaki müzakere prosedürleri için hükümler oluşturulmalıdır. Komisyon, nedenlerini üçüncü ülke veya uluslararası kuruluşlara zamanında bildirmeli ve durumu düzeltmek için bunlarla müzakerelerde bulunmalıdır.

(71) Böyle bir yeterlilik kararına dayanmayan aktarımlara sadece, kişisel verilerin korunmasını sağlayan yasal olarak bağlayıcı araçla uygun korumanın sağlandığı veya veri sorumlusunun veri aktarımını çevreleyen tüm koşulları değerlendirdiği ve bu değerlendirme temelinde mevcut kişisel verilerin korunmasına ilişkin uygun korumaların sağlandığının kabul edildiği durumlarda izin verilmelidir. Bu tür yasal olarak bağlayıcı araçlar, örneğin Üye Devletler tarafından akdedilen ve yasal düzenlerinde uygulanan ve veri sahipleri tarafından uygulanabilen, veri koruma gereklilikleri ve etkili idari veya adli tazminat alma hakkı dahil olmak üzere veri sahiplerinin haklarına uygunluğu sağlayan yasal olarak bağlayıcı olan ikili anlaşmalar olabilir. Veri sorumlusu, veri aktarımını çevreleyen tüm koşulların değerlendirmesini yaparken Europol veya Eurojust ile üçüncü ülkeler arasında akdedilen kişisel verilerin değişimini sağlayan iş birliği anlaşmalarını dikkate alabilmelidir. Veri sorumlusu ayrıca, verinin aktarım amaçlarından başka amaçlarla işlenmemesini sağlayarak kişisel verilerin aktarımının gizlilik yükümlülüklerine ve belirlilik ilkelerine tabi olacağı gerçeğini de dikkate almalıdır. Buna ek olarak, veri sorumlusu,

kişisel verilerin, ölüm cezası ya da herhangi bir zalim ve insanlık dışı muamelenin talep edilmesi, karar verilmesi ya da icra edilmesi için kullanılmayacağını dikkate almalıdır. Bu koşullar, verilerin aktarılmasına izin veren uygun güvenlik önlemleri olarak kabul edilebilirken, veri sorumlusu ek koruma talep edebilmelidir.

(72) Yeterlilik kararı veya uygun korumaların bulunmadığı durumlarda; veri sahibinin veya başka bir kişinin hayati çıkarlarını veya kişisel veri aktarımı yapan Üye Devlet hukukunun öngördüğü halde veri sahiplerinin meşru çıkarlarını korumak için gerekli olduğunda; bir Üye Devlet'in veya üçüncü bir ülkenin kamu güvenliğine yönelik yakın ve ciddi bir tehlikenin önlenmesi için; kamu güvenliğine karşı tehditlerden korunma ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla münferit bir durumda; veya hukuki iddiaların oluşturulması, ileri sürülmesi veya savunulması için münferit bir durumda; sadece belirli durumlarda aktarım veya bir aktarım kategorisi gerçekleştirilebilir. Bu istisnalar sınırlayıcı biçimde yorumlanmalı ve kesinlikle gerekli olan verilerle sınırlı olmak üzere kişisel verilerin sık, büyük ve yapısal aktarımlarına veya verilerin büyük ölçekli aktarımlarına izin vermemelidir. Bu tür aktarımlar belgelenmeli ve talep üzerine aktarımın hukuka uygunluğunu takip edebilmeleri için denetim makamına sunulmalıdır.

(73) Üye Devletler'in yetkili makamları, mevzuatın verdiği görevlerini yerine getirmelerini sağlayacak ilgili bilgileri alabilmek adına, cezai konularda adli iş birliği ve polis iş birliği alanında üçüncü ülkelerle akdettikleri yürürlükteki iki taraflı veya çok taraflı uluslararası anlaşmaları uygular. Kural olarak, bu, bazen iki taraflı ya da çok taraflı bir uluslararası anlaşmanın olmadığı durumlarda bile, işbu Direktifin amaçları kapsamında ilgili üçüncü ülkelerdeki yetkili makamlar aracılığıyla ya da en azından bunların iş birliği yapmasıyla gerçekleşir. Bununla birlikte, belirli münferit durumlarda, üçüncü ülkede böyle bir makam ile iletişim kurulması için gerekli olan olağan usuller, özellikle aktarımın zamanında gerçekleştirilemeyeceği veya üçüncü ülkedeki makamın hukuk devletine veya uluslararası insan hakları normlarına ve standartlarına saygı göstermediği durumlarda etkisiz veya uygunsuz olabilir. Bu halde, Üye Devletler'in yetkili makamları kişisel verileri bu üçüncü ülkelerde kurulu alıcılara doğrudan aktarmaya karar verebilirler. Bu durum, ceza gerektiren bir suçun mağduru olma tehlikesi altında bulunan bir kişinin hayatını kurtarmak veya terör de dahil olmak üzere yakın bir suçun işlenmesini önlemek maksadıyla kişisel verilerin aktarılmasının acil bir ihtiyaç olduğu bir durum olabilir. Yetkili makamlar ve üçüncü ülkelerde kurulu alıcılar arasında böyle bir aktarım, yalnızca belirli münferit durumlarda yapılsa bile, işbu Direktif, bu tür durumları düzenlemeye ilişkin şartları

göstermelidir. Bu şartlar, cezai konularda adli iş birliği alanındaki ve kolluk kuvvetleri ile iş birliği alanındaki mevcut iki taraflı veya çok taraflı uluslararası anlaşmaların istisnası olarak değerlendirilmemelidir. Bu kurallar, işbu Direktif'in diğer kurallarına ek olarak, özellikle işlemenin yasallığı ve Bölüm 5 ile ilgili olanlar için uygulanmalıdır.

(74) Kişisel verilerin sınırlar arasında taşınması halinde, gerçek kişilerin kendilerini bu verilerin hukuka aykırı kullanımından veya ifşasından korumaları için veri koruma haklarını kullanma yeterliliğine ilişkin risk artabilir. Aynı zamanda, denetim makamları, sınırları dışındaki şikayetleri takip edemeyebilir veya sınırları dışındaki faaliyetlerle ilgili soruşturma yürütemeyebilir. Sınır ötesi bağlamda birlikte çalışma çabaları, önleyiciliği veya telafi ediciliği yetersiz yetkiler ve tutarsız hukuki rejimler tarafından da engellenebilir. Bu nedenle, veri koruma denetim makamları arasında yabancı meslektaşlarıyla bilgi alışverişinde bulunmalarına yardımcı olmak için daha yakın bir iş birliğini teşvik etme ihtiyacı vardır.

(75) Üye Devletler'de görevlerini tam bağımsızlıkla yerine getirebilen denetim makamlarının kurulması, gerçek kişilerin kişisel verilerinin işlenmesi konusunda korunmasının temel bir bileşenidir. Denetim makamları, işbu Direktif uyarınca kabul edilen hükümlerin uygulamasını izlemeli ve gerçek kişilerin kişisel verilerinin işlenmesiyle ilgili olarak korunması için Birlik genelinde tutarlı uygulamalarına katkıda bulunmalıdır. Bu amaçla, denetim makamları birbirleriyle ve Komisyon ile iş birliği yapmalıdır.

(76) Üye Devletler, 2016/679 (AB) sayılı Regülasyon kapsamında halihazırda kurulmuş olan bir denetim makamını, işbu Direktif kapsamında kurulacak olan ulusal denetim makamları tarafından yapılacak görevlerin sorumluluğunu üstlenme konusunda görevlendirebilirler.

(77) Üye Devletler anayasal, organizasyonel ve idari yapılarını yansıtacak şekilde birden fazla denetim makamı oluşturabilmelidir. Her denetim makamına, Birlik'teki diğer denetim makamları ile karşılıklı yardımlaşma ve iş birliği ile ilgili görevler de dahil olmak üzere, görevlerini etkin bir şekilde yerine getirmeleri için gerekli olan finansal kaynaklar ve insan kaynakları, tesisler ve altyapı sağlanmalıdır. Her bir denetim makamı, genel devlet bütçesinin veya ulusal bütçenin bir parçası olabilecek ayrı, kamuya açık bir yıllık bütçeye sahip olmalıdır.

(78) Denetim makamları, mali harcamalarına ilişkin bağımsız kontrol veya izleme mekanizmalarına, bu mali kontrolün bağımsızlıklarını etkilememesi koşuluyla, tabi olmalıdır.

(79) Denetim makamının üyesi veya üyeleri için genel şartlar, Üye Devlet hukukuna göre belirlenmeli ve özellikle bu üyelerin bir parlamento veya hükümet veya hükümetin ya da hükümet üyesinin ya da parlamentonun ya da bunun bir meclisinin teklifi üzerine Üye Devlet'in Devlet Başkanı veya Üye Devlet hukuku tarafından şeffaf bir prosedür sonucunda görevlendirilen bağımsız bir organ tarafından atanmasını sağlamalıdır. Denetim makamının bağımsızlığını sağlamak adına, üye veya üyeler bütünlük içerisinde hareket etmeli, görevleriyle uyuşmayan herhangi bir eylemden kaçınmalı ve görev süreleri boyunca – kazançlı olsun veya olmasın – uyumsuz işlerde bulunmamalıdır. Çalışanlar, denetim makamının bağımsızlığını sağlamak adına, Üye Devlet hukuku tarafından görevlendirilen bağımsız bir organ tarafından müdahaleyi içerebilmesi kaydıyla, denetim makamı tarafından seçilmelidir.

(80) İşbu Direktif, ulusal mahkemelerin ve diğer adli makamların faaliyetleri için de uygulansa bile, denetim makamlarının yetkisi, hakimlerin hukuki görevlerini yerine getirmeleri sırasındaki bağımsızlıklarını korumaları için, mahkemelerin hukuki yetkilerine dayanarak hareket ettiği durumlarda kişisel verilerin işlenmesini kapsamamalıdır. Bu muafiyet, mahkemede görülen davalardaki hukuki faaliyetlerle sınırlandırılmalıdır ve hakimlerin Üye Devlet hukukuna uygun olarak dahil olabileceği diğer faaliyetlere genişletilmemelidir. Üye Devletler ayrıca, denetim makamının yetkisinin, örneğin Cumhuriyet savcılığı gibi makamların hukuki yetkilerine uygun hareket ederken diğer bağımsız yargı makamlarının kişisel verilerini işlemesini kapsamamasını sağlayabilmelidir. Her durumda, işbu Direktif'in kurallarına mahkemeler ve diğer bağımsız adli makamlar tarafından uyulması, Bildirge'nin 8'inci maddesinin 3'üncü fıkrası uyarınca her zaman bağımsız denetime tabidir.

(81) Her denetim makamı, herhangi bir veri sahibi tarafından iletilen şikâyetler ile ilgilenmeli ve konuyu soruşturmalı ya da konuyu yetkili denetim makamına iletmelidir. Bir şikâyeti takiben yapılacak soruşturma, yargı denetimine tabi olarak, ilgili özel durum için uygun olan ölçüde yapılmalıdır. Denetim makamı, veri sahibini, şikâyet ile ilgili gelişmeler ve şikâyetin sonucu hakkında makul bir süre içinde bilgilendirmelidir. Durumun daha fazla araştırma ya da başka bir denetim makamı ile koordinasyon gerektirmesi halinde, veri sahibine ara bilgi verilmelidir.

(82) İşbu Direktif ile uyumun ve Adalet Divanı tarafından yorumlandığı şekliyle ABİA kapsamında Birlik içinde uygulanmasının etkili, güvenilir ve sürekli bir şekilde izlenmesi adına, denetim makamları, her Üye Devlet'te, aynı görevlere ve görevlerini yerine getirmeleri için gerekli olan

soruşturmaya, düzeltmeye ve tavsiye vermeye ilişkin yetkiler de dahil olmak üzere aynı etkin yetkilere sahip olmalıdır. Bununla birlikte, yetkileri, ceza gerektiren suçların soruşturulması ve kovuşturulması veya yargının bağımsızlığı dahil olmak üzere, ceza yargılamasına dair belirli kurallara müdahale etmemelidir. Üye Devlet hukukuna göre savcılık makamlarının yetkilerine halel getirmeksizin, denetim makamları, işbu Direktif'e ilişkin ihlalleri adli makamların dikkatine sunma veya adli işlemlerde bulunma yetkisine de sahip olmalıdır. Denetim makamlarının yetkileri, Birlik ve Üye Devlet hukuku tarafından belirlenen uygun usul güvencelerine göre, tarafsız, adil ve makul bir süre içerisinde kullanılmalıdır. Özellikle, alınacak her bir tedbir, işbu Direktif'e uyulmasını sağlamak için uygun, gerekli ve orantılı olacak şekilde, her bir vakanın koşulları göz önünde bulundurularak, kişileri olumsuz yönde etkileyebilecek herhangi bir bireysel önlem alınmadan önce her bir ilgili kişinin dinlenme hakkına saygı gösterilerek, gereksiz masraflardan ve ilgili kişiye aşırı rahatsızlık verilmesinden kaçınılarak alınmalıdır. Mülklere erişim ile ilgili soruşturma yetkileri, daha önce yargı mercilerinden izin alınması şartı gibi, Üye Devlet hukukundaki özel şartlara uygun olarak kullanılmalıdır. Yasal olarak bağlayıcı bir kararın kabul edilmesi, kararı kabul eden denetim makamının Üye Devleti'nde yargı denetimine tabi olmalıdır.

(83) Denetim makamları, işbu Direktif uyarınca kabul edilen hükümlerin tutarlı bir şekilde uygulanmasını ve yürütülmesini sağlamak üzere, görevlerini yerine getirmede birbirlerine yardım etmelidir ve karşılıklı yardımlaşma sağlamalıdır.

(84) Kurul, Komisyon'a tavsiyelerde bulunmak ve Birlik genelinde denetim makamlarının iş birliğini teşvik etmek de dahil olmak üzere, işbu Direktif'in Birlik genelinde tutarlı bir şekilde uygulanmasına katkıda bulunmalıdır.

(85) Her veri sahibi, bir denetim makamı nezdinde şikâyette bulunma hakkına ve işbu Direktif uyarınca kabul edilen hükümler bağlamında haklarının ihlal edildiğini düşündüğü veya denetim makamının şikâyete rağmen harekete geçmediği, bir şikayeti kısmen veya tamamen reddettiği veya düşürdüğü veya veri sahibinin haklarını korumak için bu tür bir eylemin gerekli olduğu hallerde harekete geçmediği durumlarda Bildirge'nin 47'nci maddesi uyarınca etkili bir kanun yoluna başvurma hakkına sahip olmalıdır. Bir şikâyeti takiben yapılacak soruşturma, yargı denetimine tabi olarak, ilgili özel durum için uygun olan ölçüde yapılmalıdır. Yetkili denetim makamı, veri sahibini, şikâyet ile ilgili gelişmeler ve şikâyetin sonucu hakkında makul bir süre içinde bilgilendirmelidir. Durumun daha fazla araştırma ya da başka bir denetim makamı ile

koordinasyon gerektirmesi halinde, veri sahibine ara bilgi verilmelidir. Şikayetlerin sunulmasını kolaylaştırmak için, her bir denetim makamı, diğer iletişim araçlarını hariç tutmaksızın, elektronik olarak da doldurulabilecek bir şikâyet başvuru formu sağlama gibi önlemler almalıdır.

(86) Her bir gerçek ve tüzel kişi, denetim makamının kendisi ile ilgili hukuki sonuçlar doğuran bir kararına karşı yetkili ulusal mahkeme önünde etkili bir kanun yoluna başvurma hakkına sahip olmalıdır. Bu karar, özellikle, denetim makamının soruşturmaya, düzeltmeye ve tavsiye vermeye ilişkin yetkilerini kullanması veya şikayetleri reddetmesi veya düşürmesi ile ilgilidir. Ancak, bu hak, denetim makamı tarafından verilen görüşler veya tavsiyeler gibi yasal olarak bağlayıcı olmayan diğer denetim makamı önlemlerini kapsamaz. Bir denetim makamına karşı yürütülecek işlemler, denetim makamının kurulu olduğu Üye Devlet mahkemelerinde yapılmalı ve Üye Devlet hukukuna göre yürütülmelidir. Bu mahkemeler, önüne gelen ihtilafla ilgili tüm maddi ve hukuki sorunları incelemeye tam yetkili olmalıdır.

(87) Bir veri sahibi, işbu Direktif kapsamındaki haklarının ihlal edildiğini düşündüğü takdirde, kişisel verilerinin korunmasına ilişkin veri sahibinin haklarını ve çıkarlarını korumayı amaçlayan ve Üye Devlet hukukuna göre oluşturulmuş bir organı, ilgili denetim makamına kendi adına şikâyette bulunmak ve kanun yoluna başvurma hakkını kullanmak üzere yetkilendirme hakkına sahiptir. Veri sahiplerini temsil etme hakkı, 77/249/AET[10] sayılı Konsey Direktifi'nde tanımlandığı şekilde veri sahibinin ulusal mahkemeler önünde avukat tarafından temsil edilmesini zorunlu kılan Üye Devlet usul hukukuna halel getirmemelidir.

(88) Bir kişinin, işbu Direktif'e uygun olarak kabul edilen hükümlerini ihlal eden bir işleme sonucu maruz kalabileceği herhangi bir zarar, veri sorumlusu veya Üye Devlet hukuku uyarınca yetkili herhangi bir makam tarafından tazmin edilmelidir. Zarar kavramı, Adalet Divanı'nın içtihadı ışığında ve işbu Direktif'in amaçlarını tamamen yansıtacak şekilde geniş olarak yorumlanmalıdır. Bu husus, Birlik veya Üye Devlet hukukundaki diğer kuralların ihlal edilmesinden kaynaklanan tazmin taleplerine halel getirmez. Hukuka uygun olmayan veya işbu Direktif uyarınca kabul edilen hükümleri ihlal eden işlemeye atıf yapılması hali, işbu Direktif uyarınca kabul edilen uygulama tasarruflarını da kapsar. Veri sahipleri, yaşadıkları zarar için tam ve etkili şekilde tazmin edilmelidir.

[10] Avukatlar tarafından özgür hizmet sunumunun etkin bir şekilde kullanılmasını kolaylaştırma hakkında 77/249/AET sayılı ve 22 Mart 1977 tarihli Konsey Direktifi (OJ L 78, 26.3.1977, p. 17).

(89) Cezalar, özel hukuka veya kamu hukukuna tabi olması fark etmeksizin, işbu Direktif'i ihlal eden bütün gerçek veya tüzel kişilere uygulanmalıdır. Üye Devletler cezaların etkili, orantılı ve caydırıcı olmasını sağlamalı ve cezaları uygulamak için tüm önlemleri almalıdır.

(90) İşbu Direktif'in uygulanması için yeknesak şartların sağlanması adına, üçüncü bir ülke, bir bölge veya bir üçüncü ülke içindeki belirli bir bölüm veya uluslararası bir organizasyon tarafından sağlanan yeterli koruma düzeyine ve karşılıklı yardımlaşma şekli ve prosedürleri ile denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin olarak Komisyon'a uygulama yetkileri verilmelidir. Bu yetkiler, Avrupa Parlamentosu ve Konsey'in 182/2011 (AB) sayılı Regülasyonu'na[11] uygun olarak kullanılmalıdır.

(91) İnceleme prosedürü, üçüncü bir ülke, bir bölge veya bir üçüncü ülke içindeki belirli bir bölüm veya uluslararası bir organizasyon tarafından sağlanan yeterli koruma düzeyine ve karşılıklı yardımlaşma şekli ve prosedürleri ile denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin olarak, genel kapsamda olmak kaydıyla, uygulama tasarruflarının kabulü için kullanılmalıdır.

(92) Komisyon, durumun aciliyetinin böyle gerektirdiği halde, üçüncü bir ülke, bir bölge veya bir üçüncü ülke içindeki belirli bir bölüm veya uluslararası bir organizasyon ile ilgili olarak artık yeterli bir koruma düzeyi sağlanamaması durumunda bunlarla ilgili olarak derhal uygulanabilir uygulama tasarruflarını kabul etmelidir.

(93) İşbu Direktif'in amaçları, yani gerçek kişilerin temel hak ve özgürlüklerinin ve özellikle kişisel verilerin korunması ve Birlik bünyesindeki yetkili makamlar tarafından kişisel verilerin serbest alışverişinin sağlanması, Üye Devletler tarafından yeterince gerçekleştirilemeyeceğinden ve eylemin ölçeği veya etkileri nedeniyle, Birlik düzeyinde daha iyi bir şekilde gerçekleştirilebileceğinden, Birlik, ABA'nın 5'inc maddesinde belirtildiği üzere, katmanlı yetki ilkesine uygun olarak önlemler alabilir. Bu maddede belirtilen orantılılık ilkesine uygun olarak, işbu Direktif, bu hedeflere ulaşmak için gerekli olanın ötesine geçmez.

[11] Avrupa Parlamentosu ve Konsey'in Üye Devletlerin Komisyonun uygulama yetkilerini ifasını kontrolüne ilişkin kurallar ve genel prensiplere ilişkin 16 Şubat 2011 tarihli ve 182/2011 (AB) sayılı Tüzüğü (OJ L 55, 28.2.2011, p. 13).

(94) Anlaşmalar uyarınca Üye Devletler arasında kişisel verilerin işlenmesini veya Üye Devletler'in belirlenmiş olan yetkili makamlarının kurulu bilgi sistemlerine erişimini düzenleyen, işbu Direktif'in kabul edilme tarihinden önce kabul edilmiş cezai konularda adli iş birliği ve polis iş birliği alanındaki Birlik tasarruflarının özel düzenlemeleri, örneğin, 2008/615/Aİİ sayılı Konsey Kararı'nın[12] kişisel verilerin korunmasına ilişkin özel hükümleri veya Avrupa Birliği Üye Devletleri Arasında Cezai Meselelerde Karşılıklı Yardımlaşma Sözleşmesi'nin[13] 23'üncü maddesi gibi düzenlemeler etkilenmeden kalmalıdır. Bildirge'nin 8'inci maddesi ve ABİA'nın 16'ncı maddesi, kişisel verilerin korunmasına ilişkin temel hakların Birlik genelinde tutarlı bir şekilde sağlanmasını gerektirdiğinden, Komisyon, işbu Direktif ile daha önce kabul edilen Üye Devletler arasında kişisel verilerin işlenmesini veya Üye Devletler'in belirlenmiş olan yetkili makamlarının kurulu bilgi sistemlerine erişimini düzenleyen kanunlar arasındaki ilişki bakımından durumu, böylelikle, bu özel hükümlerin Direktif ile uyumlaştırılmasını değerlendirmelidir. Uygun olduğu durumlarda, Komisyon, kişisel verilerin işlenmesiyle ilgili tutarlı hukuki kuralların sağlanması amacıyla önerilerde bulunmalıdır.

(95) Kişisel verilerin Birlik içinde kapsamlı ve tutarlı bir şekilde korunmasını sağlamak için, Üye Devletlerce işbu Direktif'in yürürlüğe girme tarihinden önce imzalanan ve bu tarihten önce geçerli olan ilgili Birlik hukukuna uyan uluslararası anlaşmalar değiştirilene, yerlerine yenisi gelene veya iptal edilene kadar yürürlükte kalmalıdır.

(96) Üye Devletler'e, işbu Direktif'i aktarmaları için, yürürlük tarihinden itibaren en fazla iki yıl olmak üzere süre verilmelidir. Bu tarihte halihazırda devam eden işlemeler, işbu Direktif'in yürürlüğe girmesinden itibaren iki yıl içinde işbu Direktif'e uygun hale getirilmelidir. Bununla birlikte, bu tür bir işlemenin, işbu Direktif'in yürürlüğe girdiği tarihten önce yürürlükte olan Birlik hukukuna uygun olması durumunda, işbu Direktif'in, denetim makamı tarafından önceden istişare edilmeye ilişkin şartları, bu gerekliliklerin, doğası gereği işlemeden önce karşılanması gerektiğinden, belirtilen tarihte devam etmekte olan işlemelerde geçerli olmamalıdır. Üye Devletler'in, bu tarihten önce kurulmuş olan otomatik işleme sistemlerinin kayıt günlüğüne ilişkin yükümlülükleri karşılaması için işbu Direktif'in yürürlüğe girdiği tarihten itibaren yedi yıldan daha uzun bir uygulama süresi belirlemeleri durumunda, veri sorumlusu veya veri işleyen, kayıt günlükleri ve diğer kayıt formları gibi kendi kendini izlemeyi mümkün

[12]Özellikle terörle mücadele ve sınır aşırı suçlar ile ilgili sınır ötesi iş birliğine ilişkin 2008/615/Aİİ sayılı ve 23 Haziran 2008 tarihli Konsey Kararı (OJ L 210, 6.8.2008, p. 1).
[13] ABA'nın 34'üncü maddesine dayanan 29 Mayıs 2000 tarihli Konsey Tasarrufu, Avrupa Birliği Üye Devletleri Arasında Cezai Meselelerde Karşılıklı Yardımlaşma Sözleşmesi (OJ C 197, 12.7.2000, p. 1).

kılarak ve veri bütünlüğü ile veri güvenliğini sağlayarak veri işlemenin yasallığını gösteren etkili yöntemler kullanmalıdır.

(97) İşbu Direktif, Avrupa Parlamentosu ve Konsey'in 2011/93/AB sayılı Direktifi'nde[14] belirtilen çocukların cinsel istismarına ve çocuk pornografisine karşı mücadele kurallarına halel getirmez.

(98) Dolayısıyla, 2008/977/Aİİ sayılı Çerçeve Karar yürürlükten kaldırılmalıdır.

(99) ABA'ya ve ABİA'ya ekli 21 numaralı Protokol'ün 6(a) maddesine göre Birleşik Krallık ve İrlanda'nın özgürlük, güvenlik ve adalet alanlarına ilişkin konumu uyarınca, Birleşik Krallık ve İrlanda, işbu Direktif'te yer alan ve Birleşik Krallık ile İrlanda'nın ABİA'nın 16'ncı maddesi kapsamındaki hükümler ile uyumlu olması gereken cezai konularda adli iş birliği ve polis iş birliği usullerine hakim kurallar ile bağlı olmadığı ABİA'nın Üçüncü Kısım Başlık 5 altındaki Bölüm 4 veya Bölüm 5 kapsamındaki faaliyetler yürütülürken kişisel verilerin Üye Devletler tarafından işlenmesine ilişkin kurallar ile bağlı değildir.

(100) ABA'ya ve ABİA'ya ekli 22 numaralı Protokol'ün 2 ve 2a maddeleri uyarınca Danimarka, ABİA'nın Üçüncü Kısım Başlık 5 altındaki Bölüm 4 veya Bölüm 5 kapsamındaki faaliyetler yürütülürken kişisel verilerin Üye Devletler tarafından işlenmesine ilişkin işbu Direktif'te yer alan ve veya bunların uygulanmasına ilişkin olan kurallar ile bağlı değildir. İşbu Direktif'in, ABİA'nın Üçüncü Kısım Başlık V uyarınca Schengen müktesebatına dayandığı göz önüne alındığında, Danimarka, Protokol'ün 4'üncü maddesi uyarınca, işbu Direktif'in kabul edilmesinden sonraki altı ay içerisinde, işbu Direktif'i ulusal hukukuna uygulayıp uygulamayacağına karar vermelidir.

(101) İzlanda ve Norveç ile ilgili olarak, işbu Direktif, Avrupa Birliği Konseyi ve İzlanda Cumhuriyeti ve Norveç Krallığı tarafından akdedilen Anlaşma uyarınca öngörülen ve bu iki Devletin Schengen müktesebatının uygulanması, başvurulması ve geliştirilmesi ile ilgili olarak iş birliğine ilişkin imzalanan Anlaşma ile Schengen müktesebatına ilişkin hükümlerin geliştirilmesini içermektedir[15]

[14] 2004/68/JHA sayılı Konsey Çerçeve Kararının yerine gelen ve Avrupa Parlamentosu ve Konseyinin çocukların cinsel istismarı ve çocuk pornografisine karşı 2011/93/AB sayılı ve 13 Aralık 2011 tarihli Direktifi (OJ L 335, 17.12.2011, p. 1).
[15] OJ L 176, 10.7.1999, p. 36.

(102) İsviçre ile ilgili olarak, işbu Direktif, Schengen müktesebatına ilişkin hükümlerin, Avrupa Birliği, Avrupa Topluluğu ve İsviçre Konfederasyonu arasındaki İsviçre Konfederasyonu'nun Schengen müktesebatının yürürlüğe konması, uygulanması ve gelişiminde iş birliğine dair Anlaşma ile öngörüldüğü üzere geliştirilmesini teşkil etmektedir.[16]

(103) Lihtenştayn ile ilgili olarak, işbu Direktif, Schengen müktesebatına ilişkin hükümlerin, Avrupa Birliği, Avrupa Topluluğu, İsviçre Konfederasyonu ve Lihtenştayn Prensliği arasındaki Lihtenştayn Prensliği'nin İsviçre Konfederasyonu'nun Schengen müktesebatının yürürlüğe konması, uygulanması ve gelişiminde iş birliğine dair Anlaşma'ya katılımı hakkındaki Protokol ile öngörüldüğü üzere geliştirilmesini teşkil etmektedir.[17]

(104) İşbu Direktif temel haklara saygı duyar ve Bildirge'de ABİA'da kabul edildiği şekilde tanınan ilkelere, bilhassa özel hayata ve aile hayatına saygı gösterilmesi hakkı, kişisel verilerin korunması hakkı, etkin bir hukuk yoluna başvuru ve adil yargılanma hakkına riayet eder. Bu haklara getirilen sınırlamalar, Birlik'in kabul ettiği kamu yararı hedeflerini karşılamada veya başkalarının hak ve özgürlüklerini korumada gerekli oldukça Bildirge'nin 52(1) numaralı maddesine uygundur.

(105) Komisyon'un ve Üye Devletler'in layihalar hakkındaki 28 Eylül 2011 tarihli Ortak Politika Beyanı uyarınca, Üye Devletler, haklı durumlarda, geçiş önlemlerine, bir direktifin bileşenleri ile ulusal geçiş önlemleri arasındaki ilişkiyi açıklayan bir veya daha fazla belge eklemeyi taahhüt etmişlerdir. İşbu Direktif'e ilişkin olarak, yasa koyucu bu tür belgelerin aktarımını haklı görmektedir.

(106) 45/2001 (AT) sayılı Regülasyon'un 28(2) numaralı maddesi uyarınca Avrupa Veri Koruma Denetçisi'ne danışılmış ve Denetçi 7 Mart 2012 tarihinde bir görüş bildirmiştir.[18]

(107) İşbu Direktif, Üye Devletler'i, aydınlatma yükümlülüğüne yönelik veri sahibi haklarının yürütülmesi, cezai kovuşturma sırasında kişisel verilere erişilmesi ve kişisel verinin silinmesi veya düzeltilmesi ve işlemenin kısıtlanması ve bunların ceza muhakemesine ilişkin ulusal kurallardaki olası kısıtlamalarını uygulamaktan alıkoymamalıdır.

[16] OJ L 53, 27.2.2008, p. 52.
[17] OJ L 160, 18.6.2011, p. 21.
[18] OJ C 192, 30.6.2012, p. 7.

İŞBU DİREKTİFİ KABUL ETMİŞTİR:

BİRİNCİ BÖLÜM
Genel Hükümler

Madde 1
Konu ve Amaç

1. İşbu Direktif, kişisel verilerin, kamu güvenliğine karşı tehditlerin önlenmesi ve kamu güvenliğinin bu tehditlere karşı korunması da dahil olmak üzere, yetkili makamlarca suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin kuralları düzenlemektedir.

2. İşbu Direktif uyarınca Üye Devletler:

   a. Gerçek kişilerin, başta kişisel verilerin korunmasına ilişkin hakları olmak üzere temel hak ve özgürlüklerini koruyacak; ve
   b. Birlik hukuku veya Üye Devlet hukuku uyarınca kişisel verilerin Birlik içerisinde yetkili makamlarca paylaşılmasının gerekli olması durumunda, bu paylaşımın kişisel verilerinin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin gerekçelerle sınırlandırılmamasını veya yasaklanmamasını sağlayacaktır.

3. İşbu Direktif Üye Devletler'in, kişisel verilerin yetkili makamlarca işlenmesiyle ilgili veri sahibinin hak ve özgürlüklerinin korunmasına ilişkin olarak işbu Direktif kapsamında öngörülenden daha yüksek bir düzeyde koruma sağlamalarına engel olmamaktadır.

Madde 2
Kapsam

1. İşbu Direktif, yetkili makamlar tarafından 1'inci maddenin birinci fıkrası kapsamında yer verilen amaçlar doğrultusunda kişisel verilerin işlenmesinde uygulanacaktır.

2. İşbu Direktif, tamamen veya kısmen otomatik yollarla kişisel verilerin işlenmesini ve bir veri kayıt sisteminin parçası teşkil etmesi veya ileride edecek olması kaydıyla, otomatik olmayan yollarla kişisel verilerin işlenmesi bakımından uygulanacaktır.

3. İşbu Direktif hükümleri aşağıdaki hallerde uygulama alanı bulmayacaktır:

   a. Birlik hukuku kapsamı dışında kalan faaliyetler dahilinde kişisel verilerin işlenmesi;
   b. Birlik kurumları, organları, makamları ve ajansları tarafından kişisel verilerin işlenmesi.

Madde 3
Tanımlar

İşbu Direktif'in uygulanmasında:

1. "kişisel veri" kimliği belirli veya belirlenebilir gerçek kişiye ("veri sahibi") ait her türlü bilgiyi; kimliği belirlenebilir gerçek kişi, özellikle isim, kimlik numarası, konum verisi, çevrimiçi tanımlayıcılar veya fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ilişkin unsurlardan biri veya birkaçı ile belirlenebilir olan kişiyi;
2. "işleme" kişisel veriler veya kişisel veri setleri üzerinde gerçekleştirilen, otomatik yollarla gerçekleştirilip gerçekleştirilmediğine bakılmaksızın, kişisel verilerin elde edilmesi, kaydedilmesi, düzenlenmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri getirilmesi, başvurulması, kullanılması, aktarıma konu edilmek suretiyle paylaşılması, yayılması veya başka şekillerle erişilebilir kılınması, gruplandırılması veya bir araya getirilmesi, kısıtlanması, silinmesi veya imha edilmesi gibi her türlü işlemi;
3. "işlemenin kısıtlanması" ileride işlenmesinin sınırlandırılması amacıyla saklanan kişisel verilerin işaretlenmesini;
4. "profilleme" özellikle ilgili gerçek kişinin işyerindeki performansı, mali durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketleri gibi hususların analiz ve tahmin edilmesine yönelik kullanımları teşkil eden, kişisel verilerin otomatik yollarla işlenmesine ilişkin her türlü işlemi;
5. "maskeleme (*pseudonymisation*)" ilave bilgilerin ayrı bir yerde saklanması ve kişisel verilerin bir gerçek kişi ile ilişkilendirilememesine yönelik teknik ve organizasyonel tedbirlere tabi olmak kaydıyla; kişisel verilerin, ilave bilgiler ile bir araya getirilmeksizin, belirli bir veri sahibi ile ilişkilendirilemeyecek şekilde işlenmesini;
6. "kayıt sistemi" belirli kriterler doğrultusunda erişilebilen gerek merkezi gerekse fonksiyonel veya coğrafi olarak dağıtılmış veya dağıtılmış olan yapılandırılmış her türlü kişisel veri setini;
7. "yetkili makam":

    a. ceza gerektiren suçların önlenmesi, araştırılması, tespiti ve soruşturulması veya kamu güvenliğine ilişkin önlemlerin alınması ve kamu güvenliğine ilişkin tehditlerin önlenmesi de dahil olmak üzere, ceza hükümlerinin infazı hususlarında yetkilendirilmiş resmi makamları, veya
    b. Üye Devlet hukuku uyarınca ceza gerektiren suçların önlenmesi, araştırılması, tespiti ve soruşturulması veya kamu güvenliğine ilişkin önlemlerin alınması ve kamu güvenliğine ilişkin tehditlerin önlenmesi de dahil olmak üzere, ceza hükümlerinin infazı hususlarında kamu otoritesini ve gücünü kullanmak üzere yetkilendirilmiş her türlü organ ve kuruluşu;

8. "veri sorumlusu" tek başına veya başkaları ile birlikte kişisel verilerin işlenme amaç ve vasıtalarını belirleyen yetkili makamı ifade eder. İşlemenin amaç ve vasıtalarının Birlik veya Üye Devlet hukuku tarafından belirlendiği durumlarda, veri sorumlusu veya veri sorumlusunun belirlenmesinde dikkate alınan belirli kriterler Birlik veya Üye Devlet hukuku tarafından sağlanabilecektir.
9. "veri işleyen" veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu kuruluşu, ajansı veya başkaca bir makamı;
10. "alıcı" üçüncü bir kişi olup olmadığına bakılmaksızın, kişisel verilerin paylaşıldığı gerçek veya tüzel kişi, kamu kuruluşu, teşkilatı veya başkaca bir makamı ifade eder. Ancak, Üye Devlet hukuku uyarınca yapılacak bir sorgulama ile kişisel verileri elde eden resmi makamlar, alıcı olarak değerlendirilmemekte; bu verilerin ilgili resmi makamlarca işlenmesi, işlenme amacına bağlı olarak, kişisel verilerin korunmasına ilişkin kurallar ile uyumlu olduğu değerlendirilebilecektir.

11. "kişisel veri ihlali" iletilen, saklanan ve sair şekillerde işlenen kişisel verilerin kazara veya hukuka aykırı olarak yok edilmesi, kaybedilmesi, yetkisiz kişiler ile paylaşılması veya erişilmesine sebebiyet veren her türlü güvenlik ihlalini;
12. "genetik veriler" özellikle söz konusu gerçek kişiden gelen biyolojik bir numunenin analiz edilmesi sonucunda, bir gerçek kişinin fizyolojisi veya sağlığı hakkında özgün bilgiler veren bir gerçek kişinin kalıtsal veya edinilmiş genetik özellikleriyle ilgili kişisel verileri;
13. "biyometrik veri" yüz görüntüleri ve daktiloskopi verileri gibi, bir gerçek kişinin kimliğinin şüpheye yer bırakmayacak şekilde belirlenmesi veya doğrulanmasına yönelik, ilgili gerçek kişinin fiziksel, fizyolojik veya davranışsal özelliklerinin teknik işlenme sonucu ortaya çıkan verileri;
14. "sağlık ile ilgili veriler" sağlık hizmetlerinin sunulması ile ilgili olanlar da dahil olmak üzere, bir gerçek kişinin fiziksel veya zihinsel sağlığı ile ilgili olan ve kişinin sağlık durumu ile bilgileri açığa çıkaran kişisel verileri;
15. "denetleyici makam" Üye Devlet tarafından 41'inci madde uyarınca kurulacak olan bağımsız resmi makamı;
16. "uluslararası kuruluş" uluslararası kamu hukukuna tabi olarak kurulmuş olan bir kuruluş ve onun tali organlarını veya iki ya da daha fazla ülke arasında akdedilmiş bir anlaşma temelinde kurulmuş olan herhangi bir organı ifade etmektedir.

İKİNCİ BÖLÜM
Genel ilkeler

Madde 4
Kişisel Verilerin İşlenmesi

1. Üye Devletler kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulmasını sağlar:

(a) hukuka ve dürüstlük kurallarına uygun olma;
(b) belirli, açık ve meşru amaçlar için elde edilme ve bu amaçlar ile bağdaşmayan bir şekilde işlenmeme;
(c) işlendikleri amaçla ölçülü, bağlantılı ve sınırlı olma;
(d) doğru ve gerektiğinde güncel olma; işlendikleri amaç göz önünde bulundurularak, hatalı kişisel verinin gecikmeksizin silinmesi veya düzeltilmesi için, gerekli her türlü önlemin alınması;
(e) işlendikleri amaç için gerekli olan süreden daha uzun olmamak üzere, veri sahibinin kimliğinin belirlenmesine izin verecek biçimde tutulması;
(f) hukuka aykırı olarak işlenmesi veya erişilmesi ile kazara kayıp, imha veya zarara uğramasının önlenmesine ilişkin teknik ve idari tedbirlerin uygulanması da dahil olmak üzere, kişisel verilerin güvenliğinin sağlanmasını temin edecek şekilde işlenmesi;

2. 1'inci maddenin birinci fıkrası kapsamında düzenlenen amaçlar dahilinde, aşağıda yer verilen hallerde, kişisel veriler aynı veya bir başka veri sorumlusu tarafından elde edilme amacı dışında bir amaçla işlenebilecektir:

   a. Birlik veya Üye Devlet hukuku uyarınca, veri sorumlusunun işbu amaçla kişisel veri işlemek üzere yetkilendirilmiş olması; ve
   b. Birlik veya Üye Devlet hukuku uyarınca, kişisel verilerin işlenmesinin işbu diğer amaçlar için gerekli ve orantılı olması.

3. 1'inci maddenin birinci fıkrası kapsamında düzenlenen amaçlar dahilinde ve veri sahibinin hak ve özgürlüklerinin korunması bakımından yeterli önlemlerin alınması

kaydıyla, kişisel veriler kamu yararı bakımından arşivlenme, bilimsel, istatistiki veya tarihsel kullanıma ilişkin amaçlarla da işlenebilecektir.

4. Veri sorumlusu, 1'inci, 2'nci ve 3'üncü fıkralar uyarınca sorumlu olacak ve bu hükümleri uygun hareket ettiğini ispatlayacaktır.

Madde 5

Saklama ve İncelemeye İlişkin Süre Sınırları

1. Üye Devletler, kişisel verilerin silinmesi veya saklanması ihtiyacının dönemsel olarak gözden geçirilmesi amaçlarıyla, yeterli süre sınırları uygulayacaktır. Usuli tedbirler vasıtasıyla, bu süre sınırlarının gözden geçirilmesi sağlanacaktır.

Madde 6

Farklı Veri Sahibi Kategorileri Arasında Ayrım

1. Üye Devletler, aşağıdaki hallerde ve mümkün olduğu ölçüde, veri sorumlusu tarafından farklı veri sahibi kategorilerine ait kişisel veriler arasında açık bir ayrım yapılmasını sağlayacaklardır.
   a. Hakkında, bir suç işlediğine veya bir suç işlemek üzere olduğuna ilişkin ciddi gerekçeler bulunan kişiler;
   b. Bir suçtan hüküm giymiş olan kişiler;
   c. Bir suçun mağdurları veya hakkında bir suçun mağduru olabileceğine ilişkin belirli gerekçeler bulunan kişiler;
   d. Ceza soruşturmasında veya takip eden ceza kovuşturmasında tanıklık etmek üzere çağrılabilecek olan suça ilişkin diğer taraflar, suça ilişkin bilgi sağlayabilecek kişiler veya (a) ve (b) bentlerinde belirtilen kişilerin temasları bulunduğu veya ilgili olduğu kişiler.

Madde 7

Kişisel Veriler Arasındaki Ayrım ve Kişisel Verilerin Niteliğinin Doğrulanması

1. Üye Devletler, mümkün olduğunca, gerçeklere dayalı kişisel verilerin şahsi değerlendirmelere dayalı verilerden ayırt edilmesini sağlayacaktır.

2. Üye Devletler, yetkili makamlarca, yanlış, eksik veya güncel olmayan kişisel verilerin iletilmemesini veya erişilebilir kılınmamasını sağlamak üzere tüm makul önlemlerin alınması temin edecektir. Bu doğrultuda, iletilmeden veya erişilebilir kılınmadan önce, her yetkili makam tarafından, uygulanabilir olduğu ölçüde, kişisel verilerin niteliği doğrulanacaktır. Mümkün olduğu ölçüde, kişisel verilere ilişkin tüm aktarım işlemlerinde, alıcı yetkili makamın kişisel verilerin doğruluğunu, eksiksizliğini ve güvenilirliğini ve güncelliğini değerlendirmesini sağlayacak gerekli bilgiler eklenecektir.

3. Yanlış kişisel verilerin iletilmesi veya kişisel verilerin hukuka aykırı olarak iletilmesi halinde, alıcıya gecikmeksizin bildirimde bulunulur. Bu durumda, ilgili kişisel veriler düzeltilecek veya silinecek ya da bu verilerin işlenmesi 16'ncı madde uyarınca sınırlandırılacaktır.

Madde 8

İşlemenin Hukuka Uygunluğu

1. Üye Devletler, Birlik veya Üye Devlet hukuku uyarınca ve 1'inci maddenin birinci fıkrası kapsamında düzenlenen amaçlar dahilinde, yetkili makam tarafından yerine getirilen

görevin ifası için veri işlemenin zorunlu olması durumunda, işleme faaliyetinin hukuka uygun olarak yürütülmesini sağlayacaktır.

2. İşbu Direktif kapsamında kişisel verilerin işlenmesini düzenleyen Üye Devlet hukuku; asgari olarak, kişisel verilerin işlenmesi ile hedeflenenleri, işlenecek kişisel verileri ve veri işlemenin amaçlarını belirleyecektir.

Madde 9
Özel İşleme Şartları

1. Yetkili makamlar tarafından 1'inci maddenin birinci fıkrası kapsamında düzenlenen amaçlar dahilinde toplanan kişisel veriler, 1'inci maddenin birinci fıkrası kapsamında düzenlenen amaçlar dışında Birlik veya Üye Devlet hukuku tarafından izin verilmedikçe işlenemeyecektir. Kişisel verilerin bu tür başka amaçlar için işlendiği durumlarda, işleme, Birlik hukuku kapsamı dışında kalan bir faaliyette gerçekleştirilmedikçe, 2016/679 (AB) sayılı Regülasyon uygulanacaktır.

2. Yetkili makamlar, Üye Devlet hukuku tarafından, 1'inci maddenin birinci fıkrası kapsamında düzenlenen amaçlar dışındaki görevlerin yerine getirilmesi ile ilgili olarak görevlendirildiklerinde, verilerin işlenmesi Birlik hukuku kapsamı dışında kalan bir faaliyette gerçekleştirilmedikçe, kamu yararı bakımından arşivlenme, bilimsel, istatistiki veya tarihsel araştırmaya ilişkin amaçlar da dahil olmak üzere, işbu amaçlarla kişisel verilerin işlenmesi bakımından 2016/679 (AB) sayılı Regülasyon uygulanacaktır.

3. Üye Devletler, veri paylaşımında bulunan yetkili makam için uygulanacak olan Birlik veya Üye Devlet hukukunun kişisel verilerin işlenmesi için özel koşullar sağladığı durumlarda, veri paylaşımında bulunan yetkili makamın, bu tür kişisel verilerin alıcısına bu koşullara ve bunlara uygun hareket etme yükümlülüğüne ilişkin bilgi vermesini sağlayacaktır.

4. Üye Devletler, veri paylaşan yetkili makamın bu şartları diğer Üye Devletler'de yer alan alıcılara veya bu yetkili makamın Üye Devlet'i içindeki benzer veri aktarımlarına uygulanabilir olanlardan başka ABİA Başlık 5 Bölüm 4 ve 5 uyarınca kurulmuş olan teşkilat, ofis ve kurumlara uygulamamasını temin edecektir.

Madde 10
Özel Nitelikli Kişisel Verilerin İşlenmesi

1. Veri sahibinin hak ve özgürlüklerinin korunması bakımından yeterli önlemlerin alınması kaydıyla; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, dini veya felsefi inançları veya sendika üyeliği ile ilgili bilgileri içeren kişisel veriler ile bir gerçek kişinin kimliğinin şüpheye yer bırakmayacak şekilde belirlenmesi amacıyla genetik ve biyometrik veriler ile sağlık verilerinin veya bir gerçek kişinin cinsel yaşamı veya cinsel yönelimiyle ilgili veriler, yalnızca mutlak surette gerekli olduğu durumlar ile sınırlı olmak üzere aşağıdaki hallerde işlenebilecektir:

    a. Birlik Hukuku veya Üye Devlet hukuku uyarınca yetkilendirilen hallerde;
    b. Veri sahibinin ve bir başka gerçek kişinin hayati önemi haiz menfaatlerinin korunması amacıyla; veya
    c. Veri işlemenin veri sahibi tarafından açıkça alenileştirilmiş olan verilerle ilgili olduğu durumlarda.

Madde 11
Otomatik Bireysel Karar Alma

1. Veri sorumlusunun tabi olduğu asgari olarak veri sahibinin veri sorumlusu tarafından insan müdahalesi elde etme hakkını düzenleyecek şekilde, veri sahibinin hak ve özgürlüklerinin korunması bakımından yeterli önlemlerin alınmasının öngörüldüğü Birlik veya Üye Devlet hukuku uyarınca yetkilendirilmiş olmadıkça, Üye Devletler, profilleme faaliyetleri de dahil olmak üzere veri sahibi üzerinde olumsuz hukuki etkiler doğuracak veya veri sahibini önemli ölçüde etkileyecek hallerde münhasıran otomatik yollarla veri işlenmesine dayanan bir kararın alınmamasını sağlayacaklardır.

2. Bu maddenin 1'inci fıkrasında belirtilen kararlar, veri sahibinin hak ve özgürlükleri ile meşru menfaatlerinin korunmasına yönelik gerekli önlemler alınmadıkça, 10'uncu madde kapsamında belirtilen özel nitelikli kişisel veri kategorilerine dayandırılmayacaktır.
3. Birlik hukuku uyarınca, 10'uncu madde kapsamında belirtilen özel nitelikli kişisel verilere dayalı olarak gerçek kişiler arasında ayrımcılığa yol açacak şekilde profilleme faaliyetlerinin gerçekleştirilmesi yasaklanmıştır.

ÜÇÜNCÜ BÖLÜM
Veri sahibinin hakları

Madde 12
Veri Sahibi Haklarının Kullanılmasına İlişkin İletişim ve Yöntemler

1. Üye Devletler, veri sorumlusunun 13'üncü maddede belirtilen her türlü bilginin temin edilmesi ve 11'inci, 14 ila 18'inci ve 31'inci madde uyarınca kişisel verilerin işlenmesine ilişkin olarak veri sahibiyle tesis edilecek olacak iletişimlerin, kısa, anlaşılır ve kolay erişilebilir bir biçimde ve açık ve sade bir dil kullanılarak gerçekleştirilmesi hususunda makul adımlar atmasını sağlayacaktır. Söz konusu bilgiler, elektronik yöntemler de dahil olmak üzere, uygun herhangi bir yolla sunulacaktır. Genel kural itibariyle, veri sorumlusu, bilgiyi bahse konu talep ile aynı yöntemle sağlayacaktır.

2. Üye Devletler, veri sorumlusunun, 11'inci ve 14 ila 18'inci madde arasında düzenlenen veri sahibi haklarının kullanılmasını kolaylaştırmasını sağlayacaktır.

3. Üye Devletler, veri sorumlusunun, talebine ilişkin takipte bulunan veri sahibine gecikmeksizin yazılı olarak bilgi vermesini sağlayacaktır.

4. Üye Devletler, 13'üncü madde kapsamında sunulan bilgileri ve 11'inci, 14 ila 18'inci ve 31'inci madde uyarınca yapılan her türlü iletişimi veya gerçekleştirilecek işlemi ücretsiz olarak sağlayacaktır. Veri sorumlusu, veri sahibi tarafından yöneltilen taleplerin açıkça dayanaktan yoksun olması veya kapsamı aşması durumunda, bilhassa tekrarlanan mahiyette olmaları nedeniyle:

(a) bilgi veya iletişimi sağlama veya talep edilen işlemin gerçekleştirilmesini idari maliyetlerini dikkate alarak makul bir ücret talep edebilecek; veya
(b) talebin gereğini yerine getirmeyi reddedebilecektir.
Bahse konu talebin, açıkça dayanaktan yoksun veya kapsamı aşar nitelikte olduğunu ispat etmekle yükümlüdür.

5. Veri sorumlusunun, 14'üncü veya 16'ncı uyarınca, talebi yönelten gerçek kişinin kimliği ile ilgili makul şüphelerinin oluşması halinde, veri sorumlusu, veri sahibinin kimliğini doğrulamak için gerekli ek bilgilerin sağlanmasını talep edebilecektir.

Madde 13

Veri Sahibine Sağlanacak veya Veri Sahibinin Erişimine Sunulacak Bilgiler

1. Üye Devletler, veri sorumlusu tarafından asgari olarak aşağıdaki bilgilerin veri sahibinin erişimine sunulmasını sağlayacaktır:

   a. Veri sorumlusunun kimliği ve iletişim bilgileri;
   b. Mevcut olması halinde, veri koruma görevlisinin iletişim bilgileri;
   c. Kişisel verilerin hangi amaçla işleneceği;
   d. Denetleyici makama şikâyette bulunma hakkı ve denetleyici makamın iletişim bilgileri,
   e. Veri sahibinin kişisel verilere erişim, kişiler verilerin düzeltilmesi veya silinmesi ve kişisel verilerin işlenmesinin sınırlandırılması yönünde talepte bulunma hakkı.

2. Birinci fıkrada atıfta bulunulan bilgilere ek olarak, Üye Devletler, belirli durumlarda veri sahibinin haklarını kullanabilmesini sağlamak amacıyla aşağıda belirtilen bilgilerin de veri sorumlusu tarafından veri sahibine sağlanmasını kanunen temin edeceklerdir:

   a. Veri işlemenin hukuki dayanağı;
   b. Kişisel verilerin hangi süre ile saklanacağı veya bu bilginin verilmesinin mümkün olmadığı durumlarda bu sürenin belirlenmesinde kullanılan kriterleri;
   c. Mevcut olması halinde, üçüncü ülkeler veya uluslararası kuruluşlardakiler de dahil olmak üzere, kişisel verilerin aktarıldığı tarafların kategorileri;
   d. Başta kişisel verilerin veri sahibinin bilgisi dışında elde edildiği haller olmak üzere, gerekmesi halinde bu gibi ilave bilgiler.

3. Üye Devletler, aşağıda yer verilen amaçlara yönelik olarak, yasal düzenlemeler vasıtasıyla, ikinci fıkrada belirtilen bilgilerin veri sahibine sağlanmasını, gerçek kişinin temel hakları ve meşru menfaatleri açısından demokratik bir toplumda gerekli ve orantılı önlemler teşkil ettiği müddetçe, erteleyen, sınırlayan veya engelleyen tedbirlere başvurabilecektir:

   a. İdari veya adli tahkikatların, soruşturma veya kovuşturmaların engellenmesinin önüne geçilmesi;

   b. Suçların önlenmesi, tespiti, soruşturulması veya kovuşturulmasına ya da cezaların infazına halel getirilmemesi;

   c. Kamu güvenliğinin korunması;

   d. Ulusal güvenliğin korunması;

   e. Üçüncü kişilerin hak ve özgürlüklerinin korunması.

4. Üye Devletler, yasal düzenlemeler vasıtasıyla, hangi veri işleme kategorilerinin tamamen veya kısmen üçüncü fıkra kapsamında yer verilen hususlara tekabül edeceğini belirleyebileceklerdir.

Madde 14
Veri Sahibinin Erişim Hakkı

1. 15'inci maddeye tabi olmak üzere, Üye Devletler, veri sahiplerine kendileriyle ilgili kişisel verilerin işlenip işlenmediğine ilişkin olarak veri sorumlusundan bilgi talep etme ve kendisi ile ilgili kişisel verilerin işlenmesi halinde ise bu kişisel veriler ile aşağıda yer alan bilgilere erişim hakkı sağlayacaktır:

(a) kişisel verilerin işlenme amaçları ve işleme faaliyetinin hukuki dayanağı;
(b) kişisel verilerin kategorileri;
(c) başta üçüncü ülkeler ve uluslararası kuruluşlardaki alıcılar olmak üzere, kişisel verilerin aktarıldığı alıcılar veya alıcı kategorileri;
(d) mümkün olması halinde, kişisel verilerin saklanması için öngörülen süre veya mümkün olmaması halinde, bu sürenin belirlenmesinde kullanılan kriterler;
(e) veri sorumlusundan kişisel verilerinin düzeltilmesini, silinmesini veya veri sahibine ait kişisel verilerin işlenmesinin sınırlandırılmasını talep etme hakkının mevcudiyeti;
(f) denetleyici makama şikâyette bulunma hakkı ile denetleyici makama ait iletişim bilgileri;
(g) işleme tabi tutulan kişisel verilerin ve bunların kaynağına ilişkin mevcut bilgiler.

Madde 15
Erişim Hakkına İlişkin Sınırlamalar

1. Üye Devletler, aşağıda yer verilen amaçlar doğrultusunda, veri sahibinin erişim hakkını kısmen veya tamamen kısıtlamaya yönelik yasal düzenlemeleri, böyle bir düzenleme gerçek kişinin temel hakları ve meşru menfaatleri açısından demokratik bir toplumda gerekli ve orantılı bir önlem teşkil ettiği müddetçe, getirebileceklerdir.

a. İdari veya adli tahkikatların, soruşturma veya kovuşturmaların engellenmesinin önüne geçilmesi;
b. Suçların önlenmesi, tespiti, soruşturulması veya kovuşturulmasına ya da cezaların infazına halel getirilmemesi;
c. Kamu güvenliğinin korunması;
d. Ulusal güvenliğin korunması;
e. Üçüncü kişilerin hak ve özgürlüklerinin korunması.

2. Üye Devletler, yasal düzenlemeler vasıtasıyla, hangi veri işleme kategorilerinin tamamen veya kısmen birinci fıkranın (a) ve (e) bentleri arasında yer verilen hususlara tekabül edeceğini belirleyebileceklerdir.

3. Üye Devletler, birinci ve ikinci fıkralar kapsamında düzenlenen hallerde, herhangi bir şekilde erişimin reddedilmesi veya kısıtlanması söz konusu olduğunda, veri sorumlusunun, veri sahibine, gecikmeksizin bu durumu erişimin reddedilme veya kısıtlanma sebebi ile birlikte yazılı olarak bildirmesini sağlayacaktır. Birinci fıkrada yer verilen amaçlardan herhangi birinin zarar görebileceği durumlarda bu bilginin veri sahibi ile paylaşılmaması söz konusu olabilecektir. Üye Devletler, veri sorumlusunun, veri sahibine düzenleyici makam nezdinde şikâyette bulunabileceği veya kanun yoluna başvurabileceğine ilişkin bilgi vermesini sağlayacaktır.

4. Üye Devletler, veri sorumlusunun kararın dayandığı fiili veya hukuki nedenleri belgelemesini sağlayacaktır. Bu bilgi denetleyici makam nezdinde de erişilebilir kılınacaktır.

Madde 16

Kişisel Verilerin Düzeltilmesi veya Silinmesi ile İşlenmesinin Sınırlandırılması Hakkı

1. Üye Devletler, veri sahibine, veri sorumlusundan işlenen hatalı kişisel verilerinin gecikmeksizin düzeltilmesini isteme hakkını sağlayacaktır. Kişisel verilerin işlenme amacı da dikkate alınarak, veri sahibinin tamamlayıcı beyanlar da dahil olmak üzere işlenen eksik verilerinin tamamlanmasın talep etme hakkını sağlayacaktır.

2. Üye Devletler, veri sorumlusunun kişisel verileri gecikmeksizin silmesini, kişisel verilerin işlenmesinin 4'üncü, 8'inci veya 10'uncu madde hükümlerini ihlal etmesi veya kişisel verilerin veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesi amacıyla silinmesi gerektiği durumlarda veri sahibine kişisel verilerinin gecikmeksizin silinmesi talep etme hakkını sağlayacaktır.

3. Aşağıdaki hallerde, veri sorumlusu silme işlemi yerine, kişisel verilerin işlenmesinin sınırlandırılmasını sağlayacaktır:

   a. Veri sahibi tarafından işlenen kişisel verilerin doğru olmadığının iddia edilmesi ve kişisel verilerin doğruluğunun veya doğru olmadığının tespit edilmemesi halinde;
   b. Kişisel verilerin delil teşkil etmesi amacıyla korunmuş olması halinde.

   Kişisel verilerin işlenmesinin (a) bendi uyarınca sınırlandırılması halinde, veri sorumlusu sınırlandırmanın kaldırılmasından önce veri sahibini bilgilendirecektir.

4. Üye Devletler, düzeltme talebinin reddedilmesi veya kişisel verilerin işlenmesinin sınırlandırılması halinde, veri sorumlusunun gecikmeksizin bu durumu nedenleri ile birlikte veri sahibine yazılı olarak bildirmesini sağlayacaktır. Üye Devletler, aşağıda yer verilen amaçlar doğrultusunda, veri sahibine bu bilgilerin verilmesini kısmen veya tamamen kısıtlamaya yönelik yasal düzenlemeleri, böyle bir düzenleme gerçek kişinin temel hakları ve meşru menfaatleri açısından demokratik bir toplumda gerekli ve orantılı bir önlem teşkil ettiği müddetçe, getirebilecektir.

   a. İdari veya adli tahkikatların, soruşturma veya kovuşturmaların engellenmesinin önüne geçilmesi;
   b. Suçların önlenmesi, tespiti, soruşturulması veya kovuşturulmasına ya da cezaların infazına halel getirilmemesi;
   c. Kamu güvenliğinin korunması;
   d. Ulusal güvenliğin korunması;
   e. Üçüncü kişilerin hak ve özgürlüklerinin korunması.

   Üye Devletler, veri sorumlusunun, veri sahibine düzenleyici makam nezdinde şikâyette bulunabileceği veya kanun yoluna başvurabileceğine ilişkin bilgi vermesini sağlayacaktır.

5. Üye Devletler, veri sorumlusunun hatalı kişisel verilerin düzeltilmesi işlemini, hatalı kişisel verilerin kaynağını teşkil yetkili makama bildirmesini sağlayacaktır.

6. Üye Devletler, birinci, ikinci ve üçüncü fıkralar uyarınca kişisel verilerin düzeltilmesi, silinmesi veya işlenmesinin sınırlandırılması hallerinde, veri sorumlusunun ilgili kişisel verilerin, sorumlulukları kapsamında, alıcıları tarafından da düzeltilmesi, silinmesi veya işlenmesinin sınırlandırılması yönünde bilgilendirmesini sağlayacaktır.

Madde 17

Veri Sahibi Tarafından Hakların Kullanılması ve Denetleyici Makam Tarafından Doğrulanması

1. 13'üncü maddenin 3'üncü fıkrası, 15'inci maddenin 3'üncü fıkrası ve 16'ncı maddenin 4'üncü fıkrası kapsamında belirtilen hallerde, Üye Devletler; veri sahibi haklarının, yetkili denetleyici makam kanalıyla kullanabilmesini teminen gerekli önlemleri alacaktır.

2. Üye Devletler; birinci fıkra uyarınca veri sorumlusu tarafından veri sahibine, haklarının yetkili denetleyici makam kanalıyla kullanılabileceğine ilişkin bilgilendirmenin yapılmasını sağlayacaktır.

3. Birinci fıkrada atıfta bulunulan hakkın kullanılması durumunda, denetleyici makam tarafından; veri sahibine asgari olarak, gerekli tüm doğrulamaların yapıldığına veya denetleyici makam tarafından bir inceleme gerçekleştirildiğine ilişkin bilgi verilecektir. Denetleyici makam, aynı zamanda veri sahibine kanun yoluna başvurma hakkı bulunduğuna ilişkin bilgilendirme yapacaktır.

Madde 18

Ceza Soruşturma ve Kovuşturmalarında Veri Sahibinin Hakları

1. Üye Devletler, kişisel verilerin bir yargı kararında veya cezai soruşturma ve kovuşturma esnasında işlenen bir kayıt veya dosyada yer alması durumunda, 13'üncü, 14'üncü ve 16'ncı madde kapsamında belirlenen hakların Üye Devlet hukukuna uygun olarak kullanılmasını sağlayacaklardır.

DÖRDÜNCÜ BÖLÜM
Veri sorumlusu ve Veri işleyen

Birinci Kısım
Genel Yükümlülükler

Madde 19

Veri Sorumlusunun Yükümlülükleri

1. Üye Devletler; veri sorumlusunun, veri işlemenin mahiyetini, kapsamını, bağlamını, amaçlarını ve bunların yanı sıra gerçek kişilerin hak ve özgürlükleri üzerindeki çeşitli riskleri ve gerçekleşme olasılıklarını da dikkate alarak, kişisel verilerin işlenmesinin işbu Direktif hükümleri ile uyumlu olmasını sağlamak ve bu hükümlere uygun hareket edildiğinin ispatlanması amaçlarıyla, uygun teknik ve idari tedbirleri almasını sağlayacaktır. İşbu tedbirler, gerektiğinde, incelenecek ve güncellenecektir.

2. Kişisel verilerin işlenmesi faaliyetleri ile orantılı olduğu ölçüde, birinci fıkrada atıfta bulunulan tedbirler, veri sorumlusu tarafından kişisel verilerin işlenmesine ilişkin politikaların uygulamaya alınmasını da kapsayacaktır.

Madde 20
Tasarımdan ve Başlangıçtan İtibaren Kişisel Verilerin Koruması

1. Üye Devletler, işbu Direktif'in gereklerinin yerine getirilmesi ve veri sahiplerinin haklarının korunması amacıyla, veri sorumlusunun, en son teknolojiyi, uygulama maliyetini ve işlemenin mahiyetini, kapsamını, bağlamını, amaçlarını ve bunların yanı sıra gerçek kişilerin hak ve özgürlükleri üzerindeki çeşitli riskleri ve gerçekleşme olasılıklarını da dikkate alarak, gerek işleme araçlarının belirlenmesi gerekse de kişisel verilerin işlenmesi sırasında, veri koruma ilkelerinin uygulanması için tasarlanan maskeleme ve veri minimizasyonu gibi uygun teknik ve idari tedbirlerin etkin bir şekilde uygulaması amacıyla söz konusu tedbirleri veri işleme süreçlerine entegre etmesini sağlayacaktır.

2. Üye Devletler; veri sorumlusunun başlangıçtan itibaren, yalnızca işlemenin her bir özel amacı için gerekli olan kişisel verilerin işlenmesini sağlayan uygun teknik ve idari tedbirleri almasını sağlayacaktır. Bu yükümlülük, toplanan kişisel verilerin miktarı, işlemenin kapsamı, saklama süresi ve erişilebilirliği için geçerli olacaktır. Özellikle, bu tür tedbirler, başlangıçtan itibaren, kişisel verilerin, bireyin müdahalesi olmaksızın belirsiz sayıda gerçek kişi tarafından erişilebilir kılınmasını engelleyecektir.

Madde 21
Birlikte Veri Sorumluları

1. Üye Devletler; iki veya daha fazla veri sorumlusunun kişisel verilerin işleme amaç ve vasıtalarını birlikte belirlemeleri halinde bu kişilerin birlikte veri sorumlusu olduklarını düzenleyeceklerdir. Birlikte veri sorumluları, başta 13'üncü kapsamında düzenlenen bilgi verme yükümlülükleri ve veri sahibinin haklarını kullanmasına ilişkin hususlar olmak üzere, işbu Direktif hükümlerine uyum sağlama yükümlülüklerini, bu yükümlülükler veri sorumlularının tabi olduğu Birlik veya Üye Devlet hukuku uyarınca belirlenmedikçe; kendi aralarında yapacakları bir sözleşme ile şeffaf bir şekilde düzenleyebileceklerdir. Bu sözleşme kapsamında veri sahibi bakımından irtibat kişisinin belirlenmesi de sağlanacaktır. Üye Devletler; birlikte veri sorumlularından hangisinin, veri sahiplerinin haklarını kullanabilmeleri amacıyla tek irtibat kişisi olarak hareket edeceğini belirleyebileceklerdir.

2. Birinci fıkradan atıfta bulunulan sözleşme hükümlerinden bağımsız olarak Üye Devletler, veri sahibinin işbu Direktif uyarınca düzenlenen haklarını birlikte veri sorumlularından her biri nezdinde ve her birine karşı ileri sürebilmesi yönünde düzenleme yapabileceklerdir.

Madde 22
Veri İşleyen

1. Üye Devletler; kişisel verilerin veri sorumlusu adına işlenmesi halinde, veri sorumlusunun işbu Direktif gerekliliklerinin yerine getirilmesini ve veri sahibi haklarının korunmasını temin edecek şekilde, yalnızca yeterli teknik ve idari tedbirlerin alındığını taahhüt eden veri işleyenlerden faydalanmasını sağlanmayacaktır.
2. Üye Devletler; veri işleyenin, veri sorumlusunun önceden özel veya genel yazılı izni olmaksızın başka bir veri işleyen ile çalışmamasını sağlayacaktır. Genel yazılı izin

verilmesi durumunda, veri işleyen veri sorumlusuna, veri işleyen tarafların değişmesi veya başkaca veri işleyenlerin eklenmesi hususları hakkında bildirimde bulunmasını ve veri sorumlusuna bu değişikliklere itiraz etme hakkı tanımasını sağlayacaktır.

3. Üye Devletler; veri işleyen tarafından kişisel verilerin işlenmesinin, veri sorumlusu ile arasındaki ilişkide veri işleyen bakımından bağlayıcı olacak ve veri işlemenin konusu ve süresi, mahiyeti ve amaçları, kişisel veri tipleri, veri sahibi kategorileri ve veri sorumlusunun hak ve yükümlülükleri hususlarını düzenleyen bir sözleşme ya da Birlik veya Üye Devlet hukuku kapsamında başkaca bir işleme tabi olmasını sağlayacaktır. Bu sözleşme veya başkaca hukuki işlem, veri işleyen bakımından aşağıdaki hükümleri içerecektir:

   a. yalnızca veri sorumlusunun talimatları doğrultusunda kişisel verilerin işlenmesi;
   b. kişisel verileri işlemeye yetkili kişilerin, gizlilik taahhüdünde bulunduklarını veya yeterli kanuni gizlilik yükümlülüğü altında olduklarının temin edilmesi;
   c. veri sahibinin hakları ile ilgili hükümlere uygun hareket edilmesi amacıyla veri sorumlusuna gerekli her türlü desteğin sağlanması;
   d. veri sorumlusunun seçimi doğrultusunda, veri işlemeye konu hizmetlerin sona ermesi ile birlikte, kişisel verileri silinmesi veya veri sorumlusuna iade edilmesi ve Birlik veya Üye Devlet hukuku uyarınca kişisel verilerin saklanmasının zorunlu olmadığı durumlarda, mevcut kopyaların silinmesi;
   e. veri sorumlusuna işbu Madde'ye uygun hareket edildiğinin ispatlanması için gerekli bilgilerin sağlanması;

   f. başkaca bir veri işleyen ile çalışılması halinde ikinci ve üçüncü fıkra kapsamında belirlenen şartların sağlanması.

4. Üçüncü fıkrada atıfta bulunulan sözleşme veya başkaca hukuki işlem, elektronik form da dahil olmak üzere yazılı olarak yapılacaktır.

5. İşbu Direktif hükümlerine aykırı olarak, bir veri işleyenin kişisel verilerin işlenme amaç ve vasıtalarını belirlemesi halinde, veri işleyenin bu kişisel verilerin işlenmesi bakımından veri sorumlusu sıfatıyla hareket ettiği kabul edilecektir.

Madde 23

Veri Sorumlusu veya Veri İşleyen İdaresi Altında Kişisel Verilerin İşlenmesi

1. Birlik veya Üye Devlet hukuku uyarınca zorunlu olmadıkça, Üye Devletler; veri işleyen ve veri sorumlusu veya veri işleyen tarafından yetkilendirilen kişiler ile kişisel verilere erişimi bulunan kişiler, veri sorumlusunun talimatları dışında kişisel verileri işlemeyecektir.

Madde 24

İşleme Faaliyetlerine İlişkin Kayıtlar

1. Üye Devletler; veri sorumlularının kendi sorumlulukları dahilindeki, tüm veri işleme faaliyeti kategorilerinin, aşağıda belirtilen bilgileri içeren bir kaydını tutmalarını sağlayacaktır:

   a. veri sorumlusu ile mevcut olması halinde, birlikte veri sorumlusunun ve veri koruma görevlisinin kimliği ve iletişim bilgileri;
   b. kişisel verilerin işlenme amaçları;

c. üçüncü ülkelerdeki veya uluslararası kuruluşlardaki alıcılar da dahil olmak üzere kişisel verilerin aktarıldığı veya aktarılacağı alıcıların kategorileri;
d. veri sahibi ve kişisel veri kategorilerine ilişkin açıklamalar;
e. profilleme faaliyetlerinin yürütülüp yürütülmediğine ilişkin bilgi;
f. mevcut olması halinde, üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılan kişisel veri kategorileri;
g. kişisel verilerin aktarılması da dahil olmak üzere, kişisel verilerin işlenmesinin hukuki sebebi;
h. mümkün olması halinde, farklı kişisel veri kategorileri için öngörülen imha periyotları;
i. mümkün olması halinde, 29'uncu maddenin birinci fıkrası kapsamında düzenlenen teknik ve idari tedbirler.

2. Üye Devletler, veri işleyenlerin, veri sorumlusu adına yürütülen tüm işleme faaliyeti kategorilerinin, aşağıda belirtilen bilgileri içeren bir kaydını tutmalarını sağlayacaktır:

a. veri işleyen veya veri işleyenlerin ve adına veri işlenen veri sorumluları ile mevcut ise, veri koruma görevlisinin kimlik ve iletişim bilgileri;
b. her bir veri sorumlusu adına yürütülen veri işleme faaliyeti kategorileri;
c. uygulanabilir olması halinde, veri sorumlusu tarafından açıkça bu yönde bir talimatın bulunması kaydıyla, üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılan kişisel veri kategorileri ve bu üçüncü ülke veya uluslararası kuruluşa ilişkin bilgi;
d. mümkün olması halinde, 29'uncu maddenin birinci fıkrası kapsamında düzenlenen teknik ve idari tedbirler.

3. Birinci ve ikinci fıkralarda atıfta bulunulan kayıtlar, elektronik form da dahil olmak üzere yazılı olarak tutulacaktır.

Veri sorumlusu ve veri işleyen, bu kayıtları talep üzerine denetleyici makama sunacaktır.

Madde 25
İşlem Kayıtlarının Tutulması

1. Üye Devletler; otomatik veri işleme sistemlerinde en azından aşağıda belirtilen veri işleme faaliyetlerine ilişkin işlem kayıtlarının tutulmasını sağlayacaktır: kişisel verilerin elde edilmesi, değiştirilmesi, başvurulması, aktarılması da dahil olmak üzere üçüncü taraflarla paylaşılması, bir araya getirilmesi ve silinmesi. Kişisel verilere başvurulması ve kişisel verilerin erişime açılması işlemlerine ilişkin işlem kayıtları, söz konusu işlemlerin tarih ve saatlerini ve mümkün olduğu ölçüde kişisel verilere başvuran veya kişisel verileri erişime açan kişinin kimliğini ve bu kişisel verilerin alıcısının kimliğini belirlemeyi mümkün kılacak şekilde tutulacaktır.

2. İşlem kayıtları yalnızca kişisel veri işleme faaliyetlerinin hukuka uygunluğunun tespiti, iç denetim, kişisel verilerin bütünlüğünün ve güveliğinin sağlanması amaçlarıyla ve ceza kovuşturmaları kapsamında kullanılabilecektir.

3. Veri sorumlusu ve veri işleyen, işlem kayıtlarını talep üzerine denetleyici makama sunacaklardır.

Madde 26

Denetleyici Makam ile İş Birliği

1. Üye Devletler; veri sorumlusu ve veri işleyenin talep üzerine denetleyici makamla, görevlerinin icrası doğrultusunda iş birliği içerisinde olmasını sağlayacaktır.
2. Birinci fıkrada atıfta bulunulan değerlendirme, en azından öngörülen işleme faaliyetlerinin genel bir tanımını, veri sahiplerinin hak ve özgürlüklerine yönelik risklerin değerlendirmesini, bu risklerin ortadan kaldırılması için öngörülen önlemleri, kişisel verilerin korunmasına ilişkin gereksinimlere ve bu Direktif gerekliliklerine uygunluğu göstermek, veri sahiplerinin ve ilgili diğer kişilerin hakları ile meşru çıkarlarını dikkate alarak güvenlik tedbirlerini ve mekanizmaları içerecektir.

Madde 27
Veri Koruma Etki Değerlendirmesi

1. Özellikle bir kişisel veri işleme faaliyetleri, yeni teknolojilerin kullanımını ve kişisel veri işlemenin niteliği, kapsamı, içeriği ve amaçları da dikkate alındığında gerçek kişilerin temel hak ve özgülüklerine yönelik yüksek bir risk taşımaktaysa; Üye Devletler, veri sorumlusunun veri işleme faaliyetine başlamadan önce, öngörülen veri işleme faaliyetlerinin kişisel verilerin korunması üzerindeki etkisine ilişkin bir değerlendirme yapmasını sağlayacaktır.

2. Birinci fıkrada atıfta bulunulan değerlendirme, en azından öngörülen işleme operasyonlarının genel bir tanımını, veri sahiplerinin hak ve özgürlüklerine yönelik risklerin değerlendirmesini, bu risklerin ortadan kaldırılması için öngörülen önlemleri, kişisel verilerin korunmasına ilişkin gereksinimlere ve işbu Direktif gerekliliklerine uygunluğu göstermek, veri sahiplerinin ve ilgili diğer kişilerin hakları ile meşru çıkarlarını dikkate alarak güvenlik tedbirlerini ve mekanizmaları içerecektir.

Madde 28
Denetleyici Makamın Görüşüne Başvurulması

1. Üye Devletler; aşağıdaki hallerde, veri sorumlusu veya veri işleyenin, bir veri kayıt sisteminin parçası olmak üzere kişisel verileri işlemeye başlamadan önce denetleyici makamın görüşüne başvurmasını sağlayacaktır:

   a. 27'nci madde uyarınca atıf yapılan veri koruma etki değerlendirmesi ile, veri sorumlusu tarafından risk azaltıcı gerekli tedbirlerin alınmaması halinde; kişisel verilerin işlenmesinin, yüksek risk ile sonuçlanacağına işaret ettiği hallerde; veya,
   b. Özellikle yeni teknolojilerin, mekanizmaların veya prosedürlerin kullanıldığı kişisel verilerin işlenmesine ilişkin faaliyetlerde, veri sahibinin hak ve özgürlükleri bakımından yüksek risk içerdiği hallerde.

2. Üye Devletler; ulusal parlamento tarafından kabul edilen kişisel verilerin korunmasına yönelik yasal düzenlemeler ve bunlara dayalı olarak gerçekleştirilen düzenleyici işlemlere ilişkin taslakların hazırlanma sürecinde, işbu yasal düzenlemelere dayanan düzenleyici tedbirler için hazırlanan taslak süresince, denetleyici makama danışılmasını sağlayacaktır.

3. Üye Devletler; denetleyici makamın birinci fıkra uyarınca önceden görüşünün alınması şartına bağlı kişisel veri işleme faaliyetlerine ilişkin bir liste hazırlamasını sağlayacaktır.

4. 27'nci madde uyarınca, Üye Devletler; veri sorumlusu tarafından denetleyici makama veri koruma etki değerlendirilmesinin sağlanabilmesini düzenleyecek ve talep üzerine,

özellikle, veri sahibinin kişisel verilerinin korunması ve işbu ilgili tedbirlerin alınması olmak üzere denetleyici makamın, kişisel verilerin işlenmesi ile ilgili uyum değerlendirmesi yapmasına izni verecektir.

5. Üye Devletler; denetleyici makam tarafından işbu maddenin birinci fıkrasında atıfta bulunulan işleme faaliyetlerinin işbu Direktif hükümlerini ihlal ettiğinin değerlendirilmesi ve özellikle veri sorumlusu tarafından risk tespiti ve yönetiminin yeterli ölçüde yapılmaması durumlarında, düzenleyici makamın görüş talebinin alınmasını takip eden altı ay içerisinde veri sorumlusu ve uygulanabilir olması halinde, veri işleyene yazılı yönlendirmede bulunmasını ve 47'nci madde uyarınca düzenlenen yetkilerini kullanmasını sağlayacaktır. Bu süre, veri işleme faaliyetinin karmaşıklığı da dikkate alınarak bir ay kadar uzatılabilecektir. Düzenleyici makam, sürenin uzatılmasına ilişkin olarak, uzatma sebeplerini de içerecek şekilde, veri sorumlusuna ve uygulanabilir olması halinde veri işleyene, görüş talebinin alınmasını takip eden bir ay içerisinde bildirimde bulunacaktır.

İkinci Kısım
Kişisel Verilerin Güvenliği

Madde 29
Veri İşleme Faaliyetlerinin Güvenliği

1. Üye Devletler, başta 10'uncu madde kapsamında düzenlenen özel nitelikli kişisel verilerin işlenmesi olmak üzere, veri sorumlusu tarafından, en son teknolojiyi, uygulama maliyetini ve işlemenin mahiyetini, kapsamını, bağlamını, amaçlarını ve bunların yanı sıra gerçek kişilerin hak ve özgürlükleri üzerindeki çeşitli riskleri ve gerçekleşme olasılıklarını da dikkate alarak, risk düzeyine uygun teknik ve idari tedbirlerin alınmasını sağlayacaktır.

2. Kişisel verilerin otomatik yollarla işlenmesine ilişkin olarak, her bir Üye Devlet veri sorumlusu tarafından, bir risk değerlendirmesini takiben aşağıdaki amaçlarla tasarlanan tedbirlerin alınmasını sağlayacaktır:

   a. Kişisel verilerin işlenmesinde kullanılan donanımlara yetkisiz kişilerce erişilmesinin önlenmesi ("donanım erişim kontrolü");
   b. Kişisel verilerin üzerinde kayıtlandığı ortamların yetkisiz kişiler tarafından okunmasının, kopyalanmasının veya değiştirilmesinin önlenmesi ("medya kontrolü");
   c. Depolanmış kişisel verilerin yetkisiz kişiler tarafından incelenmesi, değiştirilmesi veya silinmesi ile yetkisiz kişiler tarafından veri girişi yapılmasının önlenmesi ("depolama kontrolü");
   d. Veri iletişim donanımları kullanılarak, otomatik işleme sistemlerine yetkisiz kişiler tarafından erişilmesinin önlenmesi ("kullanıcı kontrolü");
   e. Otomatik işleme sistemlerini kullanmak üzere yetkilendirilmiş kişilerin yalnızca yetkilendirme kapsamı ile sınırlı olacak şekilde erişimlerinin sağlanması ("erişim kontrolü");
   f. Veri iletişim donanımları kullanılarak, kişisel verilerin hangi makamlar ile paylaşıldığı, paylaşılacağı veya hangi makamların erişimine açıldığının belirlenebilmesinin sağlanması ("iletişim kontrolü");
   g. Otomatik işleme sistemlerine hangi verilerin girişinin yapıldığı ve bu girişlerin kimler tarafından ve ne zaman gerçekleştirildiğinin sonradan doğrulanabilmesinin sağlanması ("veri girişi kontrolü");

h. Kişisel verilerin aktarıldığı veya kişisel verilerin üzerin kayıtlandığı ortamların taşındığı durumlarda, kişisel verilerin yetkisiz kişilerce okunmasının, kopyalanmasının, değiştirilmesinin ya da silinmesinin engellenmesi ("taşıma kontrolü");
i. Kesinti halinde, kurulu sistemlerin eski haline getirilmesinin sağlanması ("kurtarma");
j. Sistemin tüm fonksiyonlarının işlerliğinin sağlanması, fonksiyonlarda ortaya çıkan hataların raporlanması ("güvenilirlik"), ve sistemin çalışmasında herhangi bir sorun yaşanması halinde kişisel verilerin bütünlüğünün bozulmamasının sağlanması ("bütünlük").

Madde 30

Kişisel Veri İhlalinin Denetleyici Makama Bildirilmesi

1. Üye Devletler, kişisel veri ihlali gerçekleşmesi durumunda, kişisel veri ihlalinin gerçek kişilerin hak ve özgürlüklerine karşı bir risk oluşturmasının beklenmediği durumlar hariç olmak üzere, ihlalin veri sorumlusu tarafından gecikmeksizin ve durum elverildiği ölçüde, ihlalin öğrenilmesinden itibaren en geç 72 saat içerisinde denetleyici makama bildirilmesini sağlayacaktır.

2. Veri işleyen, kişisel veri ihlalinin öğrenilmesini takiben gecikmeksizin ihlali veri sorumlusuna bildirir.

3. Birinci fıkrada atıfta bulunulan bildirim, asgari olarak aşağıdaki hususları kapsayacaktır:
   (a) Kişisel veri ihlalinin, mümkünse ilgili veri sahiplerinin kategorileri ve yaklaşık sayısı ve ilgili kişisel veri kayıtlarının kategorileri ve yaklaşık sayısı dahil olmak üzere, niteliğin tarifi;
   (b) Veri koruma yetkilisi veya daha fazla bilgi alınabilecek diğer irtibat kişilerinin isimleri ve iletişim bilgileri;
   (c) Kişisel veri ihlalinin muhtemel sonuçları;
   (d) Kişisel veri ihlali karşısında alınan veya alınması teklif edilen tedbirlerin, uygun/mümkün olması durumunda olası olumsuz etkileri azaltabilecek tedbirler de dahil olmak üzere, tarifi.

4. Tüm bilgilerin aynı anda bildirilmesinin mümkün olmadığı sürece, bilgiler daha fazla gecikmeye yer vermeden aşamalar halinde bildirilebilecektir.

5. Üye Devletler, birinci fıkrada belirtilen kişisel veri ihlallerinin ihlale ilişkin gerçekleri, ihlalin etkilerini ve alınan düzeltici tedbirleri de içerecek şekilde veri sorumlusu tarafından belgelenmesini sağlayacaklardır. Söz konusu belgeleme, denetleyici makamın bu maddeye uygunluk denetimini yapabilmesini sağlayacaktır.

6. İhlal edilen kişisel verinin başka bir Üye Devlet'in veri sorumlusu tarafından veya başka bir Üye Devlet'in veri sorumlusu ile paylaşılmış olması durumunda Üye Devletler, üçüncü fıkrada belirtilen bilgilerin o Üye Devlet'in veri sorumlusu ile makul süre aşılmaksızın paylaşılmasını sağlayacaklardır.

Madde 31

Kişisel Veri İhlalinin Veri Sahibine İletilmesi

1. Üye Devletler, kişisel veri ihlalinin gerçek kişilerin hak ve özgürlüklerine karşı yüksek bir risk oluşturmasının muhtemel olduğu durumlarda, sorumlunun kişisel verilerin ihlalini veri sahibine makul olan süreyi aşmaksızın iletmesini sağlayacaktır.
2. Bu maddenin 1'inci fıkrasında değinilen veri sahibiyle iletişim, kişisel veri ihlalinin niteliğini açık ve net bir dilde açıklayacak ve en azından 30'uncu maddenin 3'üncü fıkrasının (b), (c) ve (d) bentlerinde değinilen bilgi ve tedbirleri içerecektir.

3. Aşağıdaki koşullardan herhangi birinin karşılanması durumunda, 1'inci fıkrada değinilen veri sahibi ile iletişim gerekli olmayacaktır:

   (a) sorumlu, uygun teknolojik ve organizasyonel koruma önlemlerini uygulamış ve bu önlemler, kişisel veri ihlalinden etkilenen kişisel verilere, özellikle de kişisel verileri şifreleme gibi erişme yetkisi olmayan herhangi bir kişiye karşı anlaşılmaz hale getirenlere uygulanmıştır;
   (b) sorumlu, 1'inci fıkrada değinilen veri sahiplerinin hak ve özgürlüklerine yönelik yüksek riskin artık gerçekleşmemesini sağlayacak müteakip önlemleri almıştır;
   (c) orantısız bir çaba içerecektir. Böyle bir durumda, bunun yerine, veri sahiplerinin eşit derecede etkili bir şekilde bilgilendirildiği bir kamuya açık iletişim veya benzer bir tedbir olacaktır.

4. Eğer sorumlu, kişisel veri ihlalini veri sahibine halihazırda iletmediyse, denetleyici makam, kişisel veri ihlalinin yüksek bir riskle sonuçlanma olasılığını göz önüne alarak, 3'üncü fıkrada değinilen koşullardan herhangi birinin yerine getirilmesine karar verebilir veya bunu yapmasını gerektirebilir.

5. Bu maddenin 1'inci fıkrasında düzenlenen veri sahibine iletim, 13'üncü maddenin 3'üncü fıkrasında düzenlenen şart ve koşullara bağlı olarak ertelenebilecektir, kısıtlanabilecektir veya atlanabilecektir.

Üçüncü Kısım
Veri Koruma Görevlisi

Madde 32
Veri Koruma Görevlisinin Atanması

1. Üye Devletler, veri sorumlusu için, veri koruma memuru atanmasını sağlayacaktır. Üye devletler, işbu yükümlülük nedeniyle kendi yargı kapsamı içinde hareket ettiği hallerde, mahkeme ve diğer bağımsız yargı makamlarını muaf tutabilecektir.

2. Veri koruma memuru, kendisinin mesleki niteliği ve özellikle kendisinin veri koruma hukukuna dair uzman bilgisine sahip olması ve 34'üncü madde uyarınca atıf yapılan görevleri yerine getirebilme ve yerine getirebilme yetisi dikkate alınmak üzere atanacaktır.

3. Organizasyonel yapısı ve boyutu dikkate alınmak üzere, muhtelif yetkili makamlar tarafından tek bir veri koruma memuru atanabilecektir.

4. Üye devletler, veri sorumlusu için, veri koruma memurunun, iletişim bilgilerinin yayınlanmasını ve denetim makamıyla irtibata geçebilmelerini sağlayacaktır.

Madde 33
Veri Koruma Görevlisinin Konumu

1. Kişisel verilerin kullanılması ile ilgili tüm hususlar dahil olmak üzere, Üye Devletler, veri sorumlusu için, veri koruma görevlisinin uygun ve vaktinde yerinde bulunmasını sağlar.

2. 34'üncü madde uyarınca atıf yapılan görevlerin veri koruma görevlisi tarafından yerine getirilmesinde, veri sorumlusu, işbu görevlerin yerine getirilebilmesi için gerekli kaynakların, kişisel verilere erişilebilmesinin ve işleme faaliyetlerinin temin edilmesini sağlayacak ve uzman bilgisini sürdürmesini destekleyecektir.

Madde 34
Veri Koruma Görevlisinin Görevleri

1. Üye Devletler, veri sorumlusu için, veri koruma görevlisinin asgari olarak aşağıdaki görevleri yerine getirmesini düzenleyecektir:

   a. Veri sorumlusunu ve işbu Direktif ve Birlik ve Üye Devletler'in diğer veri koruması hükümleri uyarınca işleme yükümlülüklerini yerine getiren personelleri bilgilendirmek ve tavsiye vermek;
   b. Sorumluluk atama, farkındalık yaratma, işleme faaliyeti sırasında personel eğitimi ve ilgili hesap denetimi dahil olmak üzere, işbu Direktif ile, Birlik ve Üye Devletler'in diğer veri koruması hükümleri ve kişisel verilerin korunması ile ilgili veri sorumlusu ilkeleriyle uyumluluğunu denetlemek.
   c. Talep edildiği zaman veri koruma etki değerlendirmesi hususunda tavsiye vermek ve 27'nci madde uyarınca performansını/çalışma niteliğini gözlemlemek.
   d. Denetleyici makamla iş birliği yapmak.
   e. 28'inci madde uyarınca atıf yapılan ilk danışma dahil olmak üzere, işleme ile ilgili olan hususlarda, denetleyici makam için irtibat kişisi olarak hareket etmek ve uygun olması halinde, başka bir konuyla ilgili olarak danışmak.

BEŞİNCİ BÖLÜM
Kişisel Verilerin Üçüncü Ülkelere veya Uluslararası Kuruluşları Aktarımı

Madde 35
Kişisel Verilerin Aktarılmasına İlişkin Genel İlkeler

1. Üye Devletler, işlem yapılmakta olan, veya üçüncü bir ülkeye aktarıldıktan sonra işlenmesi amaçlanan veya üçüncü bir ülkeye ileriye yönelik aktarımlar da dahil olmak üzere uluslararası bir örgüte aktarıldıktan sonra işlenmesi amaçlanan veya uluslararası bir kuruluşa aktarıldıktan sonra işlenmek üzere tasarlanan kişisel verilerin, yetkili makamlar tarafından, işbu Direktif'in diğer hükümleri uyarınca kabul edilen ulusal hükümlere uymaya tabi olarak yalnızca bu Bölüm'de düzenlenen şartların yerine getirilmesi durumunda herhangi bir aktarımı sağlayacaktır, şöyle ki;

   (a) 1'inci maddede düzenlenen amaçlar için aktarma gerekmektedir;
   (b) kişisel veriler, 1'inci madde birinci fıkrasında düzenlenen amaçlar için yetkili bir makam olan üçüncü bir ülke veya uluslararası bir kuruluştaki sorumluya aktarılmaktadır;
   (c) kişisel verilerin başka bir Üye Devlet'ten iletildiği veya temin edildiği durumlarda, Üye Devlet ulusal hukukuna uygun olarak aktarımına önceden izin vermiş ise;

(d) Komisyon, 36'ncı madde uyarınca bir yeterlilik kararını kabul etmiş veya böyle bir kararın yokluğunda, 37'nci madde uyarınca uygun güvenceler sağlanmış veya mevcut olmuş veya 36'ncı madde uyarınca bir yeterlilik kararı ve 37'nci madde uyarınca uygun güvencelerin bulunmaması halinde, 38'inci madde uyarınca belirli durumlara yönelik istisnalar uygulanmaktadır; ve
(e) başka bir üçüncü ülkeye veya uluslararası kuruluşa yapılan bir aktarma söz konusu olduğunda, aynı Üye Devlet'in asıl aktarmasını yapan yetkili makam veya diğer yetkili makam, cezai suçun ciddiyeti, kişisel verilerin orijinal olarak aktarılma amacı ve üçüncü ülkede kişisel verilerin korunması seviyesi veya kişisel verilerin aktarıldığı uluslararası bir organizasyon dahil olmak üzere ilgili tüm faktörleri dikkate aldıktan sonra, ileriye yönelik aktarmayı yetkilendirir.

2. Üye Devletler, bir Üye Devlet'in veya üçüncü bir ülkenin kamu güvenliğine yönelik acil ve ciddi bir tehdidin önlenmesi veya bir Üye Devlet'in temel çıkarları için kişisel verilerin aktarılmasının gerekli olması durumunda, 1'inci fıkranın (c) bendine uygun olarak başka bir Üye Devlet tarafından ön izin alınmadan aktarımlar sağlayacaktır. Ön izin vermekten sorumlu makam gecikmeden bilgilendirilecektir.

3. Bu Bölüm'deki tüm hükümler, işbu Direktif tarafından sağlanan gerçek kişilerin korunma seviyelerine zarar vermemesini sağlamak amacıyla uygulanacaktır.

Madde 36
Bir Yeterlilik Kararı Temelinde Aktarım

1. Üye Devletler, kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarımının, Komisyon'un üçüncü ülke, bu üçüncü ülke içindeki bir bölge veya bir ya da daha fazla belirli bölüm veya uluslararası kuruluşun yeterli koruma seviyesini sağladığına karar verdiği durumlarda gerçekleşebilmesini sağlayacaktır. Bu tür bir aktarım özel bir izin gerektirmeyecektir.

2. Koruma seviyesinin yeterliliğini değerlendirirken, Komisyon, özellikle, aşağıdaki unsurları dikkate alacaktır:
   a. Hukukun üstünlüğü, insan haklarına ve temel özgürlüklere saygı, kamu güvenliği, savunma, ulusal güvenlik ve ceza hukuku ve resmi makamların kişisel verilere erişiminin yanı sıra bu tür mevzuatın uygulanmasını da içeren genel ve sektörel ilgili mevzuatı, kişisel verilerin üçüncü bir ülke veya uluslararası kuruluşa ileriye yönelik aktarımı için o ülkede veya uluslararası kuruluşta uyulması gereken kurallar da dahil olmak üzere veri koruma kuralları, mesleki kurallar ve güvenlik önlemleri, içtihat ve ayrıca etkili ve uygulanabilir veri sahibi hakları ile kişisel verisi aktarılan veri sahipleri için etkili idari ve adli yollar;
   b. Üçüncü bir ülkedeki veya uluslararası bir kuruluşun tabi olduğu, yetkilerin yeterli icrası dahil olmak üzere veri koruma kurallarını uygulamak ve veri koruma kurallarına uyumu sağlamak, veri sahiplerine haklarını kullanmada yardımcı olmak ve tavsiyelerde bulunmak ve Üye Devletler'in denetleyici makamları ile işbirliği yapmaktan sorumlu, bir veya daha fazla denetleyici makamın varlığı ve etkili işleyişi;
   c. İlgili üçüncü ülke veya uluslararası kuruluşun bulunmuş olduğu uluslararası taahhütler veya özellikle kişisel verilerin korunmasıyla ilgili olarak çok taraflı veya bölgesel sistemlere katılımının yanı sıra hukuki

olarak bağlayıcı sözleşmelerden veya belgelerden kaynaklanan diğer yükümlülükler.

3. Komisyon, koruma seviyesinin yeterliliğini değerlendirdikten sonra, uygulama tasarrufu yoluyla, üçüncü bir ülke, üçüncü bir ülke içindeki bir bölge veya bir ya da daha fazla belirli bölüm veya uluslararası bir kuruluşun işbu Madde'nin ikinci fıkrasındaki anlamıyla yeterli koruma seviyesini sağladığına karar verebilir. Uygulama tasarrufu, üçüncü ülke veya uluslararası kuruluştaki tüm ilgili gelişmeleri dikkate alan en az dört yılda bir periyodik inceleme için bir mekanizma sağlayacaktır. Uygulama tasarrufu, bölgesel ve sektörel uygulamasını belirtecek ve uygulanabilir olduğunda, işbu Madde'nin 2'nci fıkrasının (b) bendinde atıf yapılan denetleyici makam veya makamları tespit edecektir. Uygulama tasarrufu, 58'inci maddenin ikinci fıkrasında belirtilen inceleme usulüne uygun olarak kabul edilecektir.

4. Komisyon, üçüncü ülkeler ve uluslararası kuruluşlardaki üçüncü fıkra uyarınca kabul edilen kararların işleyişini etkileyebilecek gelişmeleri sürekli olarak izleyecektir.

5. Komisyon, özellikle işbu Madde'nin üçüncü fıkrasında belirtilen incelemeyi takiben, mevcut bilgilerin üçüncü bir ülke, üçüncü bir ülke içindeki bir bölge veya bir ya da daha fazla belirli bölüm veya uluslararası bir kuruluşun işbu Madde'nin ikinci fıkrasındaki anlamıyla yeterli koruma seviyesini artık gerekli ölçüde sağlamadığını ortaya koyduğu hallerde işbu Madde'nin üçüncü fıkrasında atıf yapılan kararı geriye dönük etkisi olmayan uygulama tasarrufları yoluyla kaldıracak, değiştirecek veya askıya alacaktır. Bu uygulama tasarrufları, 58'inci maddenin ikinci fıkrasında belirtilen inceleme usulüne uygun olarak kabul edilecektir.

   Usulüne uygun olarak gerekçelendirilen zorunlu aciliyet hallerinde, Komisyon, derhal 58'inci maddenin üçüncü fıkrasında atıf yapılan usule göre uygulanabilir uygulama tasarrufları kabul edecektir.

6. Komisyon, 5'inci fıkra uyarınca verilen karara neden olan durumun giderilmesi amacıyla üçüncü ülke veya uluslararası kuruluşla istişarelerde bulunacaktır.

7. Üye Devletler, 5'inci fıkraya göre bir kararın, kişisel verilerin üçüncü ülkeye, bölgeye veya bu üçüncü ülke içindeki bir veya daha belirli bölüme veya uluslararası kuruluşa 37'nci ve 38'inci maddeler uyarınca aktarımına halel getirmemesini sağlayacaklardır.

8. Komisyon, *Avrupa Birliği Resmi Gazetesi*'nde ve internet sitesinde, yeterli koruma seviyesine sahip olup olmadığına karar verdiği üçüncü ülkelerin, bölgelerin, üçüncü bir ülke içindeki belirli bölümlerin ve uluslararası kuruluşların bir listesini yayınlayacaktır.

Madde 37

Uygun Güvenlik Önlemlerine Tabi Aktarım

1. 36'ncı maddenin üçüncü fıkrası uyarınca alınan bir kararın yokluğu halinde, Üye Devletler, kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarımının aşağıdaki koşulların sağlanması durumunda gerçekleşebileceğini temin edeceklerdir:
   a. Kişisel verilerin korunmasına ilişkin uygun güvencelerin hukuki olarak bağlayıcı bir belgeyle sağlanması; veya
   b. Veri sorumlusunun kişisel veri aktarımına ilişkin tüm durumları değerlendirmesi ve kişisel verinin korunmasına ilişkin uygun güvencelerin var olduğu sonucuna ulaşması.

2. Veri sorumlusu, denetleyici makamı, 1'inci fıkranın (b) bendi uyarınca gerçekleştirilen aktarım kategorileri hakkında bildirecektir.

3. Bir aktarımın 1'inci fıkranın (b) bendine dayanması durumunda, bu tür bir aktarım belgelendirilecek ve aktarma tarih ve saati, alıcı yetkili makam hakkında bilgi, aktarımın gerekçelendirmesi ve aktarılan kişisel veriler de dahil olmak üzere talep üzerine denetleyici makamın erişimine sunulacaktır.

Madde 38
Özel Durumlar İçin İstisnalar

1. 36'ncı maddeye göre bir yeterlilik kararının veya 37'nci madde uyarınca uygun güvencelerin yokluğu halinde, Üye Devletler, üçüncü bir ülkeye veya uluslararası bir kuruluşa yapılacak bir kişisel veri aktarımı veya aktarım kategorisinin yalnızca aktarımın aşağıdakiler için gerekli olması durumunda gerçekleşebileceğini temin edeceklerdir:

    a. Veri sahibinin ya da başka bir kişinin hayati menfaatlerini korumak,
    b. Aktarımı gerçekleştiren Üye Devlet hukukunun öyle öngörmesi halinde, veri sahibinin meşru menfaatlerini korumak,
    c. Üçüncü bir ülkenin veya bir Üye Devlet'in kamu güvenliğine yönelik ciddi ve mevcut bir tehdidi önlemek,
    d. Özel durumlar, 1'inci maddenin birinci fıkrasında belirtilen amaçlar için veya,
    e. Özel bir durumda, 1'inci maddenin birinci fıkrasında belirtilen amaçlarla ilgili hukuki iddiaların oluşturulması, kullanılması veya ileri sürülmesi için.

2. Kişisel veriler, veri aktaran yetkili makamın ilgili veri sahibinin temel hak ve özgürlüklerinin 1'inci fıkranın (d) ve (e) bentlerinde düzenlenen aktarımın yapılmasındaki kamu yararına üstün geldiğini tespit etmesi halinde aktarılmayacaktır.

3. Bir aktarımın 1'inci fıkraya dayanması halinde, bu tür bir aktarım belgelendirilecek ve aktarma tarih ve saati, alıcı yetkili makam hakkında bilgi, aktarımın gerekçelendirmesi ve aktarılan kişisel veriler de dahil olmak üzere talep üzerine denetleyici makamın erişimine sunulacaktır.

Madde 39
Kişisel Verilerin Üçüncü Ülkelerdeki Alıcılara Aktarımı

1. Birlik veya Üye Devlet hukuku, 35'inci maddenin birinci fıkrasının (b) bendini uygulama dışında tutma yoluyla ve işbu Madde'nin 2'nci fıkrasında atıf yapılan herhangi bir uluslararası antlaşmaya halel getirmeksizin, bireysel ve özel durumlarda, işbu Direktif'in diğer hükümlerine uyulduğu ve aşağıdaki koşulların tümü yerine getirildiği takdirde, 3'üncü maddenin 7'nci fıkrasının (a) bendinde atıf yapılan yetkili makamların kişisel verileri doğrudan üçüncü ülkelerdeki alıcılara aktarımını sağlayabilecektir:

    (a) Aktarım, 1'inci maddenin birinci fıkrasında belirtilen amaçlar için Birlik veya Üye Devlet Hukuku uyarınca öngörülen aktaran yetkili makamın görevinin ifası amacıyla kesinlikle gereklidir;

(b) Veri aktaran yetkili makam, söz konusu durumda, ilgili veri sahibinin temel hak ve özgürlüklerinin, aktarımı gerektiren kamu menfaatine baskın gelmediğini tespit etmektedir;
(c) Veri aktaran yetkili makam, üçüncü bir ülkede 1'inci maddenin birinci fıkrasında belirtilen amaçlar için yetkili olan bir makama aktarımın, özellikle de aktarımın iyi bir zamanda gerçekleştirilememesi nedeniyle etkisiz veya uygunsuz olduğunu kanaatindedir;
(d) Üçüncü bir ülkede 1'inci maddenin birinci fıkrasında belirtilen amaçlar için yetkili olan makam, etkisiz veya uygunsuz olmadığı sürece gecikme olmadan bilgilendirilmektedir;
(e) Veri aktaran yetkili makam, alıcıyı, kişisel verilerin, bu tür veri işlemenin gerekli olması kaydıyla, yalnızca alıcı tarafından belirli amaç veya amaçlar için işleneceği hakkında bilgilendirmektedir.

2. 1'inci fıkrada atıf yapılan uluslararası bir antlaşma, cezai konularda adli iş birliği ve polis iş birliği alanında Üye Devletler ile üçüncü ülkeler arasında yürürlükte olan herhangi bir ikili veya çok taraflı uluslararası antlaşma olacaktır.

3. Veri aktaran yetkili makam, işbu Madde kapsamındaki aktarımlar hakkında denetleyici makamı bilgilendirecektir.

4. Bir aktarımın 1'inci fıkraya dayandığı durumlarda, bu aktarım belgelendirilecektir.

Madde 40
Kişisel Verilerin Korunması İçin Uluslararası İş Birliği

1. Üçüncü ülkeler ve uluslararası kuruluşlarla ilgili olarak, Komisyon ve Üye Devletler aşağıdakilere yönelik uygun adımları atacaktır:

a. kişisel verilerin korunmasına ilişkin mevzuatın etkili bir şekilde uygulanmasını kolaylaştırmak için uluslararası iş birliği mekanizmaları geliştirmek,
b. kişisel verilerin ve diğer temel hak ve özgürlüklerin korunmasına yönelik uygun güvencelere tabi olmak üzere bildirim, şikayet başvurusu, soruşturma yardımı ve bilgi alışverişi dahil olmak üzere kişisel verilerin korunmasına ilişkin mevzuatın uygulanmasında uluslararası karşılıklı yardım sağlamak,
c. kişisel verilerin korunmasına ilişkin mevzuatın uygulanmasında uluslararası iş birliğini ilerletmeyi amaçlayan tartışmalara ve faaliyetlere ilgili paydaşları dahil etmek,
d. üçüncü ülkelerle olan yetki uyuşmazlıkları da dahil olmak üzere kişisel verilerin korunması mevzuatı ve uygulamasının alışverişini ve belgelendirilmesini teşvik etmek.

ALTINCI BÖLÜM
Bağımsız Denetleyici Makamlar

Birinci Kısım
Bağımsız Statü

Madde 41
Denetleyici Makam

1. Her Üye Devlet, veri işleme ile ilgili olarak gerçek kişilerin temel hak ve özgürlüklerinin korunması ve Birlik içerisinde kişisel verilerin serbest dolaşımının kolaylaştırılması için

işbu Direktif'in uygulanmasını izlemekle görevli bir veya daha fazla bağımsız resmi makam öngörecektir ("denetleyici makam").

2. Her denetleyici makam, işbu Direktif'in Birlik genelinde tutarlı bir biçimde uygulanmasına katkıda bulunacaktır. Bu amaç doğrultusunda, denetleyici makamlar birbirleriyle ve Komisyon ile 7'nci Bölüm'e uygun olarak iş birliği yapacaklardır.

3. Üye Devletler, 2016/679 (AB) sayılı Regülasyon uyarınca kurulmuş bir denetleyici makamın işbu Direktif'te atıf yapılan denetleyici makam olmasını ve işbu Madde'nin birinci fıkrası uyarınca kurulacak denetim makamının görevlerini üstlenmesini sağlayabileceklerdir.

4. Bir Üye Devlet'te birden fazla denetleyici makam kurulmuş olması halinde, Üye Devlet, bu denetleyici makamlardan hangisinin 51'inci maddede atıf yapılan Kurul'da bu makamları temsile yetkili olduğunu belirleyecektir.

Madde 42
Bağımsızlık

1. Her Üye Devlet, her bir denetleyici makamın işbu Direktif'e uygun olarak görevlerini yerine getirirken ve yetkilerini kullanırken tam bağımsız hareket etmesini sağlayacaktır.

2. Üye Devletler, denetleyici makamlarının üye veya üyelerinin, dolaylı veya doğrudan dış etkenlerden etkilenmeden, kimseden talimat almadan ve beklemeden, görevlerini işbu Direktif'e uygun olarak yerine getirmelerini ve yetkilerini işbu Direktif'e uygun olarak kullanmalarını sağlayacaktır.

3. Üye Devletler'in denetleyici makamlarının üyeleri görevleriyle bağdaşmayan her türlü eylemden kaçınacak ve memuriyetleri süresince, kazanç getirsin veya getirmesin, görevleriyle bağdaşmayan herhangi bir iş ile meşgul olamayacaklardır.

4. Her Üye Devlet, her bir denetleyici makama, karşılıklı yardımlaşma, iş birliği ve Kurul'a katılım bağlamında yapılacaklar da dahil olmak üzere, görevlerinin etkin bir şekilde ifası ve yetkilerinin icrası için gerekli olan insani, teknik ve mali kaynakları, yerleri ve altyapıyı temin edecektir.
5. Her Üye Devlet, her bir denetleyici makamın, ilgili denetim makamının üye veya üyelerinin münhasır yönetimine tabi olacak çalışanlara sahip olmasını ve bunları kendisinin seçmesini sağlayacaktır.

6. Her Üye Devlet, her bir denetleyici makamın, bağımsızlığını etkilemeyecek mali kontrole tabi olmasını ve genel devlet bütçesinin veya ulusal bütçenin bir parçası olabilecek ayrı, kamuya açık yıllık bütçeye sahip olmasını sağlayacaktır.

Madde 43
Denetleyici Makam Üyeleri İçin Genel Koşullar

1. Üye Devletler, denetleyici makamlarının her bir üyesinin aşağıdakilerden biri tarafından şeffaf bir prosedürle atanmasını sağlayacaktır:

- parlamentoları;
- hükümetleri;
- Devlet başkanları; veya

- Üye Devlet hukukuna göre atanma ile görevlendirilmiş bağımsız bir organ.

2. Her üye, özellikle kişisel verilerin korunması alanında, görevlerinin ifası ve yetkilerinin icrası için gerekli niteliklere, deneyime ve becerilere sahip olacaktır.

3. Bir üyenin görevleri, ilgili Üye Devlet'in hukukuna uygun olarak, görev süresinin sona ermesi, istifa etmesi veya zorunlu emeklilik durumunda sona erecektir.

4. Bir üye yalnızca ciddi bir suiistimal durumunda veya üye artık görevlerin ifası için gereken koşulları yerine getirmediği takdirde görevden alınacaktır.

Madde 44
Denetleyici Makamın Kurulması Hakkında Kurallar

1. Her Üye Devlet, aşağıdakilerin tümünü yasa ile sağlayacaktır:

(a) her denetleyici makamın kurulmasını,
(b) her denetleyici makamın bir üyesi olarak atanabilmek gereken nitelikler ve uygunluk koşulları,
(c) her denetleyici makamın üyesinin veya üyelerinin atanmasına ilişkin kural ve prosedürleri,
(d) 6 Mayıs 2016 tarihinden sonra yapılacak ilk atama hariç, dört yıldan az olmamak üzere her denetleyici makamın üye veya üyelerinin görev süresi, denetleyici makamın bağımsızlığının korunması için gerekli olduğunda aşamalı bir atama prosedürü yoluyla daha kısa bir süre için gerçekleşebilecek olan kısmı,
(e) her biri denetleyici makam üye veya üyelerinin yeniden atanıp atanamadıklarını ve eğer atanabiliyorlarsa kaç kez yeniden atanabildiklerini,
(f) her denetleyici makamın üye veya üyelerinin ve çalışanlarının yükümlülüklerini düzenleyen koşullar, görev süresi boyunca ve sonrasında uygun olmayan eylemler, işler ve menfaatler ile ilgili yasaklar ve istihdamın sona ermesine ilişkin kuralları.

2. Her denetleyici makamın üye veya üyeleri ve çalışanı, Birlik veya Üye Devlet yasalarına uygun olarak, yetkilerinin icrası veya görevlerinin ifası sırasında edindikleri her türlü gizli bilgi ile ilgili olarak görev süreleri boyunca ve görev süresi sonrasında mesleki gizlilik yükümlülüğüne tabi olacaktır. Görev süreleri boyunca, bu mesleki gizlilik yükümlülüğü, özellikle gerçek kişilerin işbu Direktif'in ihlal edildiğine dair raporlamalarında uygulanır.

İkinci Kısım
Yeterlik, Görevler ve Yekiler

Madde 45
Yetki

1. Her Üye Devlet, kendi topraklarında, her denetleyici makamın, işbu Direktif'e uygun olarak, verilen görevlerin yerine getirilmesi ve verilen yetkilerin kullanılması için yetkili olmasını sağlayacaktır.
2. Her Üye Devlet, her denetleyici makamın, mahkemelerin adli yetkilerinde hareket ederken yapmış oldukları işleme faaliyetlerinin denetimi hususunda yetkili olmamasını sağlayacaktır. Üye Devletler, denetleyici makamlarının, diğer bağımsız adli makamların

adli yetkilerinde hareket ederken yapmış oldukları işleme faaliyetlerinin denetimi hususunda yetkili olmamasını sağlayabilir.

Madde 46
Görevler

1. Her Üye Devlet kendi ülkesindeki her denetleyici makamın aşağıdaki görevleri yerine getirmesini sağlayacaktır:

   a. İşbu Direktif ve onun uygulama düzenlemeleri uyarınca kabul edilen hükümlerin uygulanmasını yürütmek ve izlemek,
   b. Kamu farkındalığını ve veri işleme ile ilgili risklerin, kuralların, güvencelerin ve hakların anlaşılmasını teşvik etmek,
   c. Üye Devlet hukukuna uygun olarak, ulusal parlamentoya, hükümete ve diğer kurum ve kuruluşlara gerçek kişilerin veri işleme ile ilgili hak ve özgürlüklerinin korunmasına ilişkin yasal ve idari önlemler konusunda tavsiyelerde bulunmak,
   d. Veri sorumlularının ve veri işleyenlerin işbu Direktif kapsamındaki yükümlülüklerine farkındalığını arttırmak,
   e. Talep üzerine, herhangi bir veri sahibine işbu Direktif uyarınca var olan haklarının kullanılmasına ilişkin bilgi vermek ve eğer uygunsa diğer Üye Devletler'deki denetim makamları ile bu amaçla iş birliği yapmak,
   f. 55'inci madde uyarınca bir veri sahibi veya bir organ, kuruluş veya birlik tarafından yapılan şikayetleri ele almak ve şikayetin konusunu uygun ölçüde soruşturmak ve şikayet edeni, özellikle başka bir denetleyici makam ile daha fazla araştırma ve uyumlu çalışma gerekliyse, soruşturmanın ilerleyişi ve sonucu hakkında makul bir süre içinde bilgilendirmek,
   g. 17'nci madde uyarınca işlemenin hukuka uygunluğunu kontrol etmek ve veri sahibini bu maddenin üçüncü fıkrası uyarınca kontrolün sonucu veya kontrolün gerçekleştirilmemesinin sonuçları hakkında makul bir süre içinde bilgilendirmek,
   h. Bilgi paylaşımı da dahil olmak üzere, işbu Direktif'in uygulanmasının ve tutarlılığının sağlanması amacıyla, diğer denetleyici makamlarla iş birliği yapmak ve karşılıklı yardım sağlamak,
   i. Başka bir denetleyici veya diğer resmi makamdan elde edilen bilgilere dayanan soruşturmalar da dahil olmak üzere, işbu Direktif'in uygulanması hakkında soruşturmalar yürütmek,
   j. Kişisel verilerin korunmasına etkisi olduğu ölçüde, özellikle iletişim ve bilgi teknolojilerindeki gelişmeler olmak üzere, ilgili gelişmeleri izlemek,
   k. 28'inci maddede atıf yapılan veri işleme faaliyetlerine ilişkin tavsiye sağlamak; ve
   l. Kurul'un faaliyetlerine katkıda bulunmak.

2. Her denetleyici makam, diğer iletişim araçlarını dışlamadan elektronik olarak da doldurulabilecek bir şikayet formu sağlanması gibi önlemlerle birinci fıkranın (f) bendinde atıf yapılan şikayetlerin yapılmasını kolaylaştıracaktır.

3. Her denetleyici makamın görevlerinin icrası, veri sahibi ve veri koruma görevlisi için bedelsiz olacaktır.

4. Bir talebin özellikle mükerrer olması sebebiyle açıkça temelden yoksun veya aşırı olması durumunda denetleyici makam, idari masraflar için makul bir ücretlendirme

yapabilir veya talebe ilişkin olarak harekete geçmeyi reddedebilir. Talebin açıkça temelden yoksun veya aşırı olduğunun ispat yükü denetleyici makamın üzerindedir.

Madde 47
Yetkiler

1. Her Üye Devlet, her denetleyici makamın etkin soruşturma yetkisine sahip olmasını kanunen sağlar. Bu yetkiler en azından veri sorumlusundan elde edilecek gücü ve veri işleyenin işlenmekte olan tüm kişisel verilere ve görevlerinin yerine getirilmesi için gerekli tüm bilgilere erişimini içermelidir.

2. Her Üye Devlet, yasa ile, her denetleyici makamın, örneğin aşağıdakiler gibi, etkili düzeltici yetkiye sahip olmasını sağlayacaktır:

   (a) amaçlanan işleme faaliyetlerinin işbu Direktif uyarınca kabul edilen hükümleri ihlali muhtemel olan bir veri sorumlusuna veya veri işleyene uyarılar vermek,
   (b) veri sorumlusu veya veri işleyenin, özellikle 16'ncı madde uyarınca işlemenin kısıtlanmasını veya kişisel verilerin düzeltilmesi veya silinmesini düzenleyerek, işleme faaliyetlerini işbu Direktif uyarınca kabul edilen hükümlerle uyumlu, uygun olduğu belirli bir şekilde ve sürede görmesini sağlamak,
   (c) veri işleme yasağı dahil olmak üzere geçici veya kesin bir sınırlama getirmek.

3. Her Üye Devlet, yasa ile, her denetleyici makamın, veri sorumlusuna 28'inci maddede atıf yapılan önceki istişare usulüne göre tavsiyelerde bulunmak için ve kişisel verilerin korunmasına ilişkin herhangi bir konuda re'sen veya talep üzerine, ulusal parlamentosuna veya hükümetine veya ulusal hukukuna göre diğer kurum ve kuruluşlara, kamuya görüşler vermek için tavsiye niteliğinde yetkilere sahip olmasını sağlayacaktır.

4. İşbu Madde'ye göre denetleyici makama verilen yetkilerin kullanılması, işbu Direktif'e uygun olarak Birlik ve Üye Devlet hukukunda belirtildiği şekilde, etkili yargı yolu ve kanun prosedürü dahil olmak üzere uygun güvencelere tabi olacaktır.

5. Her Üye Devlet, yasa ile, her denetleyici makama, işbu Direktif uyarınca kabul edilen hükümlerin ihlallerini adli makamların dikkatine sunma ve uygun olan hallerde, işbu Direktif uyarınca kabul edilen hükümlerin icrası için, hukuki işlem başlatma veya hukuki işlemlere dahil olma yetkisi tanıyacaktır.

Madde 48
İhlallerin Bildirilmesi

1. Üye Devletler, yetkili makamların, işbu Direktif ihlallerinin gizli raporlanmasını teşvik etmek için etkili mekanizmalar oluşturmasını sağlayacaktır.

Madde 49
Faaliyet Raporları

1. Her denetleyici makam faaliyetleri hakkında, bildirilen ihlal ve uygulanan ceza türlerinin listesini içerebilecek, yıllık bir rapor hazırlayacaktır. Bu raporlar, ulusal parlamentoya, hükümete ve Üye Devlet hukukunca belirlenen diğer makamlara iletilecektir. Bunlar, kamunun, Komisyon'un ve Kurul'un erişimine sunulacaktır.

YEDİNCİ BÖLÜM
İş birliği

Madde 50
Karşılıklı Yardımlaşma

1. Her Üye Devlet, denetleyici makamlarının, işbu Direktif'i tutarlı bir şekilde uygulamak ve tatbik etmek için birbirlerine ilgili bilgi ve karşılıklı yardım sağlamalarını ve birbirleriyle etkin iş birliği için önlemler almasını sağlayacaktır. Karşılıklı yardım, özellikle istişare, denetim ve soruşturma yapılması talepleri gibi bilgi taleplerini ve denetim tedbirlerini kapsayacaktır.

2. Her Üye Devlet, her denetleyici makamın, başka bir denetleyici makamın talebine gecikmeden ve talebi aldıktan sonra en geç bir ay içerisinde cevap vermesi için gerekli tüm uygun önlemleri almasını sağlayacaktır. Bu tür önlemler, özellikle, bir soruşturmanın yürütülmesi ile ilgili bilgilerin iletilmesini içerebilecektir.

3. Yardım talepleri, talebin amacı ve nedenleri de dahil olmak üzere gerekli tüm bilgileri içerecektir. Paylaşılan bilgiler sadece talep edildiği amaç için kullanılacaktır.

4. Talepte bulunulan denetleyici makam, aşağıdakiler haricinde, talebe uymayı reddedemez:
   (a) talebin konusu veya uygulanması istenen tedbirler için yetkili değildir; veya
   (b) talebe uyulması, işbu Direktif'i, Birlik hukukunu veya talebi alan denetleyici makamın tabi olduğu Üye Devlet hukukunu ihlal edecektir.

5. Talepte bulunulan denetleyici makam, talep eden denetleyici makamı sonuçlar veya duruma göre, talebe cevap vermek için alınan kararların ilerleyişi hakkında bilgilendirecektir. Talepte bulunulan denetleyici makam, dördüncü fıkra uyarınca bir talebi herhangi bir şekilde reddi halinde, reddin gerekçelerini açıklayacaktır.

6. Talepte bulunulan denetleyici makamlar, kural olarak, diğer denetleyici makamlar tarafından talep edilen bilgileri standart bir format kullanarak elektronik yollarla sağlayacaktır.

7. Talepte bulunulan denetleyici makamlar, karşılıklı yardım talebine istinaden gerçekleştirdikleri herhangi bir işlem için ücret talep etmeyecektir. Denetleyici makamlar, istisnai durumlarda karşılıklı yardım sağlanmasından kaynaklanan özel harcamalar için birbirlerini tazmin etme hükümleri üzerinde anlaşabileceklerdir.

8. Komisyon, uygulama tasarrufları yoluyla, işbu Madde'de atıf yapılan karşılıklı yardım için biçim ve usulleri ve denetleyici makamlar arasında ve denetleyici makamlar ile Kurul arasında elektronik yollarla bilgi alışverişi için gerekli düzenlemeleri belirleyebilmektedir. Bu uygulama tasarrufları, 58'inci maddenin ikinci fıkrasında atıf yapılan inceleme usulüne uygun olarak kabul edilecektir.

Madde 51

Kurulun Görevleri

1. 2016/679 (AB) sayılı Regülasyon ile oluşturulan Kurul, işbu Direktif kapsamında, veri işleme ile ilgili olarak aşağıda belirtilen görevleri yerine getirecektir:

   a. İşbu Direktif'in herhangi bir değişiklik teklifi dahil olmak üzere, Komisyon'a, kişisel verilerin korunması ile ilgili tüm hususlarda tavsiyede bulunmak,
   b. Kendi inisiyatifiyle, üyelerinden birinin talebi veya Komisyon'un talebi üzerine, işbu Direktif'in uygulanmasıyla ilgili herhangi bir soruyu incelemek ve işbu Direktif'in tutarlı bir şekilde uygulanmasını teşvik etmek için kılavuzlar, tavsiyeler ve iyi uygulama örnekleri çıkarmak,
   c. 47'nci maddenin birinci ve üçüncü fıkrasında atıf yapılan tedbirlerin uygulanması ile ilgili olarak denetleyici makamlar için kılavuzlar oluşturmak,
   d. Kişisel veri ihlallerini saptamak ve kişisel veri ihlallerini bildirmek için bir veri sorumlusu veya veri işleyenin gerekli olduğu özel durumlar için ve 30'uncu maddenin birinci ve ikinci maddelerinde atıf yapılan aşırı gecikmeyi tespit etmek için (b) bendi ile uyumlu olmak üzere kılavuzlar, tavsiyeler ve iyi uygulama örnekleri çıkarmak,
   e. Kişisel veri ihlalinin, 31'inci maddenin birinci fıkrasında atıf yapılan gerçek kişi hak ve özgürlükleri için yüksek risk oluşturabileceği durumlar için (b) bendi ile uyumlu olmak üzere kılavuzlar, tavsiyeler ve iyi uygulama örnekleri çıkarmak,
   f. (b) ve (c) bentlerinde atıf yapılan noktalarda, kılavuzların, tavsiyelerin ve iyi uygulama örneklerinin pratikteki uygulamasını incelemek,
   g. Komisyon'a üçüncü bir ülkede, üçüncü bir ülke içindeki bir bölge veya bir ya da daha fazla belirli bölümde veya uluslararası bir kuruluştaki koruma seviyesinin yeterliliğinin değerlendirilmesi konusunda, bu üçüncü ülke, bölge, belirli bölüm veya uluslararası kuruluşun artık yeterli düzeyde koruma sağlayıp sağlamadığını değerlendirme de dahil olmak üzere, fikir vermek,
   h. Denetleyici makamlar arasında iş birliğini ve iki taraflı ve çok taraflı etkin bilgi alışverişini ve iyi uygulamaları teşvik etmek,
   i. Ortak eğitim aktivitelerini teşvik etmek ve denetim makamları arasında, uygun olması halinde, üçüncü ülkelerin denetleyici makamları veya uluslararası kuruluşlar ile çalışan değişimini kolaylaştırmak,
   j. Veri koruması hukuku ile ilgili belge ve bilgi alışverişini teşvik etmek ve dünya genelindeki denetleyici veri koruma makamları ile pratik yapmak.

   Birinci fıkranın (g) bendi uyarınca, Komisyon, üçüncü ülkelerin hükümeti, bu ülke içerisindeki bölge veya belirli bölüm veya uluslararası kuruluşla yapılan yazışmalar da dahil olmak üzere, gerekli tüm belgeleri Kurul'a sağlayacaktır.

2. Komisyon'un Kurul'dan tavsiye talep etmesi halinde, konunun aciliyeti göz önünde bulundurularak, bir süre sınırı konulabilir.

3. Kurul, fikirlerini, kılavuzlarını, tavsiyelerini ve iyi uygulama örneklerini Komisyon'a ve 58'inci maddenin birinci fıkrasında atıf yapılan komiteye sunacak ve kamuya açıklayacaktır.

4. Komisyon, Kurul tarafından çıkarılan fikirleri, kılavuzları, tavsiyeleri ve iyi uygulama örneklerini takiben verilen kararlarla ilgili Kurul'u bilgilendirecektir.

SEKİZİNCİ BÖLÜM

Yargı Yolları, Sorumluluk ve Cezalar

Madde 52

Denetleyici Makama Şikayette Bulunma Hakkı

1. Başka herhangi bir idari veya yargı yoluna halel getirmeksizin, Üye Devletler, her veri sahibine, kendisine ilişkin kişisel verilerin işlenmesinin işbu Direktif uyarınca kabul edilen hükümleri ihlal ettiğini düşünmesi halinde başvuracağı, tek bir denetleyici makama şikayette bulunma hakkı sağlayacaktır.

2. Üye Devletler, şikayetin 45'inci maddenin birinci fıkrasına göre yetkili denetleyici makama yapılmaması halinde, gecikmesizin, şikayetin yapıldığı denetleyici makamın şikayeti yetkili denetleyici makama iletmesini sağlayacaktır. Veri sahibi bu iletim hakkında bilgilendirilecektir.

3. Üye Devletler, şikayetin yapıldığı denetleyici makama veri sahibinin talebi hakkında daha fazla yardım sağlayacaktır.

4. Veri sahibi, 53'üncü maddeye göre etkili yargı yoluna başvuru olasılığı da dahil olmak üzere, şikayetin durumu ve sonucu hakkında yetkili denetleyici makam tarafından bilgilendirilecektir.

Madde 53

Denetleyici Makama Karşı Etkili Yargı Yolu Hakkı

1. Üye Devletler, başka herhangi bir idari veya adli olmayan yargı yoluna halel getirmeksizin, gerçek veya tüzel kişilere, denetleyici makamların kendileriyle ilgili bağlayıcı kararlarına karşı başvuracağı etkili bir yargı yolu hakkı tanıyacaklardır.

2. Başka herhangi bir idari veya adli olmayan yargı yoluna halel getirmeksizin, her veri sahibi 45'inci maddenin birinci fıkrasına göre yetkili makamın şikayeti sonuçlandırmaması veya veri sahibini 52'nci maddeye göre bulunduğu şikayetin durumu veya sonucu hakkında üç ay içerisinde bilgilendirmemesi halinde başvuracağı etkili bir yargı yolu hakkına sahip olacaktır.
3. Üye Devletler, bir denetleyici makama karşı Üye Devlet mahkemeleri nezdinde başlatılacak işlemlerin, denetleyici makamın kurulduğu yer mahkemeleri önünde görülmesini sağlayacaklardır.

Madde 54

Veri Sorumlusuna veya Veri İşleyene Karşı Etkili Yargı Yolu Hakkı

1. Üye Devletler, 52'nci madde uyarınca denetleyici makama şikayette bulunmak da dahil olmak üzere mevcut herhangi bir idari veya adli olmayan yargı yoluna halel getirmeksizin, kişisel verilerinin bu hükümlere uygun olmayacak şekilde işlenmesi sonucunda veri sahibinin işbu Direktif ile kabul edilen haklarının ihlal edildiğini düşünmesi halinde başvuracağı etkili bir yargı yolu sağlayacaktır.

Madde 55

Veri Sahiplerinin Temsili

1. Üye Devletler, Üye Devlet'in usul hukuku kurallarına göre, veri sorumlusuna, kendi adına 52, 53 ve 54'üncü maddelerde atıf yapılan haklarının ifası ve kendisi adına

şikayette bulunmak için, Üye Devlet hukukuna uygun olarak kurulmuş, kar amacı gütmeyen, kamu yararına meşru hedefleri olan ve kişisel verilerin korunmasına ilişkin olarak veri sahibinin hak ve özgürlüklerinin korunması alanında aktif bir kurum, kuruluş veya birliğe kendisini temsil ettirme hakkı sağlayacaktır.

Madde 56
Tazminat Hakkı

1. Üye Devletler, Üye Devlet hukuku uyarınca yetkili bir makam veya veri sorumlusu tarafından gerçekleştirilen hukuka uygun olmayan bir veri işleme faaliyeti veya işbu Direktif uyarınca kabul edilen ulusal hükümleri ihlal eden herhangi bir eylemin sonucu olarak maddi veya manevi zarar görmüş olan herhangi bir kişinin tazminat alma hakkına sahip olmasını sağlayacaktır.

Madde 57
Ceza

1. Üye Devletler, işbu Direktif uyarınca kabul edilen hükümlerin ihlali için uygulanabilir olan cezalara ilişkin kuralları koyacak ve uygulanmalarını sağlamak için gerekli tüm önlemleri alacaktır. Öngörülen cezalar etkili, ölçülü ve caydırıcı olacaktır.

DOKUZUNCU BÖLÜM
Uygulama Tasarrufları

Madde 58
Komite Prosedürü

1. Komisyon'a, 2016/679 (AB) sayılı Regülasyon'un 93'üncü maddesi ile oluşturulan komite yardımcı olacaktır. Bu komite, 182/2011 (AB) sayılı Regülasyon anlamında bir komite olacaktır.

2. Bu fıkraya atıfta bulunulduğunda, 182/2011 (AB) sayılı Regülasyon'un 5'inci maddesi uygulanacaktır.

3. Bu fıkraya atıfta bulunulduğunda, 5'inci maddesi ile bağlantılı olarak, 182/2011 (AB) sayılı Regülasyon'un 8'inci maddesi uygulanacaktır.

ONUNCU BÖLÜM
Son Hükümler

Madde 59
2008/977/Aİİ Çerçeve Kararı'nın İlgası

1. 2008/977/Aİİ Çerçeve Kararı 6 Mayıs 2018 tarihinden itibaren etkili olmak üzere yürürlükten kaldırılmıştır.

2. Birinci fıkrada belirtilen mülga karara yapılan atıflar işbu Direktif'e yapılmış sayılacaktır.

Madde 60
Halihazırda Yürürlükte Olan Birlik Hukuki Tasarrufları

1. Cezai meselelerde adli ve kolluk iş birliği alanında 6 Mayıs 2016 tarihinde veya daha önce yürürlüğe giren, Üye Devletler arasında veri işlemeyi ve işbu Direktif

kapsamındaki Anlaşmalar uyarınca Üye Devletler'in belirlenmiş makamlarının bilgi sistemlerine erişimini düzenleyen Birlik hukuki tasarruflarındaki kişisel verilerin korunmasına ilişkin özel düzenlemeler etkilenmeden kalacaktır.

Madde 61

Cezai Meselelerde Adli ve Kolluk İş Birliği Alanında Daha Önce Akdedilen Uluslararası Anlaşmalar ile Olan İlişki

1. Üye Devletler tarafından üçüncü ülkelere veya uluslararası kuruluşlara, kişisel veri aktarımını içeren, 6 Mayıs 2016 tarihinden önce akdedilen ve bu tarihten önce geçerli olan Birlik hukuku ile uyumlu uluslararası anlaşmalar tadil edilene, ikame edilene veya kaldırılana kadar yürürlükte kalacaktır.

Madde 62

Komisyon Raporları

1. Komisyon, 6 Mayıs 2022 tarihine kadar ve bundan sonra her dört yılda bir, işbu Direktif'in değerlendirilmesi ve incelenmesi hakkında Avrupa Parlamentosu'na ve Konsey'e rapor sunacaktır. Raporlar kamuya açık olacaktır.

2. Birinci fıkrada atıf yapılan değerlendirmeler ve incelemeler bağlamında, Komisyon, özellikle 36'ncı maddenin üçüncü fıkrası ve 39'uncu madde uyarınca alınan kararlarla ilgili olarak, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına ilişkin Bölüm 5'in uygulanmasını ve işleyişini inceleyecektir.

3. Komisyon, birinci ve ikinci fıkradaki amaçlar doğrultusunda Üye Devletler'den ve denetleyici makamlardan bilgi talep edebilecektir.

4. Komisyon, birinci ve ikinci fıkrada atıf yapılan değerlendirme ve incelemeleri gerçekleştirirken, Avrupa Parlamentosu, Konsey ve diğer ilgili organ veya kaynakların konumlarını ve bulgularını dikkate alacaktır.

5. Komisyon, gerekirse, işbu Direktif'i değiştirmek amacıyla, özellikle bilgi teknolojisindeki gelişmeleri dikkate alarak ve bilgi toplumundaki gelişme ışığında, uygun teklifler sunacaktır.

6. 6 Mayıs 2019'a kadar Komisyon, işbu Direktif'e uyum sağlama ihtiyacını değerlendirmek ve uygun olan hallerde, değişiklik yapmak için gerekli teklifleri sunmak amacıyla işbu Direktif kapsamında kişisel verilerin korunmasına tutarlı bir yaklaşımı temin etmek için Birlik tarafından kabul edilen, yetkili makamlar tarafından 60'ıncı maddede atıf yapılanlar da dahil 1'inci maddenin birinci fıkrasında belirtilen amaçlarla veri işlemeyi düzenleyen diğer hukuki tasarrufları inceler.

Madde 63

İç Hukuka Aktarma

1. Üye Devletler, 6 Mayıs 2018 tarihine kadar işbu Direktif'e uymak için gereken yasaları, regülasyonları ve idari düzenlemeleri kabul edecek ve yayınlayacaklardır. Komisyon'a bu hükümlerin metnini derhal bildireceklerdir. Bu hükümleri 6 Mayıs 2018 tarihinden itibaren uygulayacaklardır.

Üye Devletler söz konusu tedbirleri kabul ettiklerinde, tedbirlerde işbu Direktif'e atıf yapılır veya bu tedbirler resmi olarak yayımlanırken bu yönde bir atfa yer verilir. Üye Devletler, söz konusu atfın nasıl yapılacağını belirler.

2. Orantısız bir çabayı gerektirdiği takdirde, bir Üye Devlet, istisnai olarak, birinci fıkrayı uygulama dışında tutma yoluyla, 6 Mayıs 2016'dan önce kurulan otomatik işleme sistemlerinin 6 Mayıs 2023'e kadar işbu Direktif'in 25'inci maddesinin birinci fıkrasına uygun hale getirilmesini sağlayabilir.

3. Olağanüstü hallerde, bir Üye Devlet, işbu Madde'nin birinci ve ikinci fıkralarını uygulama dışında tutma yoluyla, işbu Madde'nin ikinci fıkrasında atıfta bulunulan bir otomatik işleme sistemini, söz konusu otomatik işleme sisteminin işletimi için ciddi zorluklar ortaya çıkacaksa, iş Madde'nin ikinci fıkrasında belirtilen süreden sonraki belirli bir süre içerisinde, 25'inci maddenin birinci fıkrasına uygun hale getirebilir. İlgili Üye Devlet, bu ciddi zorlukların nedenlerini ve otomatik işleme sistemini 25'inci maddenin birinci fıkrasına uygun hale getireceği bu belirli sürenin gerekçelerini Komisyon'a bildirecektir. Belirtilen süre, her halükarda, 6 Mayıs 2026'dan sonra olmayacaktır.

4. Üye Devletler, işbu Direktif'in kapsadığı alanda kabul ettikleri ulusal hukukun temel düzenlemelerinin metnini Komisyon'a ileteceklerdir.

Madde 64

Yürürlüğe Girme

1. İşbu Direktif Avrupa Birliği Resmi Gazetesi'nde yayımlanmasını takip eden günde yürürlüğe girecektir.

Madde 65

Muhataplar

1. İşbu Direktif'in muhatabı Üye Devletler'dir.

2. 27 Nisan 2016 tarihinde Brüksel'de düzenlenmiştir.

Avrupa Parlamentosu Adına
Başkan
M. SCHULZ
Konsey Adına
Başkan
J.A. HENNIS-PLASSCHAERT