95/46/AT sayılı Direktif'i yürürlükten kaldıran, gerçek kişilerin kişisel verilerin işlenmesi bakımından korunması ve bu tür verilerin serbest dolaşımı hakkında

27 Nisan 2016 tarihli ve

(AB) 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü)

(AEA ile ilişkili metin)

AVRUPA PARLAMENTOSU VE AVRUPA BİRLİĞİ KONSEYİ;

Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'yı ve bu Antlaşma'nın özellikle 16. maddesini göz önünde tutarak,

Avrupa Komisyonunun önerisini göz önünde tutarak,

Taslak yasama tasarrufunun ulusal parlamentolara gönderilmesini müteakip,

Avrupa Ekonomik ve Sosyal Komitesinin görüşünü[1] göz önünde tutarak,

Bölgeler Komitesinin görüşünü[2] göz önünde tutarak,

Olağan yasama usulü[3] uyarınca hareket ederek,

Aşağıdaki gerekçelerle:

(1) Kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunması temel bir haktır. Avrupa Birliği Temel Haklar Şartı'nın ("Şart") 8(1) maddesi ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın (ABİA) 16(1) maddesi herkesin kendisiyle ilgili kişisel verilerin korunması hakkına sahip olduğunu öngörür.

(2) Kendilerine ait kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunmasına ilişkin ilkeler ve kurallar, uyrukları veya ikametgâhları ne olursa olsun, bu kişilerin temel hak ve özgürlüklerine, özellikle de kişisel verilerin korunması haklarına saygı göstermelidir. Bu Tüzük, bir özgürlük, güvenlik ve adalet alanının ve ekonomik birliğin gerçekleştirilmesine ve ekonomik ve sosyal ilerlemeye, iç pazarda ekonomilerin güçlenmesine ve yakınsamasına ve gerçek kişilerin refahına katkıda bulunmayı amaçlar.

(3) 95/46/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi[4] işleme faaliyetleriyle ilgili olarak gerçek kişilerin temel hak ve özgürlüklerinin korunmasının uyumlaştırılmasını ve Üye Devletler arasında kişisel verilerin serbest akışının sağlanmasını hedefler.

---

[1] ABRG C 229, 31.7.2012, s.90.

[2] ABRG C 391, 18.12.2012, s.127

[3] 12 Mart 2014 tarihli Avrupa Parlamentosu Tutumu (henüz Resmi Gazete'de yayımlanmamıştır) ve 8 Nisan 2016 tarihli ilk okumadaki Konsey Tutumu (henüz Resmi Gazete'de yayımlanmamıştır). 14 Nisan 2016 tarihli Avrupa Parlamentosu Tutumu

[4] Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımı bakımından bireylerin korunmasına ilişkin 24 Ekim 1995 tarihli ve 95/46/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi (ATRG L 281, 23.11.1995, s.31).

(4) Kişisel verilerin işlenmesi insanlığa hizmet edecek şekilde tasarlanmalıdır. Kişisel verilerin korunması hakkı mutlak bir hak değildir; toplum içindeki işleviyle ilişkili olarak ele alınmalı ve orantılılık ilkesine uygun olarak diğer temek haklarla denge içinde olmalıdır. Bu Tüzük tüm temel haklara saygı gösterir ve özel hayata ve aile hayatına, konuta ve iletişime saygı, kişisel verilerin korunması, düşünce, vicdan ve din özgürlüğü, ifade ve bilgi edinme özgürlüğü, iş yapma özgürlüğü, etkili bir hukuk yolu ve adil yargılanma hakkı ile kültür, din ve dil çeşitliliği başta olmak üzere, Antlaşmalarda güvence altına alındığı gibi Şart'ta tanınmış olan özgürlük ve ilkeleri gözetir.

(5) İç pazarın işleyişinden kaynaklanan ekonomik ve sosyal bütünleşme, kişisel verilerin sınır ötesi akışlarında önemli ölçüde artışa sebep olmuştur. Birlik genelinde gerçek kişiler, dernekler ve teşebbüsler dâhil olmak üzere kamu ve özel sektör aktörleri arasında kişisel verilerin paylaşımı artmıştır. Birlik hukuku, Üye Devletlerdeki ulusal makamlara, kendi görevlerini veya başka bir Üye Devlet'te bulunan bir makam adına görevlerini yerine getirebilmeleri için iş birliği yapma ve kişisel verileri paylaşma çağrısında bulunur.

(6) Teknoloji alanındaki hızlı gelişmeler ve küreselleşme, kişisel verilerin korunması için yeni zorluklar getirmiştir. Kişisel verilerin toplanma ve paylaşılma ölçeği kayda değer şekilde artmıştır. Teknoloji, özel şirketlerin ve kamu kuruluşlarının faaliyetlerini sürdürmek için kişisel verileri benzeri görülmemiş bir ölçekte kullanmalarına imkân tanır. Gerçek kişiler, kişisel bilgileri giderek daha fazla kamusal ve küresel erişime sunmaktadır. Teknoloji, ekonomiyi ve sosyal hayatı dönüştürmüştür ve kişisel verilerin yüksek düzeyde korunmasını sağlayarak, Birlik içinde serbest akışını ve üçüncü ülkelere ve uluslararası kuruluşlara aktarılmasını daha da kolaylaştırmalıdır.

(7) Bu gelişmeler, dijital ekonominin iç pazarın tamamında gelişmesine imkân verecek güvenin oluşturulmasının önemi dikkate alındığında, Birlik içinde güçlü uygulama ile desteklenen sağlam ve daha tutarlı bir veri koruma çerçevesinin oluşturulmasını gerektirir. Gerçek kişiler kendi kişisel verilerinin kontrolüne sahip olmalıdır. Gerçek kişiler, iktisadi işletmeler ve kamu makamları için hukuki ve uygulamaya ilişkin belirlilik artırılmalıdır.

(8) Bu Tüzük'ün kurallarında Üye Devlet hukuku uyarınca belirlemeler veya kısıtlamalar öngörülmesi hâlinde Üye Devletler, tutarlılık ve ulusal hükümlerin uygulanacağı kişilerce anlaşılır olması amacıyla gerekli olduğu ölçüde bu Tüzük'ün unsurlarını kendi ulusal hukukuna dâhil edebilirler.

(9) 95/46/AT sayılı Direktif'in amaç ve ilkeleri geçerliliğini sürdürmekle birlikte, Birlik genelinde verilerin korunmasıyla ilgili uygulamadaki parçalı yapıyı, hukuki belirsizliği veya özellikle çevrim içi faaliyetle ilgili olmak üzere gerçek kişilerin korunmasına ilişkin kayda değer riskler bulunduğu yönündeki yaygın algıyı önleyebilmiş değildir. Üye Devletlerde kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin, özellikle kişisel verilerin korunması hakkı olmak üzere hak ve özgürlüklerinin korunma düzeyindeki farklılıklar Birlik içinde kişisel verilerin serbest akışını engelleyebilir. Bu farklılıklar sonuç olarak Birlik düzeyinde ekonomik faaliyetlerin sürdürülmesine engel teşkil edebilir, rekabeti bozabilir ve Birlik hukuku kapsamında ilgili makamların sorumluluklarını yerine getirmesini sekteye uğratabilir. Koruma düzeylerindeki söz konusu farklılıklar, 95/46/AT sayılı Direktif'in icra edilmesi ve uygulanmasında farklılıklar olmasından kaynaklanır.

(10) Gerçek kişilerin tutarlı bir şekilde ve yüksek seviyede korunmasının sağlanması ve Birlik içinde kişisel veri akışları önündeki engellerin kaldırılması amacıyla bu tür verilerin işlenmesiyle ilgili olarak gerçek kişilerin hak ve özgürlüklerini koruma düzeyi tüm Üye Devletlerde eşdeğer olmalıdır. Kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin temel hak ve özgürlüklerinin korunmasına ilişkin kuralların Birlik genelinde tutarlı ve

homojen bir şekilde uygulanması sağlanmalıdır. Kişisel verilerin yasal bir yükümlülüğe uyulması, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin kullanılması çerçevesinde işlenmesiyle ilgili olarak Üye Devletlerin, ulusal mevzuat hükümlerini korumalarına veya bu Tüzük'ün kurallarının uygulanmasını daha ayrıntılı belirlemek üzere yeni mevzuat hükümleri getirmelerine izin verilmelidir. 95/46/AT sayılı Direktif'i uygulayan genel ve yatay veri koruma mevzuatı ile bağlantılı olarak Üye Devletlerin, daha spesifik hükümlere ihtiyaç duyan alanlarda sektör bazlı birçok mevzuatı vardır. Bu Tüzük ayrıca Üye Devletlere, özel kategorilerdeki kişisel verilerin ("hassas veriler") işlenmesi dâhil olmak üzere kendi kurallarını belirlemeleri için bir hareket alanı sağlar. Bu çerçevede bu Tüzük, kişisel verilerin işlenmesinin hukuka uygun olduğu koşulların daha net bir şekilde belirlenmesi dâhil olmak üzere belirli işleme durumlarına ilişkin koşulları ortaya koyan Üye Devlet mevzuatını engellemez.

(11) Birlik genelinde kişisel verilerin etkili olarak korunması, veri öznelerinin haklarının ve kişisel verileri işleyen ve işlenmesinde belirleyici olan kişilerin yükümlülüklerinin güçlendirilmesinin ve detaylı şekilde ortaya konulmasının yanı sıra, Üye Devletlerde kişisel verilerin korunmasına ilişkin kurallara uyumun sağlanmasında ve izlenmesinde eş değer yetkilerin kullanılmasını ve ihlaller karşısında eş değer yaptırımların uygulanmasını gerektirir.

(12) ABİA'nın 16(2) maddesi Avrupa Parlamentosu ve Konseyin, kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kuralları belirlemesini zorunlu kılar.

(13) Birlik genelinde gerçek kişiler için tutarlı bir koruma düzeyi sağlamak ve kişisel verilerin iç pazarda serbest dolaşımını engelleyen sapmaları önlemek amacıyla; mikro, küçük ve orta ölçekli işletmeler dâhil iktisadi işletmeler için hukuki belirlilik ve şeffaflık temin etmek, tüm Üye Devletlerdeki gerçek kişilere hukuki olarak eşit düzeyde uygulanabilir haklar ile veri sorumluları ve veri işleyenlere sorumluluklar ve yükümlülükler getirmek ve tüm Üye Devletlerde kişisel verilerin işlenmesinin tutarlı bir şekilde izlenmesini, eş değer yaptırımları ve farklı Üye Devletlerin denetim makamları arasında etkili işbirliğini sağlamak üzere bir Tüzük gereklidir. İç pazarın düzgün işleyişi, Birlik içinde kişisel verilerin serbest dolaşımının, kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunmasıyla bağlantılı nedenlerle kısıtlanmamasını veya yasaklanmamasını gerektirir. Mikro, küçük ve orta ölçekli işletmelerin özel durumunun dikkate alınması amacıyla bu Tüzük 250'den az çalışanı olan teşekküller için kayıt tutma konusunda bir derogasyon içerir. Ayrıca, Birlik kurumları ve organları ile Üye Devletler ve onların denetim makamları, bu Tüzük'ün uygulanmasında mikro, küçük ve orta ölçekli işletmelerin özel ihtiyaçlarını dikkate almaya teşvik edilir. Mikro, küçük ve orta ölçekli işletmeler kavramı için, 2003/361/AT sayılı Komisyon Tavsiyesi[5] Ekinin 2. maddesi referans alınmalıdır.

(14) Bu Tüzük ile sağlanan koruma, uyrukları veya ikametgâhları fark etmeksizin kişisel verilerinin işlenmesiyle ilgili olarak, gerçek kişilere uygulanmalıdır. Bu Tüzük, tüzel kişinin adı ve türü ile irtibat bilgileri dâhil tüzel kişilere ve özellikle tüzel kişi olarak kurulmuş teşebbüslere ilişkin kişisel verilerin işlenmesini kapsamaz.

(15) Hukuki boşluklardan yararlanmaya yönelik ciddi bir risk oluşmasını önlemek için, gerçek kişilerin korunması teknolojik bakımdan tarafsız olmalı ve kullanılan tekniklere bağlı olmamalıdır. Gerçek kişilerin korunması, kişisel verilerin otomatik yollarla işlenmesinin yanı sıra kişisel verilerin bir dosyalama sisteminde yer aldığı veya yer almasının

[5] Mikro, küçük ve orta ölçekli işletmelerin tanımına ilişkin 6 Mayıs 2003 tarihli Komisyon Tavsiyesi (C(2003) 1422) (ABRG L 124, 20.5.2003, s.36).

amaçlandığı durumlarda manuel işlemeye de uygulanmalıdır. Belirli kriterlere göre yapılandırılmamış dosyalar veya dosya setleri ile bunların kapak sayfaları bu Tüzük'ün kapsamına girmemelidir.

(16) Bu Tüzük, milli güvenliğe ilişkin faaliyetler gibi, Birlik hukuku kapsamı dışında kalan faaliyetlerle ilgili olarak temel hak ve özgürlüklerin korunması veya kişisel verilerin serbest akışı konularına uygulanmaz. Bu Tüzük, Birlik'in ortak dış ve güvenlik politikasına ilişkin faaliyetlerin yürütülmesi sırasında Üye Devletler tarafından kişisel verilerin işlenmesine uygulanmaz.

(17) (AT) 45/2001 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü[6], Birlik kurumları, organları, ofisleri ve ajansları tarafından kişisel verilerin işlenmesine uygulanır. (AT) 45/2001 sayılı Tüzük ve kişisel verilerin bu şekilde işlenmesine ilişkin Birlik'in diğer hukuki tasarrufları, bu Tüzük'te belirlenen ilke ve kurallara uyarlanmalı ve bu Tüzük doğrultusunda uygulanmalıdır. Birlik içinde güçlü ve tutarlı bir veri koruma çerçevesi sağlamak amacıyla, (AT) 45/2001 sayılı Tüzük'e ilişkin gerekli uyarlamalar, bu Tüzük ile aynı zamanda uygulamaya imkân vermek üzere bu Tüzük'ün kabul edilmesini müteakip yapılmalıdır.

(18) Bu Tüzük, gerçek bir kişi tarafından kişisel verilerin tamamen kişisel veya hane içi bir faaliyet sırasında ve dolayısıyla profesyonel veya ticari bir faaliyetle bağlantılı olmayan şekilde işlenmesine uygulanmaz. Kişisel veya hane içi faaliyetler, yazışmaları ve adreslerin tutulmasını veya bu tür faaliyetler bağlamında gerçekleştirilen sosyal ağ kullanımı ve çevrim içi faaliyetleri içerebilir. Bununla birlikte, bu Tüzük, bu tür kişisel veya hane içi faaliyetler için kişisel verilerin işlenmesine ilişkin yolları sağlayan veri sorumlularına veya veri işleyenlere uygulanır.

(19) Kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezaların infaz edilmesi amacıyla, kişisel verilerin yetkili makamlar tarafından işlenmesiyle ilgili olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımı özel bir Birlik hukuki tasarrufunun konusudur. Dolayısıyla bu Tüzük, söz konusu amaçlara yönelik veri işleme faaliyetlerine uygulanmamalıdır. Ancak, bu Tüzük kapsamında kamu makamları tarafından işlenen kişisel veriler, bu amaçlar için kullanıldıklarında daha özel bir Birlik hukuki tasarrufuna, (AB) 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi'ne[7], tabi olmalıdır. Üye Devletler, 2016/680/AB sayılı Direktif kapsamında yetkili makamlara; kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi dâhil suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezaların infaz edilmesi amaçlarıyla yürütülmeyen görevler verebilirler, şu kadar ki söz konusu diğer amaçlarla veri işleme, Birlik hukuku kapsamında olduğu müddetçe, bu Tüzük kapsamında sayılır.

Bu Tüzük kapsamına giren amaçlar için yetkili makamlar tarafından kişisel verilerin işlenmesiyle ilgili olarak Üye Devletler, bu Tüzük'ün kurallarının uygulanmasını uyarlamak amacıyla mevcut hükümleri koruyabilmeli veya daha özel hükümler getirebilmelidirler. Bu tür hükümler, ilgili Üye Devletin anayasal, kurumsal ve idari yapısını dikkate alarak, sözü edilen diğer amaçlar için söz konusu yetkili makamlar

---

[6] Bireylerin, kişisel verilerin Topluluk kurum ve organlarınca işlenmesi ile ilgili olarak korunması ve bu tür verilerin serbest dolaşımı hakkında 18 Aralık 2000 tarihli ve (AT) 45/2001 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ATRG L 8, 12.1.2001, s.1).

[7] 2008/977/Aİİ sayılı Konsey Çerçeve Kararı'nı yürürlükten kaldıran ve suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi amacıyla kişisel verilerin yetkili makamlar tarafından işlenmesi bakımından gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımı hakkında 27 Nisan 2016 tarihli ve (AB) 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi (söz konusu Resmi Gazete'nin 89. sayfasına bakınız).

tarafından kişisel verilerin işlenmesine ilişkin özel şartları daha açık bir şekilde belirleyebilir. Kişisel verilerin özel organlar tarafından işlenmesinin bu Tüzük kapsamına girmesi hâlinde, bu Tüzük, Üye Devletlere, kamu güvenliği ve kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezaların infaz edilmesi gibi bazı önemli menfaatleri güvence altına almak amacıyla, sınırlamanın demokratik bir toplumda gerekli ve orantılı bir tedbir teşkil etmesi hâlinde özel koşullar çerçevesinde belirli yükümlülükleri ve hakları mevzuatla sınırlama imkânı vermelidir. Bu, örneğin kara paranın aklanmasıyla mücadele veya adli tıp laboratuvarlarının faaliyetleri çerçevesinde geçerlidir.

(20) Her ne kadar bu Tüzük, diğerlerinin yanı sıra, mahkemelerin ve diğer adli makamların faaliyetlerine uygulansa da Birlik veya Üye Devlet hukuku, kişisel verilerin mahkemeler ve diğer adli makamlar tarafından işlenmesiyle ilgili işleme süreçlerini ve usullerini belirleyebilir. Denetim makamlarının yetkisi, karar verme dâhil yargısal görevlerini yerine getirirken yargı bağımsızlığını korumak amacıyla, mahkemelerin kendi yargı yetkisi çerçevesinde hareket ederken kişisel verileri işlemesini kapsamamalıdır. Bu tür veri işleme faaliyetlerinin denetimini, özellikle bu Tüzük'ün kurallarına uyulmasını sağlamak, yargı mensuplarının bu Tüzük kapsamındaki yükümlülüklerine ilişkin farkındalıklarını artırmak ve bu tür veri işleme faaliyetleriyle ilgili şikâyetleri ele almak üzere, Üye Devlet'in yargı sistemi içindeki belirli organlara tevdi etmek mümkün olmalıdır.

(21) Bu Tüzük, 2000/31/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi'nin[8], uygulanmasına ve özellikle bu Direktif'in 12 ilâ 15. maddelerinde yer alan aracı hizmet sağlayıcıların yükümlülüklerine ilişkin kurallara halel getirmez. Söz konusu Direktif, Üye Devletler arasında bilgi toplumu hizmetlerinin serbest dolaşımını sağlayarak iç pazarın düzgün işleyişine katkıda bulunmayı hedefler.

(22) Birlik içinde bir veri sorumlusu veya veri işleyenin kuruluşunun faaliyetleri bağlamında kişisel verilerin herhangi bir şekilde işlenmesi, işleme faaliyetinin Birlik içinde gerçekleşip gerçekleşmediğine bakılmaksızın, bu Tüzük uyarınca gerçekleştirilmelidir. Kuruluş, faaliyetin istikrarlı düzenlemeler yoluyla etkili ve fiilen gerçekleştirilmesi anlamına gelir. Bu tür düzenlemelerin hukuki şekli, bir şube veya tüzel kişiliğe sahip bir bağlı şirket aracılığıyla olması fark etmeksizin, bu bakımdan belirleyici faktör değildir.

(23) Gerçek kişilerin bu Tüzük kapsamında sahip oldukları korumadan mahrum kalmamalarını sağlamak üzere Birlik içindeki veri öznelerinin kişisel verilerinin Birlik içinde kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesi, işleme faaliyetlerinin, bir ödeme ile bağlantılı olup olmadığına bakılmaksızın, bu tür veri öznelerine mal veya hizmet sunmakla ilgili olduğu hâllerde bu Tüzük'e tabi olmalıdır. Bu tür bir veri sorumlusu veya veri işleyenin, Birlik içindeki veri öznelerine mal veya hizmet sunup sunmadığını belirlemek için, veri sorumlusunun veya veri işleyenin, Birlik'te bir veya daha fazla Üye Devlet içindeki veri öznelerine hizmet sunmayı öngördüğünün belli olup olmadığı tespit edilmelidir. Birlik içinde veri sorumlusunun, veri işleyenin veya bir aracının internet sitesine, bir e-posta adresine veya diğer irtibat bilgilerine basit şekilde erişebilirlik veya veri sorumlusunun yerleşik olduğu üçüncü ülkede genel olarak kullanılan bir dilin kullanımı bu tür bir niyeti tespit etmek için yeterli değilken, söz konusu diğer dilde mal ve hizmet siparişi verme imkânı ile birlikte bir veya daha fazla Üye Devlet içinde genel olarak kullanılan bir dilin veya para biriminin kullanılması veya Birlik içindeki müşterilerden veya

[8] Başta elektronik ticaret olmak üzere, bilgi toplumu hizmetlerinin İç Pazar'daki bazı hukuki veçheleri hakkında 8 Haziran 2000 tarihli ve 2000/31/AT sayılı Direktif (ATRG L 178, 17.7.2000, s. 1).

kullanıcılardan bahsetme gibi faktörler, veri sorumlusunun Birlik içindeki veri öznelerine mal veya hizmet sunmayı öngördüğünü belli edebilir.

(24) Birlik içinde yerleşik olmayan bir veri sorumlusu veya veri işleyen tarafından Birlik içindeki veri öznelerinin kişisel verilerinin işlenmesi, bu tür veri öznelerinin davranışlarının, Birlik içinde gerçekleştiği ölçüde, izlenmesiyle ilgili olduğunda da bu Tüzük'e tabi olmalıdır. Bir işleme faaliyetinin veri öznelerinin davranışlarını izleme olarak değerlendirilip değerlendirilemeyeceğini belirlemek için, özellikle kendisi ile ilgili kararlar almak veya kişisel tercihlerini, davranışlarını ve tutumlarını analiz veya tahmin etmek amacıyla bir gerçek kişinin profillenmesini teşkil eden kişisel veri işleme tekniklerinin potansiyel sonradan kullanımı dâhil olmak üzere, gerçek kişilerin internet üzerinde takip edilip edilmediğinin tespit edilmesi gereklidir.

(25) Üye Devlet hukukunun uluslararası kamu hukuku gereğince uygulanması hâlinde bu Tüzük ayrıca, Birlik içinde kurulu olmayan örneğin bir Üye Devlet'in diplomatik misyonu veya konsolosluğunda bulunan bir veri sorumlusuna da uygulanmalıdır.

(26) Veri koruma ilkeleri, kimliği belirlenmiş veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgiye uygulanmalıdır. Ek bilgilerin kullanılmasıyla gerçek bir kişiyle ilişkilendirilebilecek takma ad verilmiş kişisel veriler, kimliği belirlenebilir bir gerçek kişiye ilişkin bilgiler olarak değerlendirilmelidir. Bir gerçek kişinin kimliğinin belirlenebilir olup olmadığını tespit için, veri sorumlusu veya başka bir kişi tarafından gerçek kişiyi doğrudan veya dolaylı olarak belirlemek amacıyla, grup içinden seçme gibi, kullanılması makul bir şekilde muhtemel tüm yöntemler dikkate alınmalıdır. Gerçek kişinin kimliğini belirlemek amacıyla söz konusu yöntemlerin kullanılması konusunda makul bir olasılığın bulunup bulunmadığını tespit etmek için, işleme sırasındaki mevcut teknoloji ve teknolojik gelişmeler göz önünde tutularak, kimliğin belirlenmesi için gerekli süre ve maliyetler gibi tüm nesnel faktörler dikkate alınmalıdır. Bu nedenle veri koruma ilkeleri, anonim bilgilere, şöyle ki kimliği belirlenmiş veya belirlenebilir bir gerçek kişiyle ilgili olmayan bilgilere veya veri öznesinin kimliğinin belirlenebilir olmadığı veya artık belirlenebilir olmayacağı bir şekilde anonim hâle getirilen kişisel verilere uygulanmamalıdır. Bu nedenle bu Tüzük, istatistiki veya araştırmaya yönelik amaçlar dâhil olmak üzere bu tür anonim bilgilerin işlenmesiyle ilgili bulunmamaktadır.

(27) Bu Tüzük vefat eden kişilerin kişisel verilerine uygulanmaz. Üye Devletler, vefat eden kişilerin kişisel verilerinin işlenmesine ilişkin kurallar öngörebilirler.

(28) Kişisel verilerde takma ad kullanımının uygulanması, ilgili veri öznelerine yönelik riskleri azaltabilir ve veri sorumlularının ve veri işleyenlerin veri koruma yükümlülüklerini yerine getirmelerine yardımcı olabilir. Bu Tüzük'te "takma ad kullanımı"nın açık bir şekilde getirilmesi, diğer veri koruma önlemlerini engelleme amacı taşımaz.

(29) Kişisel veriler işlenirken takma ad kullanımı uygulanmasını teşvik etmek amacıyla, takma ad kullanımına ilişkin tedbirler, bir yandan genel bir analize imkân verirken bir yandan da söz konusu veri sorumlusu, ilgili işleme için bu Tüzük'ün uygulanmasını sağlamak ve kişisel verilerin belirli bir veri öznesi ile ilişkilendirilmesi için ek bilgilerin ayrı bir şekilde tutulmasını temin etmek amacıyla gerekli teknik ve kurumsal tedbirleri aldığında aynı veri sorumlusu nezdinde mümkün olmalıdır. Kişisel verileri işleyen veri sorumlusu, aynı veri sorumlusu nezdindeki yetkili kişileri belirtmelidir.

(30) Gerçek kişiler, kullandıkları cihaz, uygulama, araç ve protokollerin, internet protokolü adresleri, çerez tanımlayıcıları veya radyo frekansı ile tanımlama etiketleri gibi diğer tanımlayıcılar şeklinde sağlamış olduğu çevrim içi tanımlayıcılarla ilişkilendirilebilir. Bu; tanımlayıcılar, özellikle sunuculardan edinilen emsalsiz tanımlayıcılar ve diğer bilgiler ile

birleştirildiğinde, gerçek kişilerin profillerini oluşturmak ve onları tanımlamak için kullanılabilecek izler bırakabilir.

(31) Vergi ve gümrük idareleri, mali soruşturma birimleri, bağımsız idari makamlar veya menkul kıymet piyasalarının düzenlenmesi ve denetiminden sorumlu finansal piyasa otoriteleri gibi resmi görevlerinin yerine getirilmesi için yasal yükümlülük uyarınca kişisel verilerin açıklandığı kamu makamları, Birlik veya Üye Devlet mevzuatına uygun olarak, genel yarar kapsamında belirli bir soruşturmayı yürütmek için gereken kişisel verileri alırlarsa alıcı olarak kabul edilmemelidir. Kamu makamları tarafından gönderilen açıklama talepleri her zaman yazılı, gerekçeli ve arızi olmalı ve bir dosyalama sisteminin bütünüyle ilgili olmamalı ya da dosyalama sistemlerinin birbirine bağlanmasına yol açmamalıdır. Kişisel verilerin bu kamu makamları tarafından işlenmesi, işlemenin amaçları doğrultusunda, geçerli veri koruma kurallarına uygun olmalıdır.

(32) Rıza, veri öznesinin kendisiyle ilgili kişisel verilerin işlenmesine ilişkin serbestçe verilmiş, spesifik, aydınlatılmış ve şüpheye yer bırakmayacak bir şekilde mutabakatının belirtilmesini sağlayan açık ve olumlu bir eylemiyle, örneğin elektronik araçlarla yapılanlar da dâhil olmak üzere yazılı bir beyanla veya sözlü bir ifadeyle verilmelidir. Bu, bir internet sitesini ziyaret ederken bir kutunun işaretlenmesini, bilgi toplumu hizmetleri için teknik ayarların seçilmesini ya da veri öznesinin kişisel verilerinin önerilen biçimde işlenmesini kabul ettiğini bu bağlamda açıkça gösteren başka bir beyan veya davranışı içerebilir. Dolayısıyla sükût, önceden işaretlenmiş kutular ya da hareketsizlik rıza teşkil etmez. Rıza, aynı amaç ya da amaçlar doğrultusunda gerçekleştirilen tüm işleme faaliyetlerini kapsamalıdır. Veri işlemenin birden fazla amacı olduğunda, rıza bunların tamamına verilmelidir. Veri öznesinin rızasının elektronik yollarla iletilen bir talep üzerine verilecek olması hâlinde talep, açık ve kısa olmalı, rızayı gerektiren hizmetin kullanımını gereksiz yere aksatmamalıdır.

(33) Veri toplama sırasında bilimsel araştırma amacıyla kişisel veri işlemenin amacı çoğu zaman tam olarak belirlenemez. Bu nedenle veri öznelerinin, bilimsel araştırmalar için kabul edilen etik standartlara uygun olduğunda, belirli bilimsel araştırma alanlarına rıza vermelerine izin verilmelidir. Veri özneleri, belirlenen amaca uygun biçimde, yalnızca belirli araştırma alanlarına veya araştırma projelerinin belirli bölümlerine rıza verebilmelidir.

(34) Genetik veriler, bir gerçek kişiden alınan biyolojik bir numunenin, özellikle kromozomal, deoksiribonükleik asit (DNA) veya ribonükleik asit (RNA) analizinden ya da eşdeğer bilgilerin elde edilmesini sağlayan bir başka elementin analizinden elde edilen, söz konusu gerçek kişinin kalıtsal veya edinilmiş genetik özellikleriyle ilgili kişisel veriler olarak tanımlanmalıdır.

(35) Sağlıkla ilgili kişisel veriler, veri öznesinin, geçmiş, mevcut veya gelecekteki fiziksel veya ruhsal sağlık durumuna ilişkin bilgileri ortaya koyan tüm verileri içermelidir. Bu, 2011/24/AB sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde[9] atıfta bulunulduğu üzere sağlık bakım hizmetlerine kaydolma ya da o hizmetlerin sağlanması sırasında bir gerçek kişi hakkında toplanan bilgileri; bir gerçek kişiyi sağlık amaçları doğrultusunda, başkasıyla karıştırılmayacak bir biçimde belirlemek için o kişiye atanan bir sayı, simge veya hususu; genetik veriler ve biyolojik numuneler dâhil olmak üzere, vücudun bir kısmının ya da vücuda ait bir maddenin test edilmesi veya incelenmesinden elde edilen bilgileri ve örneğin bir hastalık, engellilik, hastalık riski, tıbbi geçmiş, klinik tedavi veya veri öznesinin

[9] Sınır ötesi sağlık hizmetlerinde hasta haklarının uygulanması hakkında 9 Mart 2011 tarihli ve 2011/24/AB sayılı Direktif (ABRG L 88, 4.4.2011, s.45).

fizyolojik veya biyomedikal durumuna benzer her bilgiyi, doktor ya da başka bir sağlık profesyoneli, hastane, tıbbi cihaz ya da in vitro tanı testi gibi kaynağından bağımsız olarak içerir.

(36) Kişisel verilerin işlenmesine ilişkin amaç ve yöntemlere ilişkin kararların, veri sorumlusunun Birlik'teki başka bir kuruluşunda alınmaması halinde, Birlik'teki bir veri sorumlusunun ana kuruluşu, Birlik içindeki merkezi idare yeri olmalıdır, böyle bir halde diğer kuruluş ana kuruluş sayılır. Bir veri sorumlusunun Birlik içindeki ana kuruluşu objektif kriterlere göre belirlenmeli ve istikrarlı düzenlemeler yoluyla veri işleme amaçları ve araçlarıyla ilgili temel kararları belirleyen yönetim faaliyetlerinin etkili ve fiilen uygulanmasını sağlamalıdır. Bu kriter, kişisel verilerin o yerde işlenip işlenmediğine bağlı olmamalıdır. Kişisel verilerin işlenmesine veya işleme faaliyetlerine yönelik teknik araçların ve teknolojilerin varlığı ve kullanımı, kendi başına bir ana kuruluş meydana getirmez ve dolayısıyla bir ana kuruluş için belirleyici kriter değildir. Veri işleyenin ana kuruluşu, merkezi idarenin Birlik içindeki yeri veya Birlik içinde bir merkezi idaresi yoksa, ana işleme faaliyetlerinin Birlik içinde gerçekleştirildiği yer olmalıdır. Hem veri sorumlusu hem de veri işleyeni ilgilendiren durumlarda, yetkili baş denetim makamı, veri sorumlusunun ana kuruluşunun bulunduğu Üye Devlet'in denetim makamı olarak kalmalıdır, ancak veri işleyenin denetim makamı, ilgili bir denetim makamı olarak kabul edilmeli ve söz konusu denetim makamı, bu Tüzük'te öngörülen iş birliği prosedürüne katılmalıdır. Her halükarda, veri işleyenin bir veya daha fazla kuruluşa sahip olduğu Üye Devlet'in veya Üye Devletlerin denetim makamları, taslak kararın yalnızca veri sorumlusunu ilgilendirdiği durumlarda ilgili denetim makamları olarak değerlendirilmemelidir. Veri işleme faaliyetinin bir teşebbüsler grubu tarafından gerçekleştirildiği durumlarda, işleme amaçlarının ve yöntemlerinin başka bir teşebbüs tarafından belirlendiği hâller dışında, idare eden teşebbüsün ana kuruluşu, teşebbüsler grubunun ana kuruluşu olarak kabul edilmelidir.

(37) Bir teşebbüsler grubu, idare eden teşebbüs ile onun tarafından idare edilen teşebbüslerini kapsamalıdır; bu durumda, idare eden teşebbüs, diğer teşebbüsler üzerinde, örneğin mülkiyet, mali katılım veya yönetimine ilişkin kurallar veya kişisel verilerin korumasına ilişkin kuralların uygulanmasını sağlama yetkisi nedeniyle, hâkim bir etki yaratabilecek teşebbüs olmalıdır. Kendisine bağlı teşebbüslerde kişisel verilerin işlenmesini idare eden bir teşebbüs, bu teşebbüslerle birlikte bir teşebbüsler grubu olarak kabul edilmelidir.

(38) Çocuklar, kişisel verilerin işlenmesine ilişkin riskler, sonuçlar, ilgili güvenceler ve kendi hakları konusunda daha az bilgiye sahip olmaları nedeniyle kişisel verileriyle bağlantılı olarak özel bir korumayı hak eder. Böyle bir özel koruma, özellikle, pazarlama, ya da kişilik veya kullanıcı profili oluşturma amacıyla çocukların kişisel verilerinin kullanılmasında ve doğrudan doğruya çocuğa sunulan hizmetler kullanılırken çocuklara ilişkin kişisel verilerin toplanmasında uygulanmalıdır. Doğrudan çocuğa sunulan önleyici hizmetler veya danışmanlık hizmetleri bağlamında çocuklar üzerinde velayet hakkına sahip olanların rızası gerekli olmamalıdır.

(39) Her kişisel veri işleme işlemi, hukuka ve hakkaniyete uygun olmalıdır. Kendileriyle ilgili kişisel verilerin toplanması, kullanılması, bunlara bakılması veya bunların bir başka şekilde işlenmesi ve kişisel verilerin ne ölçüde işlendiği ya da işleneceği gerçek kişiler için şeffaf olmalıdır. Şeffaflık ilkesi, bu kişisel verilerin işlenmesine ilişkin her türlü bilgi ve bilgilendirmenin kolayca erişilebilir ve anlaşılır olmasını ve açık ve yalın bir dil kullanılmasını gerektirir. Bu ilke, özellikle, ilgili gerçek kişiler bakımından adil ve şeffaf bir işleme faaliyetini, bunların teyit alma hakkını ve işlenmekte olan kendilerine ilişkin kişisel verilerin iletilmesini temin etmek üzere veri sorumlusunun kimliği, işleme amaçları ve ilave bilgilerin veri öznelerine iletilmesini ilgilendirir. Gerçek kişiler, kişisel verilerin

işlenmesine ilişkin riskler, kurallar, güvenceler ve haklar ile söz konusu veri işlemeyle ilgili haklarını nasıl kullanacakları konusunda bilgilendirilmelidir. Özellikle, kişisel verilerin işlenmesinde güdülen özel amaçlar açık, meşru ve kişisel verilerin toplandığı sırada belirlenmiş olmalıdır. Kişisel veriler, işlenme amaçlarına uygun, işlenme amaçlarıyla ilgili ve bunlarla sınırlı olmalıdır. Bu, özellikle kişisel verilerin depolandığı sürenin kesin bir şekilde asgari süre ile sınırlı olmasını gerektirir. Kişisel veriler, ancak işlemenin amacı başka yollarla makul bir şekilde yerine getirilemiyorsa işlenmelidir. Kişisel verilerin gerekenden daha uzun süre tutulmamasını sağlamak için veri sorumlusu, kalıcı olarak silme veya periyodik gözden geçirme için süre sınırlarını belirlemelidir. Doğru olmayan kişisel verilerin düzeltilmesi veya silinmesini sağlamaya yönelik makul tüm adımlar atılmalıdır. Kişisel veriler, kişisel verilere ve işleme için kullanılan ekipmana izinsiz erişimin veya bunların kullanımının önlenmesi de dâhil olmak üzere, kişisel verilerin uygun biçimde güvenliğini ve gizliliğini sağlayacak şekilde işlenmelidir.

(40) İşlemenin hukuka uygun olması için kişisel veriler, ilgili veri öznesinin rızasına veya bu Tüzük'te ya da bu Tüzük'te atıfta bulunulan diğer Birlik veya Üye Devlet mevzuatında belirlenen, başka bir meşru temele dayalı olarak işlenmelidir; bu veri sorumlusunun tabi olduğu yasal yükümlülüğe uyum veya veri öznesinin taraf olduğu bir sözleşmenin ifası bakımından gerekliliği veya bir sözleşme yapılmadan önce veri öznesinin talepleri doğrultusunda harekete geçilmesi hususlarını da içerir.

(41) Bu Tüzük'ün hukuki bir dayanağa veya bir yasama tedbirine atıfta bulunduğu durumlarda bu, ilgili Üye Devlet'in anayasal düzeninin gerekliliklerine halel gelmeksizin, bir parlamento tarafından kabul edilen bir yasama tasarrufunu zorunlu kılmaz. Bununla birlikte, Avrupa Birliği Adalet Divanının (Adalet Divanı) ve Avrupa İnsan Hakları Mahkemesinin içtihadına uygun olarak, böyle bir hukuki dayanak veya yasama tedbiri açık ve kesin olmalı ve uygulaması, buna tabi olan kişiler tarafından öngörülebilir olmalıdır.

(42) İşlemenin veri öznesinin rızasına dayandığı hâllerde, veri sorumlusu, veri öznesinin veri işleme faaliyetine rıza verdiğini gösterebilmelidir. Özellikle başka bir konuya ilişkin yazılı bir beyan söz konusu olduğunda, güvenceler, veri öznesinin rızanın verildiğinin ve kapsamının farkında olmasını sağlamalıdır. 93/13/AET sayılı Konsey Direktifi[10] uyarınca, veri sorumlusu tarafından önceden hazırlanmış bir rıza beyanı, anlaşılır ve kolayca erişilebilir şekilde olmalı, açık ve sade bir dile sahip olmalı ve adil olmayan koşullar içermemelidir. Rızanın bilgilendirmeye dayalı olması için, veri öznesi en azından veri sorumlusunun kimliğinden ve kişisel verilerin hangi amaçla işleneceğinden haberdar olmalıdır. Veri öznesinin gerçek veya özgür bir seçme hakkı yoksa veya zarara uğramaksızın rıza vermeyi reddedemiyor ya da rızasını geri alamıyorsa rıza özgürce verilmiş kabul edilmemelidir.

(43) Rızanın özgürce verilmesini temin etmek için, veri öznesi ile veri sorumlusu arasında açık bir dengesizliğin olduğu belirli durumlarda, özellikle veri sorumlusu bir kamu makamı olduğunda ve bu nedenle rızanın söz konusu spesifik durumun tüm koşullarında özgürce verilmesi olası olmadığında rıza, kişisel verilerin işlenmesi için geçerli bir hukuki dayanak sağlamamalıdır. Münferit durumda farklı kişisel veri işleme işlemlerine ayrı ayrı rıza verilmesi uygun olduğu halde buna izin verilmiyorsa ya da bir hizmetin sağlanması da dâhil olmak üzere bir sözleşmenin ifası, bu tür bir ifa için böyle bir rızanın gerekli olmamasına rağmen rızaya bağlanmışsa, rızanın özgürce verilmediği kabul edilir.

---

[10] Tüketici sözleşmelerinde adil olmayan koşullar hakkında 5 Nisan 1993 tarihli ve 93/13/AET sayılı Konsey Direktifi (ATRG L 95, 21.4.1993, s.29).

(44) Bir sözleşme veya sözleşme yapma niyeti bağlamında gerekli olması hâlinde veri işleme, hukuka uygun olmalıdır.

(45) Veri işlemenin veri sorumlusunun tabi olduğu yasal yükümlülüğe uygun olarak gerçekleştirilmesi veya işlemenin kamu yararına bir görevin yerine getirilmesi veya bir resmi yetkinin ifası açısından gerekli olması hâlinde, işlemenin Birlik ya da Üye Devlet hukukunda dayanağı olmalıdır. Bu Tüzük, her bir münferit işleme için özel mevzuat gerektirmez. Mevzuattaki bir hüküm, veri sorumlusunun tabi olduğu bir yasal yükümlülüğe dayanan veya veri işlemenin kamu yararına gerçekleştirilen bir görevin yerine getirilmesi ya da resmi bir yetkinin kullanılması için gerekli olan birden fazla işleme faaliyetine dayanak olarak yeterli olabilir. Ayrıca, işlemenin amacı Birlik veya Üye Devlet mevzuatında belirlenmelidir. Ayrıca, söz konusu mevzuat, kişisel veri işlemenin hukuka uygunluğunu düzenleyen bu Tüzük'ün genel koşullarını detaylandırabilir; veri sorumlusunu, işlemeye tabi olan kişisel verilerin türünü, ilgili veri öznelerini, kişisel verilerin açıklanabileceği teşekkülleri, amaç sınırlamalarını, depolama süresini ve hukuka ve hakkaniyete uygun bir işleme için gerekli diğer önlemleri belirlemeye yönelik şartlar tesis edebilir. Kamu yararına bir görevi yerine getiren veya resmi yetkiyi kullanan veri sorumlusunun; bir kamu makamı mı, kamu hukukuna tabi bir başka gerçek veya tüzel kişi mi, yoksa halk sağlığı, sosyal koruma ve sağlık bakım hizmetlerinin yönetimi gibi sağlık amaçları da dâhil olmak üzere, kamu yararının bunu gerektirdiği durumlarda, özel hukuka tabi, örneğin bir meslek örgütü mü olacağı Birlik veya Üye Devlet hukukuna göre belirlenmelidir.

(46) Kişisel verilerin işlenmesinin, veri öznesinin veya bir başka gerçek kişinin hayatı açısından temel bir menfaatin korunmasının gerektiği hâllerde de hukuka uygun olduğu kabul edilmelidir. Kişisel verilerin, başka bir gerçek kişinin hayati menfaatine dayanılarak işlenmesi, ilke olarak, yalnızca işlemenin başka bir hukuki dayanağa açıkça dayandırılamayacağı durumlarda gerçekleştirilmelidir. Bazı işleme türleri, başta doğal ve insan kaynaklı felaketler olmak üzere, insani acil durumlarda ya da salgınların ve bunların yayılmasının izlenmesi dâhil olmak üzere insani amaçlar doğrultusunda işlemenin gerekli olması gibi hem kamu yararına hem de veri öznesinin hayati menfaatine hizmet edebilir.

(47) Kişisel verilerin açıklanabileceği veri sorumlusu da dâhil olmak üzere bir veri sorumlusunun veya bir üçüncü kişinin meşru menfaatleri, veri öznesinin menfaatleri veya temel hak ve özgürlükleri daha ağır basmadığı müddetçe, veri öznelerinin veri sorumlusuyla olan ilişkilerine dayalı makul beklentileri dikkate alınarak, veri işleme faaliyeti için hukuki dayanak oluşturabilir. Bu tür meşru menfaat, veri öznesi ile veri sorumlusu arasında konu ile ilgili ve uygun bir ilişkinin olduğu durumlarda, örneğin veri öznesi bir müşteri olduğunda ya da veri sorumlusunun hizmetinde bulunduğunda mevcut olabilir. Her durumda, meşru bir menfaatin varlığı, veri öznesinin, kişisel verilerin toplanması sırasında ve bağlamında söz konusu amaçla veri işlenmesini makul surette bekleyip bekleyemeyeceği de dâhil olmak üzere, dikkatli bir değerlendirme yapılmasını gerekli kılacaktır. Özellikle, veri öznelerinin verilerin daha fazla işlenmesini makul surette beklemediği durumlarda kişisel verilerin işlenmesi hâlinde, veri öznesinin menfaatleri ve temel hakları, veri sorumlusunun menfaati karşısında daha ağır basabilir. Kamu kuruluşlarının kişisel verileri işlemesi için gereken hukuki dayanağın mevzuatla öngörülmesinin yasa koyucunun görevi olduğu göz önünde bulundurulduğunda, buradaki hukuki sebep, kamu kuruluşlarının kendi görevlerini yerine getirirken veri işlemelerinde uygulanmamalıdır. Hilenin önlenmesi amacıyla kesinlikle gerekli olan kişisel verilerin işlenmesi de, ilgili veri sorumlusunun meşru menfaatini oluşturur. Kişisel verilerin doğrudan pazarlama amacıyla işlenmesi, meşru menfaat için gerçekleştirilmiş bir işlem olarak kabul edilebilir.

(48) Merkezi bir organa bağlı bir teşebbüsler veya kurumlar grubunun mensubu olan veri sorumluları, müşterilerin veya çalışanların kişisel verilerinin işlenmesi de dâhil olmak üzere, teşebbüsler grubu içinde kişisel verilerin dâhili idari amaçlarla iletilmesinde meşru menfaat sahibi olabilirler. Kişisel verilerin bir teşebbüs grubu içindeki üçüncü bir ülkede kain bir teşebbüse aktarılmasına ilişkin genel ilkeler geçerliliğini korur.

(49) Ağ ve bilgi güvenliğini, başka bir ifadeyle, bir ağ veya bilgi sisteminin belirli bir güvenilirlik düzeyinde, depolanan veya iletilen verinin ulaşılabilirliği, özgünlüğü, bütünlüğü ve gizliliğinden ödün verilmesine neden olacak kaza veya yasa dışı ya da kötü niyetli eylemlere direnme kabiliyetini ve kamu makamları, bilgisayar acil durum müdahale ekipleri (CERT), bilgisayar güvenlik ihlali müdahale ekipleri (CSIRT), elektronik iletişim ağ ve hizmet sağlayıcıları ve güvenlik teknolojilerinin ve hizmetlerinin sağlayıcıları tarafından sunulan veya bunlar üzerinden erişilebilen ilgili hizmetlerin güvenliğini sağlamak amacıyla kişisel verilerin, kesinlikle gereken ölçüde ve orantılı bir biçimde işlenmesi, ilgili veri sorumlusunun meşru menfaatini oluşturur. Bu, örneğin, elektronik iletişim ağlarına izinsiz erişimi ve kötü niyetli kod dağıtımının engellemesini ve "hizmet reddi" saldırıları ile bilgisayar ve elektronik iletişim sistemlerine verilen zararın durdurulmasını içerebilir.

(50) Kişisel verilerin başlangıçtaki toplanma amaçları dışındaki amaçlarla işlenmesine, yalnızca işlemenin kişisel verilerin başlangıçtaki toplanma amaçlarıyla uyumlu olduğu durumlarda izin verilmelidir. Böyle bir durumda, kişisel verilerin toplanmasına izin veren hukuki dayanağın dışında bir dayanak aranmaz. Veri işlemenin, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin kullanılması için gerekli olması halinde, Birlik veya Üye Devlet hukuku, hangi görev ve amaçlar bakımından, sonraki işlemenin uyumlu ve hukuka uygun sayılacağını belirleyebilir. Kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda yapılan sonraki işlemeler, uyumlu hukuka uygun işleme faaliyetleri olarak kabul edilmelidir. Kişisel verilerin işlenmesi için Birlik veya Üye Devlet hukuku tarafından sağlanan yasal dayanak, sonraki işlemeler için de yasal dayanak oluşturabilir. Sonraki işleme amacının kişisel verilerin başlangıçta toplanma amacına uygun olup olmadığını tespit etmek için, veri sorumlusu, orijinal işlemenin hukuka uygunluğuna ilişkin tüm gereklilikleri yerine getirdikten sonra, diğerlerinin yanı sıra, aşağıdakileri dikkate almalıdır: Bu amaçlar ile planlanan sonraki işlemenin amaçları arasındaki her türlü bağlantı; kişisel verilerin hangi bağlamda toplandığı, özellikle bunların sonraki kullanımlarına ilişkin olarak veri öznelerinin veri sorumlularıyla ilişkilerine dayalı makul beklentileri; kişisel verilerin mahiyeti; planlanan sonraki işlemenin veri özneleri için doğuracağı sonuçlar ve hem orijinal hem de planlanan sonraki işleme operasyonlarında uygun güvencelerin varlığı.

Veri öznesinin rıza verdiği veya veri işlemenin, özellikle genel kamu yararının önemli amaçlarının korunmasında demokratik bir toplumda gerekli ve orantılı bir tedbir oluşturan Birlik veya Üye Devlet hukukuna dayandığı durumlarda, veri sorumlusunun, amaçların uygunluğuna bakılmaksızın, kişisel verileri sonraki işlemeye tabi tutmasına izin verilmelidir. Her durumda, bu Tüzük'te belirtilen ilkelerin uygulanması ve özellikle veri öznesinin bu diğer amaçlara ilişkin ve itiraz hakkı da dâhil olmak üzere, haklarına ilişkin bilgi sahibi olması sağlanmalıdır. Suç teşkil eden fiillerinin veya kamu güvenliğine yönelik tehditlerin bulunmasının imkân dâhilinde olduğunun veri sorumlusu tarafından belirtilmesi ve aynı suç teşkil eden fiile ilişkin münferit vakalarda veya birden fazla vakada ya da kamu güvenliğine yönelik tehditlerle ilgili kişisel verilerin yetkili bir makama iletilmesi, veri sorumlusu tarafından gözetilen meşru menfaat kapsamında görülmelidir. Ancak, işleme hukuki, mesleki veya bir başka bağlayıcı sır saklama yükümlülüğüyle uyumlu değilse, veri

sorumlusunun meşru menfaatine olan bu tür bir iletim veya sonraki kişisel veri işlemeleri yasaklanmalıdır.

(51) Mahiyeti gereği, özellikle temel hak ve özgürlükler bakımından hassas nitelikli kişisel veriler, işlenme bağlamı temel hak ve özgürlüklere yönelik önemli riskler oluşturabileceğinden özel korumayı hak eder. Bu Tüzük'te "ırksal köken" teriminin kullanılması, ayrı insan ırklarının varlığını belirlemeye çalışan teorilerin Birlik tarafından kabul edildiği anlamına gelmediğinden, bu kişisel veriler, ırksal veya etnik kökeni ortaya koyan kişisel verileri içermelidir. Fotoğrafların işlenmesi, sistematik olarak özel kategorilerdeki kişisel verilerin işlenmesi olarak değerlendirilmemelidir, çünkü bunlar yalnızca bir gerçek kişinin kimliğinin benzersiz bir şekilde belirlenmesine veya doğrulanmasına izin veren belirli bir teknik yolla işlendiklerinde biyometrik verilerin tanımı kapsamında yer alırlar. Yasal bir yükümlülüğe uymak veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin kullanılması için, bu Tüzük kurallarının uygulanmasını sağlamak amacıyla, Üye Devletlerin hukukunda veri korumaya ilişkin spesifik hükümlerin olabileceği dikkate alınarak, bu Tüzük'te belirtilen özel durumlarda işlemeye izin verilmedikçe, bu tür kişisel veriler işlenmemelidir. Bu tür bir işleme için özel gerekliliklere ek olarak, özellikle hukuka uygun işlemenin koşulları ile ilgili olarak, bu Tüzük'ün genel ilkeleri ve diğer kuralları uygulanmalıdır. Bu türden özel kategorilerdeki kişisel verilerin işlenmesine ilişkin genel yasağın istisnaları, diğerlerinin yanı sıra, veri öznesinin açık bir biçimde rıza verdiği veya belirli gerekliliklere istinaden, özellikle de veri işleme faaliyetinin, temel özgürlüklerin kullanılmasına izin vermek amacıyla, bazı dernekler ya da vakıflar tarafından meşru faaliyetleri esnasında gerçekleştirildiği durumlarda, açıkça öngörülmelidir.

(52) Kişisel verileri ve diğer temel hakları korumak amacıyla, bu şekilde hareket etmenin kamu yararına olduğu durumlarda, özellikle iş hukuku, emeklilik ve sağlık güvenliği dâhil sosyal koruma hukuku alanlarında, izleme ve uyarı maksatlarıyla, bulaşıcı hastalıkların ve sağlığa yönelik diğer ciddi tehditlerin önlenmesi veya kontrolü ile ilgili alanlarda kişisel verilerin işlenmesinde de, özel kategorilerdeki kişisel verilerin işlenmesine ilişkin yasağa istisnalar getirilmesine, Birlik veya Üye Devlet hukukunda öngörüldüğünde ve uygun güvencelere tabi olarak izin verilmelidir. Bu tür bir istisna, özellikle sağlık sigortası sistemindeki hizmetler ve yardımlara ilişkin taleplerin karşılanmasına yönelik usullerin kalitesini ve maliyet etkinliğini sağlamak amacıyla, halk sağlığı ve sağlık hizmetlerinin yönetimi dâhil olmak üzere, sağlık amaçları için veya kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda getirilebilir. Mahkeme süreçlerinde veya idari ya da mahkeme dışı usullerde, hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması açısından gerekli olduğu durumlarda da bu tür bir kişisel verinin işlenmesine bir istisna ile izin verilmelidir

(53) Daha yüksek koruma gerektiren özel kategorilerdeki kişisel veriler, sağlıkla bağlantılı amaçlar için sadece; başta bu tür verilerin yönetim tarafından ve merkezi ulusal sağlık makamları tarafından kalite kontrolü, yönetim bilgisi ve sağlık ile sosyal bakım hizmetlerinin genel ulusal ve yerel denetimi olmak üzere, özellikle sağlık veya sosyal bakım hizmetleri ile sistemlerinin yönetilmesi bağlamında gerçek kişilerin ve bir bütün olarak toplumun yararı için bu amaçlara ulaşmak bakımından gerekli olduğunda, sağlık veya sosyal bakım hizmetlerinin ve sınır ötesi tedavi veya sağlık güvenliğinin devamlılığının sağlanması için, izleme ve uyarı amaçlarıyla veya kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla, halk sağlığı alanında kamu yararına gerçekleştirilen çalışmalarda olduğu gibi kamu yararına bir hedefi karşılaması zorunlu olan Birlik veya bir Üye Devlet hukukuna dayanılarak işlenmelidir. Bu nedenle, bu Tüzük, özel ihtiyaçlar hakkında, özellikle bu tür verilerin

işlenmesinin, hukuki bir mesleki sır saklama yükümlülüğüne tabi kişiler tarafından sağlıkla ilgili belirli amaçlar için gerçekleştirildiği durumlarda, sağlıkla ilgili özel kategorilerdeki kişisel verilerin işlenmesi için uyumlaştırılmış koşullar öngörmelidir. Birlik veya Üye Devlet hukukunda, gerçek kişilerin temel haklarının ve kişisel verilerinin korunması amacıyla özel ve uygun tedbirler öngörülmelidir. Üye Devletlerin genetik veriler, biyometrik veriler veya sağlık ile ilgili veriler bakımından, sınırlamalar da dâhil olmak üzere, ek koşulları korumalarına ya da getirmelerine izin verilmelidir. Ancak, bu durum, söz konusu koşulların, bu tür verilerin sınır ötesi işlenmesi hakkında uygulandığı hallerde, verilerin Birlik içinde serbest akışını engellememelidir.

(54) Özel kategorilerdeki kişisel verilerin işlenmesi, veri öznesinin rızası aranmaksızın, halk sağlığını ilgilendiren alanlarda kamu yararı sebepleri için gerekli olabilir. Söz konusu işleme, gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla uygun ve spesifik tedbirlere tabi olmalıdır. Bu bağlamda, "halk sağlığı", (AT) 1338/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü'nde[11] tanımlandığı şekliyle, yani morbidite ve engellilik dâhil sağlık durumu, bu sağlık durumunu etkileyen belirleyiciler, sağlık hizmetleri gereksinimleri, sağlık hizmetlerine tahsis edilen kaynaklar, sağlık hizmetlerinin sağlanması ve bu hizmetlere evrensel erişimin yanı sıra, sağlık hizmetlerine yapılan harcamalar ve finansman ile mortalite nedenleri anlamında, sağlıkla ilgili tüm unsurlar şeklinde yorumlanmalıdır. Sağlık ile ilgili verilerin kamu yararı sebepleriyle işlenmesi, kişisel verilerin, işverenler veya sigorta şirketleri ve bankalar gibi üçüncü kişiler tarafından başka amaçlarla işlenmesi gibi durumlara neden olmamalıdır.

(55) Ayrıca, kişisel verilerin resmi makamlarca anayasa hukukunda veya uluslararası kamu hukukunda belirtilmiş olan hedeflere ulaşmak amacıyla veya resmi olarak tanınmış olan dini cemiyetler bakımından işlenmesi, kamu yararı gerekçesiyle gerçekleştirilir.

(56) Seçim faaliyetleri sırasında, bir Üye Devlette demokratik sistemin işleyişinin, siyasi partilerin insanların siyasi görüşlerine ilişkin veri derlemesini gerektirmesi hâlinde, bu tür verilerin işlenmesine, uygun güvenceler sağlanması koşuluyla, kamu yararına ilişkin sebeplerle izin verilebilir.

(57) Bir veri sorumlusu tarafından işlenen verilerin, veri sorumlusunun bir gerçek kişinin kimliğini belirlemesine olanak tanımaması durumunda, veri sorumlusu yalnızca bu Tüzük'ün herhangi bir hükmüne uyum sağlamak amacıyla veri öznesinin kimliğini belirlemek üzere, ek bilgi elde etmek zorunda bırakılmamalıdır. Ancak veri sorumlusu, veri öznesinin haklarından yararlanmasını desteklemek amacıyla veri öznesinin sunduğu ek bilgiyi almayı reddetmemelidir. Kimliğin belirlenmesi, veri sorumlusu tarafından sunulan çevrim içi hizmete giriş yapmak için veri öznesi tarafından kullanılan aynı referans bilgiler gibi kimlik doğrulama mekanizması aracılığıyla doğrulama örneğinde olduğu gibi, bir veri öznesinin kimliğinin dijital olarak belirlenmesini içermelidir.

(58) Şeffaflık ilkesi, kamuya veya veri öznesine iletilen her türlü bilginin kısa, kolay erişilebilir ve anlaşılabilir olmasını ve kullanılan dilin açık ve basit olmasını ve bunlara ek olarak, uygun olduğu hallerde, görselliğin kullanılmasını gerektirir. Söz konusu bilgiler, örneğin kamuya yönelik ise, bir internet sitesi aracılığıyla elektronik olarak sağlanabilir. Bu durum özellikle çevrim içi reklamcılık gibi alanlarda aktör sayısının fazla olması ve uygulamanın teknolojik karmaşıklığı nedeniyle veri öznesinin kendisi ile ilgili kişisel verilerin toplanıp toplanmadığını, kim tarafından ve hangi amaçla toplandığını bilmesi ve anlamasının zor olduğu hallerde geçerlidir. Çocukların özel olarak korunmaları gerektiği dikkate

[11] Kamu sağlığı ile iş sağlığı ve güvenliği istatistikleri hakkında 16 Aralık 2008 tarihli ve (AT) 1338/2008 sayılı Tüzük (ABRG L 354, 31.12.2008, s.70).

alındığında, işlemenin çocuklara yönelik olduğu durumlarda, her türlü bilgi ve bilgilendirme, çocukların kolaylıkla anlayabileceği kadar açık ve sade bir dilde olmalıdır.

(59) Veri öznesinin, başta ücretsiz olarak kişisel verilere erişim ve bunların düzeltilmesi veya kalıcı olarak silinmesi ve itiraz hakkının kullanılmasını talep etme ve uygun olduğu durumlarda, ücretsiz olarak, bunları elde etme mekanizmaları da dâhil olmak üzere, bu Tüzük kapsamındaki haklarının uygulanmasını kolaylaştıracak yöntemler sağlanmalıdır. Veri sorumlusu ayrıca, özellikle kişisel verilerin elektronik yollarla işlendiği durumlarda, elektronik olarak yapılacak talepler için araçlar sağlamalıdır. Veri sorumlusu, veri öznesinden gelen taleplere fazla gecikmeksizin, en geç bir ay içinde yanıt vermek ve bu türden taleplere yanıt vermeyi planlamadığı durumlarda gerekçeler sunmakla yükümlü olmalıdır.

(60) Adil ve şeffaf veri işleme ilkeleri, veri öznesinin işleme faaliyetinin varlığı ve amaçları hakkında bilgi sahibi olmasını gerektirir. Veri sorumlusu, kişisel verilerin işlendiği özel koşulları ve bağlamı dikkate alarak, adil ve şeffaf bir veri işlemeyi temin etmek bakımından gerekli ilave bilgileri veri öznesine sağlamalıdır. Ayrıca, veri öznesine profillemenin varlığı ve sonuçları hakkında bilgi verilmelidir. Kişisel verilerin veri öznesinden toplandığı durumlarda, veri öznesine kişisel verileri sağlamakla yükümlü olup olmadığı ve bu tür verileri sağlamadığı durumlarda sonuçları hakkında bilgi verilmelidir. Bu bilgiler, planlanan işlemenin kolayca görülebilir, anlaşılabilir ve açıkça okunabilir şekilde anlamlı bir genel değerlendirmesini yapmak için standart simgelerle bir arada sağlanabilir. Simgeler elektronik olarak sunulduğunda, makine tarafından okunabilir olmalıdır.

(61) Veri öznesine ilişkin kişisel verilerin işlenmesine ilişkin bilgiler, kendilerine, bu verilerin kendilerinden toplandığı sırada veya kişisel verilerin başka kaynaktan elde edilmesi durumunda, durumun koşullarına bağlı olarak makul bir süre içinde iletilmelidir. Kişisel verilerin başka bir alıcıya meşru olarak açıklanabileceği durumlarda, veri öznesi, kişisel veriler alıcıya ilk kez açıklandığında bilgi sahibi edilmelidir. Veri sorumlusunun kişisel verileri bu verilerin toplanma amacı dışında başka bir amaçla işlemeyi planladığı durumlarda, veri sorumlusu, bu sonraki işleme faaliyetinden önce, diğer amaca ilişkin bilgileri ve diğer gerekli bilgileri veri öznesine sağlamalıdır. Çeşitli kaynaklar kullanıldığı için veri öznesine kişisel verilerin kaynağının sağlanamadığı durumlarda, genel bir bilgi sağlanmalıdır.

(62) Ancak, veri öznesinin hâlihazırda bilgiye sahip olduğu durumlarda, kişisel verilerin kaydedilmesinin veya açıklanmasının mevzuatta açık bir biçimde belirtilmiş olduğu durumlarda veya veri öznesine bilgi sağlanmasının mümkün olmadığının ya da orantısız çaba gerektireceğinin anlaşıldığı hâllerde, bilgi sağlama yükümlülüğü getirmek gerekli değildir. Veri öznesine bilgi sağlanmasının mümkün olmadığının ya da orantısız çaba gerektireceğinin anlaşıldığı hâller, özellikle işleme faaliyetinin kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları veya istatistiki amaçlarla yapıldığı durumlar olabilir. Bu bağlamda, veri öznelerinin sayısı, verilerin yaşı ve kabul edilen tüm uygun güvenceler dikkate alınmalıdır.

(63) Bir veri öznesi, kendisiyle ilgili olarak toplanmış kişisel verilere erişim hakkına sahip olmalı ve işleme faaliyetinin hukuka uygun olduğunu bilmek ve teyit etmek amacıyla, bu hakkı kolaylıkla ve makul aralıklarla kullanabilmelidir. Bu, veri öznelerinin sağlıkları ile ilgili verilere, örneğin teşhisler, muayene sonuçları, tedavi eden hekimler tarafından yapılan değerlendirmeler ve yapılan herhangi bir tedavi veya müdahale gibi bilgileri içeren tıbbi kayıtlarındaki verilere erişim hakkını içerir. Bu nedenle her bir veri öznesi, özellikle kişisel verilerin hangi amaçlarla işlendiğini, uygun olduğu durumlarda, kişisel verilerin ne kadar süreliğine işlendiğini, kişisel verilerin alıcılarını, herhangi bir otomatik kişisel veri işleme

faaliyetine dâhil olan mantığı ve en azından profillemeye dayalı olduğunda bu tür bir işleme faaliyetinin sonuçlarını bilmek ve bunlar hakkında bilgilendirme almak hakkına sahip olmalıdır. Veri sorumlusu, mümkün olduğu durumlarda, veri öznesine kişisel verilerine doğrudan erişim sağlayacağı güvenli bir sisteme uzaktan erişim imkânı sunabilmelidir. Bu hak, yazılımı koruyan telif hakkı başta olmak üzere, ticari sırlar ve fikri mülkiyet dâhil, başkalarının haklarını ve özgürlüklerini olumsuz yönde etkilememelidir. Ancak, bu durumun sonucu, veri öznesine tüm bilgileri sağlamayı reddetmek olmamalıdır. Veri sorumlusunun veri öznesi ile ilgili geniş çapta bilgi işlediği durumlarda, veri sorumlusu, bilgi iletilmeden önce, veri öznesinin talebin ilgili olduğu bilgiyi veya işleme faaliyetlerini belirtmesini talep edebilmelidir.

(64) Veri sorumlusu tarafından, özellikle çevrim içi hizmetler ve çevrim içi kimlik belirleyiciler bağlamında, erişim talep eden veri öznesinin kimliğini doğrulamak üzere her türlü makul önlem kullanılmalıdır. Veri sorumlusu kişisel verileri yalnızca potansiyel taleplere yanıt verebilmek amacıyla saklamamalıdır.

(65) Veri öznesi, kendisi ile ilgili kişisel verilerin saklanmasının, bu Tüzük'e ya da veri sorumlusunun tabi olduğu Birlik veya Üye Devlet hukukuna aykırı olduğu durumlarda, bu verilerin düzeltilmesi hakkına ve "unutulma hakkına" sahip olmalıdır. Veri öznesinin kişisel verilerinin toplanması veya başka şekilde işlenmesi amaçları bakımından söz konusu kişisel verilerin artık gerekli olmaması, veri öznesinin rızasını geri alması veya kendisiyle ilgili kişisel verilerin işlenmesine itiraz etmesi ya da kişisel verilerinin işlenmesinin başka bir nedenle bu Tüzük ile uyumlu olmaması halinde, veri öznesi özellikle, kişisel verilerini kalıcı olarak sildirme ve daha fazla işlenmemesini talep etme hakkına sahip olmalıdır. Bu hak, özellikle veri öznesinin çocukken rızasını verdiği ve işleme faaliyetinden kaynaklanan risklerin tam olarak farkında olmadığı ve daha sonra bu tür kişisel verileri, özellikle internet ortamından kaldırmak istediği durumlarda kullanılır. Veri öznesi, artık çocuk olmasa bile, bu hakkı kullanabilmelidir. Bununla birlikte, ifade özgürlüğü ve bilgi edinme hakkının kullanılması, yasal bir yükümlülüğe uyulması, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin kullanılması bakımından, halk sağlığı alanında kamu yararı sebebiyle, kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla ya da hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması açısından gerekli olduğu durumlarda, kişisel verilerin daha fazla saklanması hukuka uygun olmalıdır.

(66) Çevrim içi ortamda "unutulma hakkını" güçlendirmek için, kalıcı olarak silme hakkı, kişisel verileri herkese açık hale getiren bir veri sorumlusunun, bu kişisel verilerin bağlantılarının ya da nüshalarının veya kopyalarının kalıcı olarak silinmesi için söz konusu kişisel verileri işleyen diğer veri sorumlularına bilgi vermekle de yükümlü olacağı şekilde genişletilebilmelidir. Veri sorumlusu, bu yükümlülüğü yerine getirirken, kişisel verileri işleyen veri sorumlularına veri öznesinin talebi hakkında bilgi vermek amacıyla, teknik tedbirler dâhil olmak üzere, mevcut teknoloji ve mevcut araçları dikkate alarak makul adımlar atmalıdır.

(67) Kişisel verilerin işlenmesini kısıtlama yöntemleri, diğer yöntemlerin yanı sıra, seçilen verilerin başka bir işleme sistemine geçici olarak taşınmasını, seçilen kişisel verilerin kullanıcılar için erişilemez duruma getirilmesini veya yayınlanan verilerin bir internet sitesinden geçici olarak kaldırılmasını içerebilir. İlke olarak otomatik dosyalama sistemlerinde işleme faaliyetinin kısıtlanması, kişisel verilerin sonraki işleme faaliyetlerine tabi olmayacağı ve değiştirilemeyeceği şekilde teknik araçlarla sağlanmalıdır. Kişisel verilerin işlenmesinin kısıtlı olduğu, sistemde net bir biçimde belirtilmelidir.

(68) Kişisel verilerin işlenmesinin otomatik yollarla gerçekleştirildiği durumlarda, kişilerin kendi verileri üzerindeki kontrollerini daha fazla güçlendirmek amacıyla, veri öznesinin, veri sorumlusuna sunduğu kendisiyle ilgili kişisel verileri, yapılandırılmış, yaygın olarak kullanılan, makine tarafından okunabilir ve birlikte işletilebilir bir formatta almasına ve bunları başka bir veri sorumlusuna iletmesine de izin verilmelidir. Veri sorumluları, veri taşınabilirliğini mümkün kılan birlikte işletilebilir formatları geliştirmeye teşvik edilmelidir. Bu hak, kişisel verilerin veri öznesinin kendi rızasına dayanılarak sağlandığı veya bir sözleşmenin ifası için işleme faaliyetinin gerekli olduğu durumlarda uygulanmalıdır. Bu hak, işleme faaliyetinin rıza veya sözleşme dışında bir hukuki gerekçeye dayandığı durumlarda uygulanmamalıdır. Bu hak, doğası gereği, kişisel verileri kamu görevlerini yerine getirirken işleyen veri sorumlularına karşı kullanılmamalıdır. Bu nedenle, veri sorumlusunun tabi olduğu hukuki bir yükümlülüğe uyum sağlamak veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi ya da kontrolöre verilen resmi bir yetkinin kullanılması açısından kişisel verilerin işlenmesinin gerekli olduğu durumlarda bu husus uygulanmamalıdır. Veri öznesinin kendisiyle ilgili kişisel verileri iletme veya alma hakkı, veri sorumluları için, teknik olarak uyumlu olan işleme sistemlerini kabul etme veya bunları sürdürme yükümlülüğü oluşturmamalıdır. Birden fazla veri öznesinin söz konusu olduğu, belirli bir kişisel veri setinde, kişisel verileri alma hakkı, bu Tüzük uyarınca, diğer veri öznelerinin haklarına ve özgürlüklerine halel getirmemelidir. Ayrıca bu hak, bu Tüzük'te belirtildiği haliyle, veri öznesinin kişisel verileri kalıcı olarak sildirme hakkını elde etmesine ve bu hakkın kısıtlamalarına halel getirmemelidir ve özellikle de, söz konusu sözleşmenin ifası için veri öznesi tarafından, gerekli olduğu sürece ve gerekli olduğu ölçüde sağlanan kendisi ile ilgili kişisel verilerin, kalıcı olarak silinmesini ifade etmemelidir. Teknik açıdan uygulanabilir olması halinde, veri öznesinin, kişisel verilerini bir veri sorumlusundan diğerine doğrudan ilettirme hakkı bulunmalıdır.

(69) Bununla birlikte, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi ya da veri sorumlusuna verilen resmi yetkinin kullanılması amacıyla veya bir veri sorumlusunun ya da üçüncü kişilerin meşru menfaatleri gerekçelerine dayanarak kişisel verilerin hukuka uygun olarak işlenebildiği durumlarda, veri öznesi, kendi özel durumuyla ilgili herhangi bir kişisel verinin işlenmesine itiraz etme hakkına sahip olmalıdır. Zorlayıcı meşru menfaatlerinin, veri öznesinin menfaatlerine veya temel hak ve özgürlüklerine ağır bastığının gösterilmesi sorumluluğu veri sorumlusuna aittir.

(70) Kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, veri öznesinin, bu türden bir doğrudan pazarlama ile alakalı olduğu ölçüde, ilk işleme veya sonraki işlemelerle ilgili olması fark etmeksizin, profilleme de dâhil olmak üzere, kendisi ile ilgili kişisel verilerin işlenmesine her zaman ve ücretsiz olarak itiraz etme hakkı bulunmalıdır. Bu hak, veri öznesinin dikkatine açıkça ve diğer tüm bilgilerden ayrı olarak net bir şekilde sunulmalıdır.

(71) Veri öznesi, sadece otomatik işlemeye dayalı olan ve kendisini ilgilendiren hukuki sonuçlar doğuran veya benzer şekilde kendisini büyük oranda etkileyen, sürece herhangi bir insan dahli olmadan çevrim içi kredi başvurusunun otomatik olarak reddedilmesi ya da çevrim içi işe alma uygulamaları gibi kendisi ile ilgili kişisel veçheleri değerlendiren bir tedbiri içerebilecek bir karara tabi olmama hakkına sahip olmalıdır. Bu tür veri işleme, kendisi ile ilgili hukuki sonuçlar doğurduğu veya benzer şekilde kendisini büyük oranda etkilediği durumlarda, , özellikle veri öznesinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri veya ilgi alanları, güvenilirliği ya da davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi için, gerçek bir kişiye ilişkin kişisel veçheleri değerlendiren, kişisel verilerin tüm otomatik işlenme türlerini ihtiva eden "profillemeyi" içerir. Bununla birlikte, Birlik kurumlarının veya ulusal gözetim

organlarının düzenlemeleri, standartları ve tavsiyeleri uyarınca yürütülen hile ve vergi kaçakçılığını izleme ve önleme amaçları dâhil olmak üzere ve veri sorumlusu tarafından sağlanan bir hizmetin güvenliğini ve güvenilirliğini sağlamak amacıyla veya veri öznesi ve veri sorumlusu arasında bir sözleşmenin yapılması veya ifası için gerekli olduğunda, veya veri öznesinin açık rızasını verdiğinde, veri sorumlusuna Birlik hukuku veya tabi olduğu Üye Devlet hukuku tarafından açıkça izin verildiği durumlarda, profilleme dâhil, bu türden bir veri işlemeye dayalı karar alınmasına müsaade edilmelidir. Her hâlükârda, bu tür bir veri işleme; kendi görüşünü ifade etme, bu tür bir değerlendirmeden sonra verilen karara dair açıklama elde etme ve bu karara itiraz etme amaçlarıyla, veri öznesinin spesifik olarak aydınlatılmasını ve sürece insan müdahalesinin sağlanması hakkını içermesi gereken uygun güvencelere tabi olmalıdır. Bu tedbir, bir çocukla ilgili olamaz.

Kişisel verilerin işlendiği özel koşulları ve bağlamı göz önünde bulundurarak, veri öznesi ile ilgili adil ve şeffaf bir veri işleme faaliyeti gerçekleştirilmesinin temini amacıyla, veri sorumlusu, profilleme için uygun matematiksel ve istatistiki usulleri kullanmalı, özellikle kişisel verilerde yanlışlıklara yol açan unsurların düzeltilmesini ve hata riskinin en aza indirilmesini sağlamak için uygun teknik ve kurumsal tedbirleri uygulamalı, kişisel verileri, veri öznesinin menfaatleri ve hakları bakımından ortaya çıkabilecek potansiyel riskleri göz önünde bulunduracak ve diğerlerinin yanı sıra, ırk veya etnik köken, siyasi görüş, din veya inançlar, sendika üyeliği, genetik durum veya sağlık durumu veya cinsel yönelim temeline dayanan ya da böyle bir etkiye sahip tedbirlerle sonuçlanan, gerçek kişiler üzerindeki ayrımcı etkileri önleyecek bir şekilde korumalıdır. Otomatik karar almaya ve özel kategorilerdeki kişisel verilere dayanan profillemeye sadece özel koşullar altına izin verilmelidir.

(72) Profilleme, veri işleme için hukuki gerekçeler veya veri koruma ilkeleri gibi, bu Tüzük'ün kişisel verilerin işlenmesini düzenleyen kurallarına tabidir. Bu Tüzük ile kurulan Avrupa Veri Koruma Kurulu ("Kurul"), bu bağlamda rehber ilkeler yayımlayabilmelidir.

(73) Doğal veya insan kaynaklı afetlere karşı insan hayatının korunması dahil olmak üzere kamu güvenliğini, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması ve kovuşturulması ya da cezaların infaz edilmesini, düzenlenmiş mesleklere yönelik etik ihlallerin önlenmesini, soruşturulmasını ve kovuşturulmasını veya Birlik'in ya da bir Üye Devletin önemli bir ekonomik veya mali çıkarı, genel kamu yararı gerekçesiyle halka açık sicillerin tutulması, arşivlenen kişisel verilerin eski totaliter devlet rejimleri altındaki siyasi davranışlarla ilgili spesifik bilgiler sağlamak için sonraki işlenmesi veya sosyal koruma, halk sağlığı veya insani amaçları da kapsayacak şekilde veri öznesinin veya başkalarının hak ve özgürlüklerinin korunması başta olmak üzere Birlik'in veya bir Üye Devletin genel kamu yararına yönelik diğer önemli amaçlarını temin etmek üzere, belirli ilkeler ve bilgi edinme haklarına, kişisel verilere erişim ve bunların düzeltilmesi veya kalıcı olarak silinmesine, veri taşınabilirliği hakkına, itiraz hakkına, profillemeye dayalı kararlar ile kişisel veri ihlali hakkında bir veri öznesinin bilgilendirilmesine ve veri sorumlularının ilgili belirli yükümlülüklerine ilişkin olarak, demokratik bir toplumda gerekli ve orantılı olduğu ölçüde Birlik veya Üye Devlet hukuku uyarınca kısıtlamalar getirilebilir. Bu kısıtlamalar, Şart'ta ve İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi'nde belirtilen gerekliliklere uygun olmalıdır.

(74) Veri sorumlusu tarafından veya veri sorumlusu adına gerçekleştirilen kişisel verilerin herhangi bir şekilde işlenmesi için veri sorumlusunun sorumluluk ve yükümlülüğü tesis edilmelidir. Özellikle, veri sorumlusu uygun ve etkili tedbirleri uygulamakla yükümlü olmalı ve tedbirlerin etkililiği de dâhil, veri işleme faaliyetlerinin bu Tüzük ile uyumunu

ortaya koyabilmelidir. Söz konusu tedbirler, veri işlemenin mahiyeti, kapsamı, bağlamı ve amaçları ile gerçek kişilerin hak ve özgürlüklerine yönelik riski dikkate almalıdır.

(75) Gerçek kişilerin hak ve özgürlükleri açısından değişen olasılık ve ağırlıktaki riskler, özellikle şu durumlarda fiziksel, maddi veya manevi zarara yol açabilecek kişisel veri işlemeden kaynaklanabilir: veri işlemenin ayrımcılık, kimlik hırsızlığı veya kimlikte sahtecilik, mali kayıp, itibarın zedelenmesi, mesleki sır saklamayla korunan kişisel verilerin gizliliğinin kaybedilmesi, takma adın izinsiz şekilde geri getirilmesi veya diğer önemli ekonomik veya sosyal dezavantajlar ile sonuçlanabileceği durumlar; veri öznesinin hak ve özgürlüklerinden mahrum bırakılabileceği veya kişisel verileri üzerinde kontrol sahibi olmasının engellenebileceği durumlar; ırk veya etnik köken, siyasi görüşler, din veya felsefi inançlar, sendika üyeliği ve genetik verilerin işlenmesi, sağlıkla ilgili veriler veya cinsel yaşam veya mahkûmiyet kararları ve suçlar ile ilgili veriler veya ilgili güvenlik önlemlerini açığa çıkaran kişisel verilerin işlendiği durumlar; kişisel profiller oluşturmak veya kullanmak amacıyla özellikle iş yeri performansı, ekonomik durum, sağlık, kişisel tercihler veya ilgi alanları, güvenilirlik veya davranış, konum veya hareketlerle ilgili hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere, kişisel veçhelerin değerlendirildiği durumlar; çocuklar başta olmak üzere savunmasız gerçek kişilerin kişisel verilerinin işlendiği durumlar veya işlemenin büyük oranda kişisel veri içerdiği ve çok sayıda veri öznesini etkilediği durumlar.

(76) Veri öznesinin hak ve özgürlüklerine yönelik riskin olasılığı ve ağırlığı, veri işlemenin mahiyeti, kapsamı, bağlamı ve amaçlarına göre belirlenmelidir. Risk, veri işleme faaliyetlerinin bir risk veya yüksek bir risk içerip içermediğine ilişkin objektif bir değerlendirme esasında tespit edilmelidir.

(77) Özellikle, veri işleme ile ilgili riskin belirlenmesi, bunun menşe, mahiyet, olasılık ve ağırlık açısından değerlendirilmesi ile riskin azaltılmasına yönelik iyi uygulamaların belirlenmesine ilişkin olarak, veri sorumlusu veya veri işleyen tarafından uygun tedbirlerin uygulanması ve uygunluğun gösterilmesi konusunda, bilhassa onaylı davranış kuralları, onaylı sertifikalar, Kurul tarafından sağlanan kılavuzlar veya bir veri koruma görevlisi tarafından sağlanan göstergeler aracılığıyla kılavuzluk sağlanabilir. Kurul, ayrıca gerçek kişilerin hak ve özgürlüklerine yönelik yüksek risk oluşturması muhtemel olmayan veri işleme faaliyetlerine ilişkin kılavuzlar yayınlayabilir ve bu tür durumlarda söz konusu riski ele almak üzere hangi tedbirlerin yeterli olabileceğini belirtebilir.

(78) Gerçek kişilerin kişisel verilerin işlenmesine ilişkin hak ve özgürlüklerinin korunması, bu Tüzük'ün gerekliliklerini karşılamaya uygun teknik ve kurumsal tedbirlerin alınmasını gerektirir. Bu Tüzük'e uygunluğun ortaya konulabilmesi amacıyla, veri sorumlusu iç politikaları kabul etmeli ve özellikle tasarımdan itibaren ve varsayılan olarak veri koruma ilkelerine riayet eden tedbirleri uygulamalıdır. Söz konusu tedbirler, diğerlerinin yanı sıra, kişisel verilerin işlenmesini en aza indirgeme, kişisel verilerde mümkün olan en kısa sürede takma ad kullanımı, kişisel verilerin işlevleri ve işlenmesiyle ilgili olarak şeffaflığın sağlanması, veri öznesinin veri işlemeyi takip etmesine olanak sağlanması ve veri sorumlusunun güvenlik özellikleri oluşturup bunları iyileştirmesine imkân tanınmasından oluşabilir. Kişisel verilerin işlenmesine dayalı uygulama, hizmet ve ürünlerin geliştirilmesi, tasarlanması, seçilmesi ve kullanılması veya görevlerin yerine getirilmesinde kişisel verilerin işlenmesi sırasında, son teknolojiye uygun olarak ve veri sorumlusu ve veri işleyenlerin veri koruma yükümlülüklerini yerine getirebilmelerini sağlamak amacıyla, ürün, hizmet ve uygulama üreticilerinin, söz konusu ürün, hizmet ve uygulamaları geliştirirken ve tasarlarken veri koruma hakkını dikkate almaları teşvik edilmelidir. Tasarımdan itibaren ve varsayılan olarak veri koruma ilkeleri, kamu ihaleleri bağlamında da dikkate alınmalıdır.

(79) Veri işleme faaliyetinin amaç ve yollarının veri sorumlusu tarafından diğer veri sorumlularıyla birlikte belirlendiği veya işleme faaliyetinin bir veri sorumlusu adına yapıldığı haller de dâhil olmak üzere, veri öznelerinin hak ve özgürlükleri ile denetim makamlarının izleme faaliyetleri ve tedbirlerine ilişkin veri sorumlusu ve veri işleyenlerin sorumluluk ve yükümlülüklerinin korunması, bu Tüzük kapsamındaki sorumlulukların açık bir şekilde dağıtılmasını gerektirir.

(80) Birlik içinde kurulu olmayan ve işleme faaliyetleri, veri öznesinin ödeme yapmasının gerekli olup olmadığına bakılmaksızın Birlik içindeki veri öznelerine mal veya hizmetlerin sunulmasıyla ya da Birlik içinde gerçekleştiği sürece söz konusu veri öznelerinin davranışlarının izlenmesiyle ilgili olan bir veri sorumlusu veya veri işleyenin, Birlik içinde veri öznelerinin kişisel verilerini işlediği durumlarda, veri sorumlusu veya veri işleyen; işleme faaliyetinin nadiren gerçekleştiği, geniş ölçekli olarak özel kategorilerdeki kişisel verilerin işlenmesini veya mahkûmiyet kararları veya suçlarla ilgili kişisel verilerin işlenmesini içermediği ve söz konusu işlemenin, mahiyeti, bağlamı, kapsamı ve amaçları ve veri sorumlusunun bir kamu makamı veya organı olup olmadığı dikkate alınarak, gerçek kişilerin hak ve özgürlüklerine yönelik bir riske sebebiyet vermesi ihtimalinin bulunmadığı haller hariç olmak üzere, bir temsilci atamalıdır. Temsilci, veri sorumlusu veya veri işleyen adına hareket etmelidir ve herhangi bir denetim makamı tarafından muhatap alınabilir. Temsilci, veri sorumlusunun veya veri işleyenin bu Tüzük kapsamındaki yükümlülükleri ile ilgili olarak onun adına hareket etmesi için verdiği yazılı bir yetki ile açık bir şekilde belirlenmelidir. Böyle bir temsilcinin görevlendirilmesi, veri sorumlusunun veya veri işleyenin bu Tüzük kapsamındaki sorumluluğunu veya yükümlülüğünü etkilemez. Bu temsilci, bu Tüzük'e uyum sağlanması amacıyla alınan herhangi bir önleme ilişkin olarak yetkili denetim makamlarıyla işbirliği yapılması da dâhil olmak üzere, veri sorumlusu veya veri işleyenin verdiği yetkiye göre görevlerini yerine getirmelidir. Belirlenen temsilci, veri sorumlusu veya veri işleyenin herhangi bir uygunsuzluğu durumunda, zorlayıcı işlemlere tabi tutulmalıdır.

(81) Veri sorumlusu adına veri işleyen tarafından gerçekleştirilecek işleme faaliyeti ile ilgili olarak bu Tüzük'ün gerekliliklerine uyum sağlanması amacıyla, bir veri işleyene işleme faaliyetlerini devrederken veri sorumlusu, işleme faaliyetinin güvenliği de dâhil, bu Tüzük'ün gerekliliklerini yerine getirecek teknik ve kurumsal tedbirleri uygulamak için özellikle uzman bilgisi, güvenilirlik ve kaynaklar bağlamında yalnızca yeterli güvenceleri sağlayan veri işleyenleri kullanmalıdır. Veri işleyenin onaylı davranış kurallarına veya bir onaylı belgelendirme mekanizmasına riayeti, veri sorumlusunun yükümlülüklerine uyumunu kanıtlamak için bir unsur olarak kullanılabilir. İşleme faaliyetinin bir veri işleyen tarafından yürütülmesi, Birlik veya Üye Devlet hukuku çerçevesinde düzenlenen, veri işleyeni veri sorumlusuna bağlayan ve yürütülecek işleme faaliyeti ve veri öznesinin hak ve özgürlüklerine yönelik riskler bağlamında veri işleyenin spesifik görev ve sorumlulukları dikkate alınmak suretiyle işleme faaliyetinin konusunun ve süresinin, işleme faaliyetinin mahiyetinin ve amaçlarının, kişisel verilerin türünün ve veri öznelerinin kategorilerinin belirlendiği bir sözleşme veya başka bir hukuki tasarruf ile düzenlenmelidir. Veri sorumlusu ve veri işleyen, münferit bir sözleşmeyi veya doğrudan Komisyon tarafından kabul edilen standart sözleşme hükümlerini ya da tutarlılık mekanizmasına uygun olarak bir denetim makamı ve takiben Komisyon tarafından kabul edilen standart sözleşme hükümlerini kullanmayı tercih edebilir. Veri sorumlusu adına işlemenin tamamlanmasının ardından, Birlik hukuku veya veri işleyenin tabi olduğu Üye Devlet hukuku uyarınca kişisel verilerin depolanmasına ilişkin bir gereklilik olmadığı müddetçe, veri işleyen, veri sorumlusunun seçimine bağlı olarak kişisel verileri iade etmeli veya silmelidir.

(82) Bu Tüzük'e uyumun gösterilmesi açısından, veri sorumlusu veya veri işleyen, sorumluluğu altındaki işleme faaliyetlerinin kayıtlarını tutmalıdır. Her bir veri sorumlusu ve veri işleyen, denetim makamları ile işbirliği yapmakla ve bu işleme faaliyetlerinin izlenebilmesi için söz konusu kayıtları talep üzerine sunmakla yükümlü olmalıdır.

(83) Güvenliği sağlamak ve bu Tüzük'e aykırı işlemeleri önlemek amacıyla, veri sorumlusu veya veri işleyen, işleme sürecinde yer alan riskleri değerlendirmeli ve bu riskleri azaltmaya yönelik, şifreleme gibi önlemler uygulamalıdır. Bu tedbirler, riskler ve korunacak kişisel verilerin mahiyeti ile ilgili son teknoloji ve uygulama maliyetleri dikkate alınarak, gizlilik de dâhil olmak üzere, uygun bir güvenlik düzeyini temin etmelidir. Veri güvenliği riski değerlendirilirken, iletilen, depolanan veya başka şekilde işlenen kişisel verilerin; özellikle fiziksel, maddi veya manevi zarara yol açabilen, kazara veya hukuka aykırı olarak yok edilmesi, kaybı, değiştirilmesi, izinsiz olarak açıklanması veya bunlara erişilmesi gibi işleme faaliyetinin yol açtığı riskler özellikle göz önünde bulundurulmalıdır.

(84) İşleme faaliyetlerinin gerçek kişilerin hak ve özgürlüklerine yönelik yüksek risk oluşturmasının muhtemel olduğu durumlarda bu Tüzük'e uyumun artırılması amacıyla, veri sorumlusu, özellikle riskin kaynağını, niteliğini, mahiyetini ve ağırlığını ele almak üzere bir veri koruma etki değerlendirmesinin yürütülmesinden sorumlu olmalıdır. Kişisel verilerin işlenmesi faaliyetinin bu Tüzük'e uyumlu olduğunu göstermeye yönelik olarak alınacak uygun tedbirlerin belirlenmesinde, söz konusu değerlendirmenin sonucu dikkate alınmalıdır. Bir veri koruma etki değerlendirmesi, işleme faaliyetlerinin, veri sorumlusunun mevcut teknolojisi ve uygulama maliyetleri açısından uygun tedbirlerle azaltamayacağı ölçüde yüksek bir risk içerdiğini gösterdiği takdirde, işleme faaliyeti öncesinde denetim makamı ile istişarede bulunulmalıdır.

(85) Kişisel veri ihlali, uygun bir şekilde ve zamanında ele alınmadığı takdirde, gerçek kişilere, kişisel verileri üzerindeki kontrolü kaybetmeleri veya haklarının sınırlandırılması, ayrımcılık, kimlik hırsızlığı veya kimlikte sahtecilik, takma adın izinsiz şekilde geri getirilmesi, itibarın zedelenmesi, mesleki sır saklama ile korunan kişisel verilerin gizliliğinin kaybedilmesi veya söz konusu gerçek kişiye yönelik diğer önemli ekonomik veya sosyal dezavantajlar gibi fiziksel, maddi veya manevi zarara neden olabilir. Bu sebeple, hesap verebilirlik ilkesi doğrultusunda kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından riske sebebiyet vermesinin muhtemel olmadığını kanıtlayabildiği haller hariç olmak üzere, veri sorumlusu, kişisel veri ihlali olduğunu fark eder etmez fazla gecikmeksizin ve uygun olması hâlinde, ihlalden haberdar olduktan itibaren en geç 72 saat içinde, söz konusu kişisel veri ihlalini denetim makamına bildirmelidir. Bu bildirimin 72 saat içinde yapılamadığı hallerde, bu bildirimde gecikme sebeplerine de yer verilir ve bilgiler, daha fazla gecikmeksizin aşamalı olarak sağlanabilir.

(86) Kişisel veri ihlalinin gerçek kişinin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusu, söz konusu kişinin gerekli tedbirleri alabilmesini teminen, fazla gecikmeksizin, veri öznesini kişisel veri ihlaline ilişkin bilgilendirmelidir. Söz konusu bilgilendirmede, kişisel veri ihlalinin mahiyetinin yanı sıra olası olumsuz etkilerin hafifletilmesi için söz konusu gerçek kişiye yönelik tavsiyeler yer almalıdır. Veri öznelerine yönelik söz konusu bilgilendirmeler, mantıken mümkün olan en kısa sürede ve denetim makamı ile yakın iş birliği içinde, denetim makamının kendisi veya kolluk makamları gibi ilgili diğer makamlar tarafından hazırlanan kılavuz ilkelere riayet edilerek yapılmalıdır. Örneğin, ani bir zarar riskinin azaltılmasına yönelik ihtiyaç, veri öznelerine hızlı bir şekilde bilgilendirme yapılmasını gerektirirken, devamlılık arz eden veya benzer nitelikli kişisel veri ihlallerine karşı uygun tedbirlerin

uygulanmasına yönelik ihtiyaç, bilgilendirmenin daha uzun bir sürede yapılmasını haklı gösterebilir.

(87) Kişisel veri ihlalinin gerçekleşip gerçekleşmediğinin hızla tespit edilmesi ve denetim makamı ile veri öznesine gecikmeksizin bilgi verilmesi amacıyla uygun tüm teknolojik koruma tedbirlerinin ve kurumsal tedbirlerin uygulandığından emin olunmalıdır. Bildirimin fazla gecikmeksizin yapıldığı hususu, özellikle kişisel veri ihlalinin mahiyeti ve ağırlığı ile bunun veri öznesi açısından sonuçları ve olumsuz etkileri dikkate alınarak belirlenmelidir. Söz konusu bildirim, bu Tüzük'te yer alan görev ve yetkilerine uygun olarak denetim makamının müdahalesi ile sonuçlanabilir.

(88) Kişisel veri ihlallerinin bildirilmesinde uygulanacak format ve usullere ilişkin ayrıntılı kuralların belirlenmesinde, kişisel verilerin kimlikte sahtecilik veya diğer suiistimallerin gerçekleşme olasılığını etkili bir şekilde sınırlandıran uygun teknik koruma tedbirleriyle korunup korunmadığı da dâhil olmak üzere, ihlalin gerçekleştiği koşullar dikkate alınmalıdır. Ayrıca, erken açıklamanın kişisel veri ihlaline ilişkin koşulların soruşturulmasını gereksiz yere engelleyebileceği durumlarda, söz konusu kurallar ve usuller, kolluk makamlarının meşru menfaatlerini göz önünde bulundurmalıdır.

(89) 95/46/AT sayılı Direktif, kişisel verilerin işlendiğinin denetim makamlarına bildirilmesi yönünde genel bir yükümlülük öngörmüştür. Bu yükümlülük, idari ve mali yüklere yol açarken, kişisel verilerin korunmasının iyileştirilmesine her durumda katkıda bulunmamıştır. Bu nedenle, fark gözetmeyen bu tür genel bildirim yükümlülükleri kaldırılmalı ve bunların yerini, mahiyeti, kapsamı, bağlamı ve amaçları bakımından gerçek kişilerin hak ve özgürlüklerine yönelik yüksek risk oluşturması muhtemel işleme faaliyetlerine odaklanan etkili usuller ve mekanizmalar almalıdır. Bu tür işleme faaliyetleri, özellikle yeni teknolojilerin kullanılmasını içeren veya daha önce veri sorumlusu tarafından hakkında herhangi bir veri koruma etki değerlendirilmesinin yapılmadığı ya da ilk işleme faaliyetinden bu yana geçen sürede gerekli hale gelen yeni türden faaliyetler olabilir.

(90) Söz konusu durumlarda, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarıyla riskin kaynakları dikkate alınmak suretiyle, yüksek riskin olasılığını ve şiddetini değerlendirmek amacıyla, veri sorumlusu tarafından, işleme faaliyetinden önce bir veri koruma etki değerlendirmesi yapılmalıdır. Bu etki değerlendirmesi, özellikle söz konusu riski azaltmaya, kişisel verilerin korunmasını sağlamaya ve bu Tüzük'e uyum sağlandığını göstermeye yönelik öngörülen tedbirleri, güvenceleri ve mekanizmaları içermelidir.

(91) Bu özellikle, büyük miktarda kişisel veriyi bölgesel, ulusal veya uluslar üstü düzeyde işlemeyi hedefleyen, çok sayıda veri öznesini etkileyebilecek ve örneğin, elde bulunan teknolojik bilgi düzeyine göre büyük ölçüde yeni bir teknolojinin kullanıldığı ve verilerin hassasiyeti nedeniyle yüksek riske yol açması muhtemel olan büyük ölçekli işleme faaliyetleri ile veri öznelerinin haklarını kullanmasını zorlaştıran işleme faaliyetleri başta olmak üzere, veri öznelerinin hak ve özgürlükleri açısından yüksek riske yol açan diğer işleme faaliyetlerinde uygulanmalıdır. Veri koruma etki değerlendirmesi, ayrıca, profillemeye dayalı olarak, gerçek kişilerle ilgili kişisel veçhelere ilişkin sistematik ve kapsamlı bir değerlendirmenin ardından ya da özel kategorilerdeki kişisel verilerin, biyometrik verilerin veya mahkûmiyet kararlarına ve suçlara veya ilgili güvenlik tedbirlerine ilişkin verilerin işlenmesinin ardından, belirli gerçek kişilere yönelik kararların alınması amacıyla kişisel verilerin işlendiği durumlarda da yapılmalıdır. Veri koruma etki değerlendirmesi, optik-elektronik cihazların kullanıldığı faaliyetler veya yetkili denetim makamının; özellikle veri öznelerinin bir hakkı, hizmeti veya sözleşmeyi kullanmalarına engel teşkil etmesi veya sistematik olarak geniş ölçekte yapılması nedeniyle işleme faaliyetinin, veri öznelerinin hak ve özgürlükleri açısından yüksek risk oluşturma ihtimali

olduğunu düşündüğü diğer faaliyetler başta olmak üzere, kamuya açık alanların geniş ölçekte izlenmesi için de aynı derecede gereklidir. İşleme faaliyetinin, tek bir hekim, başka bir sağlık çalışanı veya avukat tarafından hastalardan veya müvekkillerden alınan kişisel verilerle ilgili olması durumunda, kişisel verilerin işlenmesi, geniş ölçekte işleme olarak değerlendirilmemelidir. Bu tür durumlarda, veri koruma etki değerlendirmesi zorunlu olmamalıdır.

(92) Örneğin kamu makamlarının veya organlarının ortak bir uygulama veya işleme platformu tesis etmek istedikleri veya birkaç veri sorumlusunun bir sanayi sektörünün tamamına veya bir kısmına yönelik ya da yaygın kullanılan yatay bir faaliyete ilişkin ortak bir uygulama veya işleme ortamı getirmeyi planladıkları durumlarda, veri koruma etki değerlendirmesinin konusunun tek bir projeden daha kapsamlı olması makul ve hesaplı olabilir.

(93) Bir kamu makamı veya kamu organının görevlerini yerine getirmesinin dayandığı ve belirli bir işleme faaliyetini ya da faaliyetler dizisini düzenleyen Üye Devlet mevzuatının kabulü bağlamında, Üye Devletler, işleme faaliyetlerinden önce böyle bir değerlendirme yapılmasını gerekli görebilirler.

(94) Bir veri koruma etki değerlendirmesinin; riski azaltmaya yönelik güvencelerin, güvenlik tedbirlerinin ve mekanizmalarının bulunmadığı hallerde işleme faaliyetinin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk oluşturacağını göstermesi ve veri sorumlusunun, riskin mevcut teknolojiler ve uygulama maliyetleri açısından makul yollarla azaltılamayacağı kanaatinde olması durumunda, işleme faaliyetlerine başlamadan önce denetim makamı ile istişarede bulunulması gerekir. Bu tür yüksek risk, işleme faaliyetinin bazı türlerinden, kapsamından ve sıklığından kaynaklanabilir ve aynı zamanda gerçek kişinin hak ve özgürlüklerine zarar verilmesine veya müdahaleye yol açabilir. Denetim makamı, belirli bir süre içinde istişare talebine yanıt vermelidir. Ancak, denetim makamının söz konusu sürede herhangi bir yanıt vermemesi, işleme faaliyetlerini yasaklama yetkisi de dâhil olmak üzere, denetim makamının bu Tüzük'te belirtilen görev ve yetkileri uyarınca gerçekleştireceği hiçbir müdahaleye halel getirmez. Bu istişare sürecinin bir parçası olarak, gerçek kişilerin hak ve özgürlüklerine yönelik riskin azaltılması için öngörülen tedbirler başta olmak üzere, söz konusu işleme faaliyetine ilişkin yürütülen veri koruma etki değerlendirmesinin sonucu denetim makamına sunulabilir.

(95) Veri işleyen, gerekli hallerde ve talep üzerine, veri koruma etki değerlendirmelerinin gerçekleştirilmesinden ve denetim makamı ile ön istişare yapılmasından kaynaklanan yükümlülüklere uyumun sağlanmasında veri sorumlusuna yardımcı olmalıdır.

(96) Planlanan işleme faaliyetinin bu Tüzük'e uyumunun sağlanması ve özellikle veri öznesi açısından riskin azaltılması amacıyla, kişisel verilerin işlenmesini öngören yasal veya düzenleyici tedbirin hazırlanması aşamasında denetim makamı ile de istişarede bulunulmalıdır.

(97) İşleme faaliyetinin, kendi yargı yetkisi çerçevesinde hareket eden mahkemeler veya bağımsız yargı makamları haricindeki bir kamu makamı tarafından gerçekleştirilmesi hâlinde; özel sektörde, işleme faaliyetinin, temel faaliyetleri veri öznelerinin geniş ölçekte düzenli ve sistematik bir şekilde izlenmesini gerektiren işleme faaliyetlerini içeren bir veri sorumlusu tarafından gerçekleştirilmesi hâlinde veya veri sorumlusu veya veri işleyenin temel faaliyetlerinin özel kategorilerdeki kişisel verilerin ve mahkûmiyet kararlarına ve suçlara ilişkin verilerin geniş ölçekte işlenmesini içermesi hâlinde; bu Tüzüğe iç uyumun izlenmesi için, veri sorumlusu veya veri işleyene, veri koruma hukuku ve uygulamalarına ilişkin uzmanlık bilgisine sahip bir kişi yardımcı olmalıdır. Özel sektörde, veri sorumlusunun temel faaliyetleri, birincil faaliyetleriyle ilgilidir ve kişisel verilerin bir yan

faaliyet olarak işlenmesi ile ilgisi yoktur. Gerekli uzmanlık bilgisi düzeyi, özellikle, gerçekleştirilen veri işleme faaliyetlerine ve veri sorumlusu veya veri işleyen tarafından işlenen kişisel verilerin gerektirdiği korumaya göre belirlenmelidir. Bu tür veri koruma görevlileri, veri sorumlusunun çalışanı olup olmamalarına bakılmaksızın, görev ve sorumluluklarını bağımsız bir biçimde gerçekleştirecek bir konumda olmalıdır.

(98) Veri sorumlusu ya da veri işleyen kategorilerini temsil eden birlikler ve diğer organlar, bu Tüzük sınırları dâhilinde ve bu Tüzük'ün etkili bir şekilde uygulanmasını kolaylaştıracak şekilde, belirli sektörlerde gerçekleştirilen işleme faaliyetlerinin kendilerine has özelliklerini ve mikro, küçük ve orta ölçekli işletmelerin spesifik ihtiyaçlarını dikkate almak suretiyle davranış kuralları oluşturmak yönünde teşvik edilmelidirler. Söz konusu davranış kuralları, özellikle, işleme faaliyetinin gerçek kişilerin hak ve özgürlükleri açısından yol açacağı riskleri dikkate alarak, veri sorumlusu veya veri işleyenin yükümlülüklerini belirleyebilir.

(99) Davranış kurallarının hazırlanmasında ya da bu kuralların değiştirilmesi veya kapsamının genişletilmesi durumunda, veri sorumlusu ya da veri işleyen kategorilerini temsil eden birlikler ve diğer organlar, uygun hallerde veri özneleri de dâhil olmak üzere ilgili paydaşlarla istişarede bulunmalı ve söz konusu istişarelere cevaben bildirilen görüş ve fikirleri dikkate almalıdır.

(100) Bu Tüzük'e uyumu ve şeffaflığı arttırmak üzere, veri öznelerinin ilgili ürün ve hizmetlerin veri koruma düzeyini hızlı bir şekilde değerlendirmelerine olanak verecek şekilde, belgelendirme mekanizmaları ile veri koruma mühür ve işaretlerinin oluşturulması teşvik edilmelidir.

(101) Birlik dışındaki ülkelerle ve uluslararası kuruluşlarla karşılıklı kişisel veri akışı, uluslararası ticaretin ve uluslararası iş birliğinin genişlemesi bakımından gereklidir. Söz konusu veri akışındaki artış, kişisel verilerin korunması bakımından yeni zorlukları ve endişeleri beraberinde getirmiştir. Bununla birlikte, kişisel verilerin Birlik içinden üçüncü ülkelerdeki veri sorumlularına, veri işleyenlere veya diğer alıcılara veya uluslararası kuruluşlara aktarıldığı hallerde, üçüncü ülkeden veya uluslararası kuruluştan, aynı ülkedeki veya başka bir üçüncü ülkedeki veya başka bir uluslararası kuruluştaki veri sorumlularına veya veri işleyenlere tekrar aktarımlar da dâhil olmak üzere, Birlik içinde bu Tüzük ile temin edilen gerçek kişilere yönelik koruma düzeyine zarar verilmemelidir. Her hâlükârda, üçüncü ülkelere ve uluslararası kuruluşlara yapılan aktarımlar, ancak bu Tüzük ile tam uyum sağlanması hâlinde gerçekleşebilir. Bir aktarım ancak, bu Tüzük'ün diğer hükümlerine tabi olarak, veri sorumlusu veya veri işleyen tarafından bu Tüzük'ün kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına ilişkin hükümlerinde belirtilen koşullara uyum sağlanması hâlinde gerçekleşebilir.

(102) Bu Tüzük, Birlik ve üçüncü ülkeler arasında akdedilen ve veri özneleri için uygun güvenceleri de içerecek şekilde kişisel veri aktarımlarını düzenleyen anlaşmalara halel getirmez. Üye Devletler, söz konusu anlaşmalar bu Tüzük'ü veya Birlik hukukunun diğer hükümlerini etkilemediği ve veri öznelerinin temel haklarına yönelik uygun düzeyde bir koruma içerdiği sürece, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasını içeren uluslararası anlaşmalar akdedebilirler.

(103) Komisyon, bir üçüncü ülkenin, bir veya üçüncü ülkedeki bir bölgenin veya belirli bir sektörün veya bir uluslararası kuruluşun, uygun düzeyde veri koruması sağladığına ve dolayısıyla bu düzeyde koruma sağladığı düşünülen üçüncü ülke veya uluslararası kuruluşun Birlik içinde de gereken hukuki belirliliği ve yeknesaklığı sağladığına, tüm Birlik bakımından geçerli olacak şekilde karar verebilir. Bu gibi durumlarda, kişisel verilerin, söz konusu üçüncü ülkeye veya uluslararası kuruluşa aktarımı, ilave bir onaya

ihtiyaç olmaksızın gerçekleşebilir. Komisyon, söz konusu üçüncü ülkeye veya uluslararası kuruluşa gerekçelerin tamamının yer aldığı bir açıklama ve bildirim iletmek suretiyle, söz konusu kararın yürürlükten kaldırılmasına da karar verebilir.

(104) Komisyon, başta insan haklarının korunması olmak üzere Birlik'in üzerine kurulu olduğu temel değerlere uygun olarak, üçüncü ülkeye veya bir üçüncü ülkedeki bir bölgeye veya belirli bir sektöre ilişkin değerlendirmesinde, belirli bir üçüncü ülkede hukukun üstünlüğüne, adalete erişime, uluslararası insan hakları norm ve standartlarına ve kamu güvenliği, savunma ve milli güvenlik mevzuatı ile kamu düzeni ve ceza hukuku dâhil olmak üzere, genel ve sektörel hukuk konularına nasıl riayet edildiğini dikkate almalıdır. Üçüncü ülkedeki bir bölge veya belirli bir sektöre ilişkin bir yeterlilik kararı verilirken, bu ülkedeki özel işleme faaliyetleri ve geçerli hukuki standartların kapsamı ve yürürlükteki mevzuat gibi açık ve nesnel kriterler dikkate alınmalıdır. Üçüncü ülke, özellikle kişisel verilerin bir veya daha fazla sayıdaki belirli sektörde işlenmesi hâlinde, Birlik içinde sağlanan güvencelere temelde eşdeğer olacak yeterli düzeyde bir koruma sağlayan güvenceler sunmalıdır. Üçüncü ülke özellikle, etkili bağımsız veri koruma denetimi sağlamalı ve Üye Devletlerin veri koruma makamları ile iş birliği mekanizmaları öngörmelidir ve veri öznelerine etkili ve uygulanabilir haklar ile etkili idari ve adli tazmin sağlanmalıdır.

(105) Komisyon, üçüncü ülke veya uluslararası kuruluşun üstlendiği uluslararası taahhütlerin haricinde, kişisel verilerin korunması ile ilgili olanlar başta olmak üzere, üçüncü ülkenin veya uluslararası kuruluşun çok taraflı veya bölgesel sistemlere katılımından kaynaklanan yükümlülükleri ve bu yükümlülüklerin uygulanmasını dikkate almalıdır. Özellikle, üçüncü ülkenin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi ve Ek Protokolü'ne katılımı dikkate alınmalıdır. Komisyon, üçüncü ülkelerdeki veya uluslararası kuruluşlardaki koruma düzeyine ilişkin olarak değerlendirmede bulunurken Kurula danışmalıdır.

(106) Komisyon, bir üçüncü ülkedeki veya üçüncü ülkedeki bir bölgedeki veya belirli bir sektördeki veya uluslararası bir kuruluştaki koruma düzeyine ilişkin kararların işleyişini izlemelidir ve 95/46/AT sayılı Direktif'in 25(6) maddesine ve 26(4) maddesine dayalı olarak kabul edilen kararların işleyişini izlemelidir. Komisyon yeterlilik kararlarında, kararların işleyişi bakımından düzenli bir gözden geçirme mekanizması sağlamalıdır. Gözden geçirme, söz konusu üçüncü ülke veya uluslararası kuruluş ile istişare içinde gerçekleştirilmeli ve üçüncü ülke veya uluslararası kuruluştaki ilgili tüm gelişmeler göz önünde bulundurulmalıdır. Komisyon, izlemenin ve gözden geçirme faaliyetlerinin amaçları bakımından, Avrupa Parlamentosu ve Konseyin yanı sıra ilgili diğer organ ve kaynakların görüş ve bulgularını dikkate almalıdır. Komisyon, makul bir süre içinde, söz konusu kararların işleyişini değerlendirmelidir ve ilgili bulguları, 16 Şubat 2011 tarihli ve (AB) 182/2011 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü[12] kapsamında söz konusu Tüzük ile oluşturulan Komiteye, Avrupa Parlamentosuna ve Konseye bildirmelidir.

(107) Komisyon, bir üçüncü ülkenin veya üçüncü ülkedeki bir bölge veya belirli bir sektörün veya bir uluslararası kuruluşun artık yeterli düzeyde bir veri koruması sağlamadığına karar verebilir. Bunun sonucunda, bağlayıcı şirket kuralları da dahil, uygun güvencelere tabi aktarımlara ilişkin olarak bu Tüzük'te yer alan gereklilikler ve spesifik durumlara yönelik derogasyonlar karşılanmadığı sürece, söz konusu üçüncü ülkeye veya uluslararası kuruluşa kişisel verilerin aktarımı yasaklanmalıdır. Bu durumda, Komisyon ile söz konusu

[12] Komisyonun uygulama yetkilerini kullanması ile ilgili olarak Üye Devletler tarafından yararlanılacak kontrol mekanizmalarına ilişkin kurallar ve genel ilkeleri belirleyen 16 Şubat 2011 tarihli ve (AB) 182/2011 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ABRG L 55, 28.2.2011, s. 13).

üçüncü ülkeler veya uluslararası kuruluşlar arasında istişare sağlanmasına imkân tanınmalıdır. Komisyon, makul bir süre içinde, üçüncü ülkeyi veya uluslararası kuruluşu gerekçeler konusunda bilgilendirmelidir ve durumun düzeltilmesi için istişarelere başlamalıdır.

(108) Yeterlilik kararı olmaması hâlinde, veri sorumlusu veya veri işleyen, veri öznesi için uygun güvenceler temin etmek suretiyle üçüncü ülkedeki veri koruma eksiğini telafi edecek tedbirler almalıdır. Söz konusu uygun güvenceler, bağlayıcı şirket kurallarının, Komisyon tarafından kabul edilen standart veri koruma hükümlerinin, bir denetim makamı tarafından kabul edilen standart veri koruma hükümlerinin veya bir denetim makamı tarafından izin verilen sözleşme hükümlerinin kullanılması şeklinde olabilir Bu güvenceler, Birlik içinde veya üçüncü ülkede, etkili idari ve adli şikâyet ve tazminat talep etme hakkını da içerecek şekilde, uygulanabilir veri öznesi haklarının ve etkili kanun yollarının mevcut olması da dâhil olmak üzere, veri koruma gereklilikleri ile Birlik içinde işlemeye uygun veri öznesi haklarına uyulmasını sağlamalıdır. Güvenceler, başta kişisel verilerin işlenmesine yönelik genel ilkelere uyum olmak üzere, tasarımdan itibaren ve varsayılan olarak veri koruma ilkeleri ile de ilişkili olmalıdır. Veri aktarımları aynı zamanda veri özneleri için uygulanabilir ve etkili haklar öngören, mutabakat zaptı gibi idari düzenlemelere eklenecek olan hükümlere de dayalı olmak üzere, kamu makamları veya organları tarafından, üçüncü ülkelerdeki kamu kuruluşları veya organları ile ya da eşdeğer görev ve işleyişe sahip uluslararası kuruluşlarla da gerçekleştirilebilir. Güvencelerin yasal bağlayıcılığı olmayan idari düzenlemelerde öngörülmesi hâlinde, yetkili denetim makamından izin alınmalıdır.

(109) Veri sorumlusu veya veri işleyenin Komisyon veya denetim makamı tarafından kabul edilen standart veri koruma hükümlerini kullanması, veri sorumlularının veya veri işleyenlerin standart veri koruma hükümlerini veri işleyen ile başka bir veri işleyen arasındaki bir sözleşme gibi daha kapsamlı bir sözleşmeye dâhil etmelerine veya doğrudan veya dolaylı olarak Komisyon veya denetim makamınca kabul edilmiş olan hükümlerle çatışmadığı veya veri öznelerinin temel hak ve özgürlüklerine halel gelmediği müddetçe başka hükümler veya ilave güvenceler eklemelerine engel teşkil etmemelidir. Veri sorumluları ve veri işleyenler, sözleşmeye bağlı taahhütler vasıtasıyla standart koruma hükümlerini tamamlayacak ilave güvenceler sağlamaya teşvik edilmelidir.

(110) Ortak bir ekonomik faaliyette bulunan bir teşebbüsler grubu veya bir işletmeler grubu, bahse konu şirket kuralları aktarımlar veya kişisel veri aktarım kategorileri için uygun güvencelerin sağlanmasına yönelik tüm temel ilkeleri ve uygulanabilir hakları içerdiği müddetçe, Birlik'ten ortak bir ekonomik faaliyette bulunan aynı teşebbüs grubu veya işletmeler grubunun organizasyonlarına gerçekleştirdiği uluslararası aktarımlarda, onaylı bağlayıcı şirket kurallarını kullanabilmelidir.

(111) Veri öznesinin açık rızasını vermiş olduğu belirli şartlar altında, aktarımın bir sözleşme veya hak talebi için gerekli ve nadir olması hâlinde, adli işlemler kapsamında veya düzenleyici organlar nezdindeki süreçler de dâhil olmak üzere idari veya mahkeme dışı usuller kapsamında olup olmadığına bakılmaksızın, aktarımın sağlanması imkânı tanınmalıdır. Birlik veya Üye Devlet hukukuyla belirlenen, kamu yararına ilişkin önemli gerekçelerin gerektirdiği hallerde veya aktarımın mevzuatla oluşturulmuş ve kamunun veya meşru menfaati bulunan kişilerin istişaresi için tutulan bir sicilden yapılması durumunda da veri aktarımının sağlanması imkânı tanınmalıdır İkinci durumda, veri aktarımı, sicilde bulunan kişisel verilerin tamamını veya tüm veri kategorilerini içermemelidir ve sicilin meşru menfaati bulunan kişilerin istişaresine açık olması hâlinde aktarım yalnızca bu kişilerin talebi üzerine veya bu kişilerin alıcı konumunda olduğu

durumlarda veri öznelerinin menfaatleri ve temel hakları bütünüyle dikkate alınarak gerçekleştirilmelidir.

(112) Bu istisnalar özellikle, rekabet kuruluşları, vergi veya gümrük idareleri arasında, mali denetim makamları arasında, sosyal güvenlik konularında yetkili birimler arasında veya örneğin salgın hastalıklarda temas geçmişinin incelenmesi ya da sporda dopingin azaltılması ve/veya önlenmesinin amaçlandığı durumlarda kamu sağlığı alanında uluslararası veri paylaşımı gibi kamu yararına ilişkin önemli gerekçelerle zorunlu ve gerekli veri aktarımlarında uygulanmalıdır. Veri öznesinin rıza veremeyecek durumda olması hâlinde, aktarımın veri öznesinin veya diğer kişilerin, fiziksel bütünlük veya yaşam da dâhil, hayati menfaatlerinin korunması açısından gerekli olması durumunda kişisel verilerin aktarılması hukuka uygun olarak kabul edilmelidir. Bir yeterlilik kararı olmaması durumunda, Birlik veya Üye Devlet hukukunda, kamu yararına ilişkin önemli gerekçelerden dolayı, özel kategorilerdeki kişisel verilerin bir üçüncü ülkeye veya bir uluslararası kuruluşa aktarılmasına ilişkin sınırlar açık bir şekilde konabilir. Üye Devletler söz konusu hükümleri Komisyon'a bildirir. Cenevre Sözleşmeleri kapsamında gerekli bir görevi yerine getirmek veya silahlı çatışmalarda uygulanabilir uluslararası insancıl hukuka uyum sağlamak amacıyla, fiziksel veya hukuki olarak rıza veremeyecek durumdaki bir veri öznesinin kişisel verilerinin uluslararası bir insani yardım kuruluşuna aktarılması, kamu yararına ilişkin önemli bir gerekçe olması veya veri öznesinin hayati menfaatine olması nedeniyle gerekli kabul edilebilir.

(113) Bunun yanı sıra, yinelemeli nitelikte olmadığı değerlendirilen ve yalnızca sınırlı sayıda veri öznesini ilgilendiren aktarımlar da, veri sorumlusu tarafından gözetilen ve karşısında veri öznesinin menfaatleri veya hakları ile özgürlüklerinin ağır basmadığı zorlayıcı meşru menfaatler doğrultusunda ve veri sorumlusunun veri aktarımı ile ilgili tüm koşulları değerlendirmiş olması şartıyla gerçekleştirilebilir. Veri sorumlusu, kişisel verilerin mahiyetini, önerilen işleme faaliyetinin veya faaliyetlerinin amacını ve süresini ve bunların yanı sıra, menşe ülke, üçüncü ülke ve nihai hedef ülkedeki durumu özellikle dikkate almalıdır ve kişisel verilerinin işlenmesi bakımından gerçek kişilerin temel hak ve özgürlüklerini koruyacak uygun güvenceler sağlamalıdır. Söz konusu aktarımlar yalnızca, aktarım için diğer hiçbir gerekçenin uygulanabilir olmadığı geriye kalan durumlarda mümkün olmalıdır. Bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar bakımından, toplumun daha fazla bilgi edinme yönündeki meşru beklentileri dikkate alınmalıdır. Veri sorumlusu, denetim makamını ve veri öznesini aktarım hususunda bilgilendirir.

(114) Her hâlükârda, Komisyon tarafından bir üçüncü ülkedeki yeterli veri koruma düzeyine ilişkin karar alınmamış olması hâlinde, veri sorumlusu veya veri işleyen; veri öznelerinin temel haklardan ve güvencelerden yararlanmaya devam edebilmelerini teminen, söz konusu veriler aktarıldıktan sonra bu verilerin Birlik içinde işlenmesi hakkında uygulanabilir ve etkili haklar sağlayan çözümleri kullanmalıdır.

(115) Bazı üçüncü ülkeler, gerçek ve tüzel kişilerin Üye Devletlerin yargı yetkisi dâhilindeki işleme faaliyetlerinin doğrudan düzenlenmesini amaçlayan kanunlar, tüzükler ve diğer hukuki tasarruflar kabul eder. Bu tasarruflar, üçüncü ülkelerdeki mahkemelerce veya heyetlerce veya idari makamlarca alınan, bir veri sorumlusunun veya veri işleyenin kişisel verileri aktarmasını veya açıklamasını gerektiren ve Birlik ya da bir Üye Devlet ile talepte bulunan üçüncü ülke arasında yürürlükte olan bir karşılıklı hukuki yardım antlaşması gibi bir uluslararası anlaşmaya dayanmayan kararları içerebilir. Söz konusu kanunların, tüzüklerin ve diğer hukuki tasarrufların sınırların dışında uygulanması uluslararası hukukun ihlali anlamına gelebilir ve bu Tüzük ile Birlik içinde sağlanan, gerçek kişilerin korunması amacına ulaşılmasını engelleyebilir. Aktarımlara, ancak üçüncü ülkelere

aktarım için bu Tüzük'te öngörülen şartların karşılanması hâlinde izin verilmelidir. Bu durum, diğerlerinin yanı sıra, verileri açıklamanın, Birlik hukuku veya veri sorumlusunun tabi olduğu Üye Devlet hukukunda kabul edilen, kamu yararına ilişkin önemli bir gerekçe için gerekli olduğu hallerde söz konusu olabilir.

(116) Kişisel verilerin Birlik sınırları dışına çıkması, gerçek kişilerin kendilerini özellikle söz konusu bilginin hukuka aykırı olarak kullanılmasından veya açıklanmasından korumaya yönelik veri koruma haklarını kullanabilmelerine yönelik riski artırabilir. Bunun yanı sıra, denetim makamları, sınırları dışındaki faaliyetlerle ilgili şikâyetleri takip edemeyeceğine veya bunlara ilişkin soruşturma yürütemeyeceğine karar verebilir. Denetim makamlarının sınır-ötesi çerçevede birlikte çalışma yönündeki çabaları da, önlemeye veya düzeltmeye yönelik yetkilerinin yetersiz olması, hukuk rejimlerinin uyumsuzluğu ve kaynak kısıtları gibi uygulamaya ilişkin zorluklar nedeniyle engellenebilir. Bu nedenle, veri koruma denetim makamlarının uluslararası muhataplarıyla bilgi alışverişinde bulunmalarına ve birlikte soruşturma yürütmelerine yardımcı olacak daha yakın bir iş birliğinin geliştirilmesine ihtiyaç bulunmaktadır. Kişisel verilerin korunmasına ilişkin mevzuatın uygulanması için gereken karşılıklı uluslararası yardımın kolaylaştırılmasına ve sağlanmasına yönelik uluslararası iş birliği mekanizmalarının geliştirilmesi amacıyla, Komisyon ve denetim makamları, mütekabiliyet temelinde ve bu Tüzük uyarınca, üçüncü ülkelerdeki yetkili makamlarla, bilgi alışverişinde bulunmalı ve yetkilerinin kullanılmasına ilişkin faaliyetlerde iş birliği yapmalıdır.

(117) Üye Devletlerde görevlerini yerine getirmek ve yetkilerini kullanmak üzere tam bağımsızlık içinde yetkilendirilmiş denetim makamlarının kurulması, gerçek kişilerin, kişisel verilerinin işlenmesiyle ilgili olarak korunmalarının temel unsurlarından biridir. Üye Devletler, anayasal, kurumsal ve idari yapılarını yansıtacak şekilde birden fazla denetim makamı kurabilmelidirler.

(118) Denetim makamlarının bağımsızlığı, bu makamların mali harcamaları bakımından kontrol ve izleme mekanizmalarına veya yargı denetimine tabi olmayacağı anlamına gelmemelidir.

(119) Bir Üye Devlet, birden fazla denetim makamı tesis ederken, bahse konu denetim makamlarının tutarlılık mekanizmasına etkin biçimde katılımını sağlayacak mekanizmaları da mevzuatla tesis etmelidir. Söz konusu Üye Devlet özellikle, diğer denetim makamları, Kurul ve Komisyon arasında hızlı ve sorunsuz iş birliğinin sağlanması amacıyla, bu makamların söz konusu mekanizmaya etkin katılımlarının sağlanması bakımından tek temas noktası işlevini üstlenen denetim makamını belirlemelidir.

(120) Her denetim makamına Birlik çapında diğer denetim makamlarıyla karşılıklı yardım ve iş birliğine ilişkin olanlar da dâhil olmak üzere, görevlerini etkili biçimde yerine getirebilmeleri için gereken mali kaynaklar, insan kaynakları, tesisler ve altyapı sağlanmalıdır. Her denetim makamının, genel devlet bütçesi veya ulusal bütçenin parçası olabilecek ayrı bir yıllık kamu bütçesi olmalıdır.

(121) Denetim makamı üyesi veya üyeleriyle ilgili genel şartlar, her Üye Devlet'te mevzuatla belirlenmelidir ve özellikle bu üyelerin hükumet veya bir hükumet üyesinin ya da parlamento veya parlamento alt meclisinin ya da Üye Devlet hukuku uyarınca yetkilendirilmiş bağımsız bir organın önerisi üzerine, şeffaf bir usulle, parlamento, hükumet ya da Üye Devlet'in devlet başkanı tarafından atanmasını öngörmelidir. Denetim makamının bağımsızlığını sağlamak amacıyla, üye veya üyeler dürüstlük içinde hareket etmeli; görevlerine uygun olmayan eylemlerden kaçınmalı ve görev süreleri boyunca, maddi getirisi olsun ya da olmasın, bu göreve uygun olmayan hiçbir işle iştigal

etmemelidirler. Denetim makamının, Üye Devlet hukuku ile tesis edilmiş bağımsız bir organ ya da denetim makamı tarafından seçilmiş kendi personeli bulunmalıdır ve söz konusu personel denetim makamı üyesi veya üyelerinin münhasır yönlendirmesine tabi olmalıdır.

(122) Her denetim makamı, bu Tüzük uyarınca kendisine verilen görevleri yerine getirmek ve yetkileri kullanmak üzere kendi Üye Devleti topraklarında yetkili olmalıdır. Bu husus, özellikle kendi Üye Devlet topraklarındaki veri sorumlusuna veya veri işleyene ait kuruluşun faaliyetleri bağlamındaki işleme faaliyetini, kamu yararına hareket eden kamu makamları veya özel organlar tarafından gerçekleştirilen kişisel verilerin işlenmesi faaliyetini, kendi topraklarındaki veri öznelerini etkileyen işleme faaliyetini, ya da Birlik içinde yerleşik olmayan veri sorumlusu veya veri işleyen tarafından gerçekleştirilen ancak denetim makamının topraklarında ikamet eden veri öznelerinin hedef alındığı işleme faaliyetini kapsamalıdır. Veri öznesi tarafından yapılan şikâyetlerin ele alınması, bu Tüzük'ün uygulanmasına ilişkin soruşturmalar yürütülmesi ve kişisel verilerin işlenmesine ilişkin riskler, kurallar, güvenceler ve haklar konusunda kamu farkındalığının artırılması da bu kapsamda yer almalıdır.

(123) Denetim makamları, kişisel verilerinin işlenmesiyle ilgili olarak gerçek kişileri korumak ve kişisel verilerin iç pazarda serbest akışını kolaylaştırmak amacıyla bu Tüzük uyarınca hükümlerin uygulanmasını izlemeli ve Birlik içinde tutarlı bir şekilde uygulanmalarına katkı sağlamalıdır. Bu amaçla denetim makamları, karşılıklı yardım sağlanması ve iş birliği konusunda Üye Devletler arasında herhangi bir anlaşmaya gerek duymaksızın birbirleriyle ve Komisyon ile iş birliği yapmalıdırlar.

(124) Kişisel veri işleme faaliyetinin, veri sorumlusu veya veri işleyenin Birlik içindeki bir kuruluşunun faaliyetleri bağlamında gerçekleşmesi ve söz konusu veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te kurulu olması hâlinde veya bir veri sorumlusu veya veri işleyenin Birlik içindeki tek bir kuruluşunun faaliyetleri bağlamında gerçekleşen veri işlemenin, birden fazla Üye Devlet'teki veri öznelerini kayda değer ölçüde etkilemesi veya etkileme ihtimali bulunması hâlinde, veri sorumlusu veya veri işleyenin ana kuruluşunun veya veri sorumlusu veya veri işleyenin tek kuruluşunun denetim makamı, baş makam sıfatıyla hareket etmelidir. Denetim makamı ilgili diğer makamlarla, bunların Üye Devletlerinin topraklarında veri sorumlusu veya veri işleyenin bir kuruluş sahibi olması, bunların topraklarında ikamet eden veri öznelerinin kayda değer ölçüde etkilenmesi veya bunlara bir şikâyetin iletilmesi durumunda, iş birliği yapmalıdır. Ayrıca, söz konusu Üye Devlet'te ikamet etmeyen bir veri öznesi şikâyette bulunduğunda, şikâyetin yapıldığı denetim makamı da aynı zamanda bir ilgili denetim makamı olmalıdır. Kurul, bu Tüzük'ün uygulanmasına ilişkin her türlü konu hakkında kılavuz yayımlama görevleri çerçevesinde, özellikle söz konusu işlemenin birden fazla Üye Devlet'teki veri öznelerini kayda değer ölçüde etkileyip etkilemediğini belirlemek amacıyla dikkate alınması gereken kriterlere ve neyin yerinde ve gerekçeli bir itiraz teşkil edeceğine ilişkin kılavuzlar yayımlayabilmelidir.

(125) Baş makam, bu Tüzük uyarınca kendisine verilen yetkilerin uygulanmasına yönelik tedbirlere ilişkin bağlayıcı kararlar almaya yetkili olmalıdır. Denetim makamı, baş makam sıfatıyla, karar alma sürecinde yer alan denetim makamlarını konuya yakından dâhil etmeli ve bu makamlar ile koordinasyonu sağlamalıdır. Veri öznesi tarafından yapılan şikâyetin tamamen veya kısmen reddedilmesi kararı verilecekse, söz konusu karar şikâyetin iletildiği denetim makamı tarafından alınmalıdır.

(126) Karar, baş denetim makamı ve ilgili denetim makamlarının ortak mutabakatıyla alınmalı; veri sorumlusu veya veri işleyenin ana veya tek kuruluşuna yönelik olmalı ve veri

sorumlusu ve veri işleyen açısından bağlayıcı olmalıdır. Veri sorumlusu veya veri işleyen, bu Tüzük'e uyum sağlanması ve Birlik içindeki işleme faaliyetleri ile ilgili olarak bahse konu veri sorumlusu veya veri işleyenin ana kuruluşunun baş denetim makamına bildirilen kararın uygulanması için gereken tedbirleri almalıdır.

(127) Baş denetim makamı olarak hareket etmeyen her denetim makamı, veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te kurulu olduğu, ancak örneğin işleme faaliyetinin konusunun, bir Üye Devlet'te, çalışanların kişisel verilerinin spesifik olarak istihdam bağlamında işlenmesine ilişkin olduğu durumlar gibi, anılan konunun sadece tek bir Üye Devlet'te yürütülen işleme faaliyetine ilişkin olduğu ve yalnızca söz konusu Üye Devlet'teki veri öznelerini kapsadığı durumlarda, yerel vakaları ele almaya yetkili olmalıdır. Bu tür durumlarda, denetim makamı, baş denetim makamını, konu hakkında gecikmeksizin bilgilendirmelidir. Baş denetim makamı, bilgilendirildikten sonra, konuyu baş denetim makamı ve diğer ilgili denetim makamları arasındaki iş birliğine ("tek hizmet noktası mekanizması") ilişkin hüküm uyarınca ele alıp almayacağına ya da bilgiyi veren denetim makamının vakayı yerel düzeyde ele alıp almaması gerektiğine karar vermelidir. Baş denetim makamı vakayı ele alıp almayacağına karar verirken, veri sorumlusu veya veri işleyene karşı alınan kararın etkili bir şekilde uygulanmasını sağlamak üzere, veri sorumlusu veya veri işleyenin, bilgiyi veren denetim makamının bulunduğu Üye Devlet'te bir kuruluşunun olup olmadığını dikkate almalıdır. Baş denetim makamının vakayı ele almaya karar vermesi hâlinde, bilgiyi veren denetim makamının bir karar taslağı sunma imkânı olmalıdır ve baş denetim makamı, söz konusu tek hizmet noktası mekanizması çerçevesinde karar taslağını hazırlarken, bu taslağı önemle göz önünde bulundurmalıdır

(128) İşlemenin kamu makamları veya özel organlar tarafından kamu yararına gerçekleştirildiği durumlarda, baş denetim makamına ve tek hizmet noktası mekanizmasına ilişkin kurallar uygulanmamalıdır. Bu tür durumlarda, söz konusu kamu kuruluşunun veya özel organın kurulu olduğu Üye Devlet'teki denetim makamı, bu Tüzük uyarınca kendisine verilen yetkileri kullanmaya muktedir olan tek denetim makamı olmalıdır.

(129) Bu Tüzük'ün tüm Birlik içinde tutarlı bir şekilde izlenmesini ve uygulanmasını sağlamak maksadıyla, her Üye Devlet içinde denetim makamları, özellikle de gerçek kişilerden şikâyet gelmesi durumunda, Üye Devlet hukuku çerçevesinde soruşturma makamlarının yetkilerine halel gelmeksizin, bu Tüzük'e ilişkin ihlalleri adli makamların dikkatine sunmak ve hukuk süreçlerine dâhil olmak üzere; soruşturma yetkileri, düzeltme yetkileri ve yaptırımlar, izin ve danışma yetkileri dâhil, aynı görevleri ve tesirli yetkileri haiz olmalıdır. Söz konusu yetkiler, işleme yasağı da dâhil olmak üzere geçici veya kati bir sınırlama getirme yetkisini de içermelidir. Üye Devletler, bu Tüzük kapsamında kişisel verilerin korunmasına ilişkin başka görevler belirleyebilir. Denetim makamlarının yetkileri, Birlik ve Üye Devlet hukukunda belirlenen uygun usuli güvenceler uyarınca tarafsız, adil ve makul bir süre içinde kullanılmalıdır. Bu Tüzük'e uyumun sağlamasını teminen ve her münferit vakanın koşullarını dikkate alınması suretiyle; özellikle her bir tedbir uygun, gerekli ve orantılı olmalı, kişiyi olumsuz yönde etkileyebilecek bireysel bir tedbir alınmadan önce herkesin dinlenilme hakkını gözetmeli, gereksiz harcamalara ve veri öznelerine yönelik aşırı zorluklara meydan vermemelidir. Tesislere erişime ilişkin soruşturma yetkileri, ön adli izin alınması koşulu gibi Üye Devlet'in usul hukuku kapsamındaki belirli şartlar uyarınca kullanılmalıdır. Denetim makamı tarafından alınan ve hukuki bağlayıcılığı bulunan her tedbir yazılı, açık ve net olmalı; tedbiri alan denetim makamını ve tedbirin alınma tarihini belirtmeli; denetim makamı başkanının veya başkan tarafından yetkilendirilen denetim makamı üyesinin imzasını taşımalı; tedbirin gerekçelerini sunmalı ve etkili bir hukuk yoluna başvurma hakkına işaret etmelidir. Bu durum, Üye Devlet'in usul hukuku uyarınca öngörülen ek gerekliliklere engel teşkil

etmemelidir. Hukuki olarak bağlayıcı olan bir kararın kabul edilmesi, bu kararın, kararı kabul eden denetim makamının bulunduğu Üye Devlet'te yargı denetimine mahal verebileceği anlamına gelir.

(130) Şikâyetin yapıldığı denetim makamının baş denetim makamı olmadığı durumlarda baş denetim makamı, şikâyetin yapıldığı denetim makamı ile bu Tüzük'te belirtilen işbirliği ve tutarlılığa ilişkin hükümlere uygun olarak yakın işbirliği içinde bulunmalıdır. Bu tür durumlarda baş denetim makamı, idari para cezaları kesilmesi de dâhil, hukuki sonuçlar doğuracak tedbirleri alırken şikâyetin yapıldığı ve baş denetim makamı ile irtibat halinde kendi Üye Devleti'nin topraklarında soruşturma yürütülmesi konusunda yetkili olması gereken denetim makamının görüşünü önemle göz önünde bulundurmalıdır.

(131) Başka bir denetim makamının veri sorumlusu veya veri işleyenin işleme faaliyetleri için baş denetim makamı olarak hareket etmesi gerektiği; ancak şikâyetin somut konusunun veya olası ihlalin, yalnızca şikâyetin iletildiği veya olası ihlalin tespit edildiği Üye Devlet'teki veri sorumlusunun veya veri işleyenin işleme faaliyetlerini ilgilendirdiği ve konunun diğer Üye Devletlerdeki veri öznelerini kayda değer ölçüde etkilemediği veya etkileme olasılığının bulunmadığı hallerde, şikâyeti alan veya bu Tüzüğün olası ihlallerine yol açan durumları tespit eden ya da bunlardan başka şekilde haberdar olan denetim makamı, veri sorumlusuyla barışçıl bir çözüm yoluna gitmelidir ve bunun yetersiz kalması halinde, her türlü yetkisini kullanmalıdır. Bu durum şunları içermelidir: denetim makamının bulunduğu Üye Devlet toprağında yürütülen özel işleme faaliyeti veya söz konusu Üye Devlet toprağında bulunan veri özneleri bakımından; özellikle denetim makamının bulunduğu Üye Devlet'in toprağında bulunan veri öznelerini hedefleyen mal veya hizmet sunumu bağlamında yürütülen işleme faaliyeti veya Üye Devlet hukuku çerçevesinde ilgili hukuki yükümlülükler dikkate alınarak değerlendirilmesi gereken işleme faaliyeti.

(132) Denetim makamları tarafından halka yönelik düzenlenen farkındalık arttırıcı faaliyetler, eğitim bağlamında; gerçek kişilerin yanı sıra mikro, küçük ve orta ölçekli işletmeler de dâhil, veri sorumluları ve veri işleyenlere yönelik özel tedbirleri kapsamalıdır.

(133) Denetim makamları, bu Tüzük'ün iç pazarda tutarlı bir şekilde tatbik edilmesini ve uygulanmasını sağlayacak şekilde, görevlerini yerine getirirken birbirlerine destek olmalı ve karşılıklı yardımda bulunmalıdırlar. Karşılıklı yardım talep eden bir denetim makamı, karşılıklı yardım talebine diğer denetim makamının talebi almasından itibaren bir ay içinde herhangi bir yanıt alamazsa, bir geçici tedbir kabul edebilir.

(134) Her denetim makamı, uygun durumlarda, diğer denetim makamları ile ortak operasyonlara katılmalıdır. Talebin iletildiği denetim makamı, verilen süre içinde talebe yanıt vermekle yükümlü olmalıdır.

(135) Bu Tüzük'ün Birlik içinde tutarlı bir şekilde uygulanmasını sağlamak maksadıyla, denetim makamları arasında işbirliğine yönelik bir tutarlılık mekanizması kurulmalıdır. Söz konusu mekanizma özellikle, denetim makamının, birden fazla Üye Devlet'te kayda değer sayıda veri öznesini önemli ölçüde etkileyen işleme faaliyetleri bakımından hukuki sonuçlar doğuracak bir tedbir alma niyetinde olduğunda uygulanmalıdır. Herhangi bir ilgili denetim makamının veya Komisyonun söz konusu konunun tutarlılık mekanizması bağlamında ele alınması gerektiğini öne sürdüğü durumlarda da bu mekanizma uygulanmalıdır. Bu mekanizma ile Komisyonun Antlaşmalar'dan kaynaklanan yetkilerini kullanması sırasında alabileceği tedbirlere halel gelmez.

(136) Kurul, tutarlılık mekanizmasını uygularken, üyelerinin çoğunluğunun bu yönde karar vermesi veya herhangi bir ilgili denetim makamının veya Komisyonun bu yönde talepte

bulunması durumunda, belirli bir süre içinde görüş bildirmelidir. Kurul, denetim makamları arasında anlaşmazlıklar olması durumunda hukuki bağlayıcılığı olan kararlar alma yetkisine de sahip olmalıdır. Bu amaçla Kurul, denetim makamları arasında, özellikle de işbirliği mekanizması içinde baş denetim makamı ve ilgili denetim makamları arasında, davanın esası ve özellikle bu Tüzük'ün ihlal edilip edilmediği konusunda çelişkili görüşlerin bulunduğu, açıkça belirlenmiş durumlarda, ilke olarak üyelerinin üçte iki çoğunluğuyla hukuki bağlayıcılığı olan kararlar almalıdır.

(137) Veri öznelerinin hak ve özgürlüklerini korumak için, özellikle de bir veri öznesinin hakkının kullanılmasının önemli ölçüde engellenmesi tehlikesi bulunan hâllerde, acil olarak harekete geçmek gerekebilir. Bu nedenle bir denetim makamı, kendi topraklarında üç ayı geçmemesi gereken belirli bir geçerlilik süresi için uygun şekilde gerekçelendirilmiş geçici tedbirleri alabilmelidir.

(138) Söz konusu mekanizmanın uygulanması, bunun uygulanmasının zorunlu olduğu durumlarda, denetim makamı tarafından alınan ve hukuki sonuçlar doğurması amaçlanan tedbirin hukuka uygunluğu için bir koşul olmalıdır. Sınır ötesi ile ilişkili diğer durumlarda, baş denetim makamı ve ilgili denetim makamları arasında işbirliği mekanizması uygulanmalıdır ve ilgili denetim makamları arasında karşılıklı yardım ve ortak operasyonlar, tutarlılık mekanizmasını harekete geçirmeden, ikili veya çok taraflı olarak yürütülebilmelidir.

(139) Bu Tüzük'ün tutarlı bir şekilde uygulanmasını teşvik etmek için, Birliğin bağımsız bir organı olarak Kurul tesis edilmelidir. Kurul, hedeflerini gerçekleştirmek için tüzel kişiliğe sahip olmalıdır. Kurul, Başkanı tarafından temsil edilmelidir. Kurul, 95/46/AT sayılı Direktif ile kurulan Kişisel Verilerin İşlenmesi Bakımından Bireylerin Korunması Hakkında Çalışma Grubu'nun yerini almalıdır. Kurul, her Üye Devlet'in denetim makamının başkanı ile Avrupa Veri Koruma Denetçisi veya bunların her birinin temsilcilerinden meydana gelmelidir. Komisyon, Kurul'un faaliyetlerine oy hakkı olmaksızın katılmalı ve Avrupa Veri Koruma Denetçisinin özel oy kullanma hakları olmalıdır. Kurul, üçüncü ülkelerde veya uluslararası kuruluşlardaki koruma düzeyi konusunda Komisyona tavsiyede bulunma ve Birlik genelinde denetim makamları arasında işbirliğini teşvik etme dâhil, bu Tüzük'ün Birlik genelinde tutarlı bir şekilde uygulanmasına katkıda bulunmalıdır. Kurul, görevlerini yerine getirirken bağımsız hareket etmelidir.

(140) Kurul'a, Avrupa Veri Koruma Denetçisi tarafından sağlanan bir sekretarya yardımcı olmalıdır. Bu Tüzük ile Kurul'a verilen görevlerin yerine getirilmesine dâhil edilen Avrupa Veri Koruma Denetçiliği personeli, görevlerini münhasıran Kurul Başkanı'nın talimatları doğrultusunda yerine getirmeli ve Kurul Başkanı'nın altında olmalıdır.

(141) Her veri öznesinin, bu Tüzük kapsamında yer alan haklarının ihlâl edildiğini değerlendirmesi veya denetim makamının bir şikâyet üzerine harekete geçmemesi, bir şikâyeti kısmen veya tamamen geri çevirmesi veya reddetmesi ya da harekete geçmesi veri öznesinin haklarının korunması için gerekliyken harekete geçmemesi hâlinde, özellikle mutat meskeninin bulunduğu Üye Devlet'te olmak üzere, tek bir denetim makamına şikâyette bulunma ve Şart'ın 47. maddesi uyarınca etkili bir hukuk yoluna başvurma hakkı olmalıdır. Bir şikâyeti müteakip soruşturma, yargı denetimine tabi olarak, münferit olay bakımından uygun olduğu ölçüde yürütülmelidir. Denetim makamı, makul süre içinde, şikâyetin durumu ve sonucu hakkında veri öznesine bilgi vermelidir. Durumun başka bir denetim makamı ile birlikte daha ayrıntılı soruşturma veya koordinasyonu gerektirmesi hâlinde, veri öznesine ara ara bilgi verilmelidir. Her denetim makamı, şikâyette bulunulmasını kolaylaştırmak amacıyla diğer iletişim araçlarını hariç

tutmaksızın, elektronik olarak da doldurulabilecek bir şikâyet formunun sağlanması gibi tedbirler almalıdır.

(142) Veri öznesinin, bu Tüzük kapsamındaki haklarının ihlâl edildiğini değerlendirdiği hâllerde, bir Üye Devlet hukuku uyarınca kurulmuş olan, kamu yararına yasal hedefleri bulunan ve kişisel verilerin korunması alanında aktif olan, kar amacı gütmeyen bir organ, organizasyon veya birliğe, bir denetim makamı nezdinde kendi adına şikâyette bulunma, veri özneleri adına adli yollara başvuru hakkını kullanma veya Üye Devlet hukukunda öngörülmesi hâlinde, veri özneleri adına tazminat alma hakkını kullanma yetkisini verme hakkına sahip olmalıdır. Üye Devlet, böyle bir organ, organizasyon veya birliğe, söz konusu Üye Devlet'te veri öznesinin yetki vermesinden bağımsız olarak şikâyette bulunma hakkı ve kişisel verilerin bu Tüzük'ü ihlâl ederek işlenmesi sonucunda veri öznesinin haklarının ihlâl edilmiş olduğunu değerlendirmesi için gerekçeleri olması durumunda etkili bir hukuk yoluna başvurma hakkı verebilir. Söz konusu organ, organizasyon veya birliğin, veri öznesinin yetki vermesinden bağımsız olarak veri öznesi adına tazminat talep etmesine izin verilemez.

(143)Herhangi bir gerçek veya tüzel kişi, ABİA'nın 263. maddesinde öngörülen koşullar çerçevesinde Kurul kararlarının iptali için Adalet Divanında dava açma hakkına sahiptir. Bu tür kararların muhatapları sıfatıyla, bunlara itiraz etmek isteyen ilgili denetim makamlarının, ABİA'nın 263. maddesi uyarınca, söz konusu kararların kendilerine bildirildiği tarihten itibaren iki ay içinde dava açmaları gerekir. Kurul'un kararları veri sorumlusu, veri işleyen veya şikâyet sahibini doğrudan ve kişisel olarak ilgilendirdiğinde, ABİA'nın 263. maddesi uyarınca, bunlar, söz konusu kararların Kurul'un internet sitesinde yayımlandığı tarihten itibaren iki ay içinde iptal davası açabilir. ABİA'nın 263. maddesinde öngörülen söz konusu hakka halel gelmeksizin, her gerçek veya tüzel kişi için, bir denetim makamının söz konusu kişiyle ilgili hukuki sonuçlar doğuran bir kararına karşı yetkili bir ulusal mahkemede etkili bir hukuk yolu olmalıdır. Böyle bir karar, özellikle denetim makamı tarafından soruşturma, düzeltme ve izin verme yetkilerinin kullanılması veya şikâyetlerin geri çevrilmesi ya da reddedilmesi ile ilgilidir. Ancak, etkili bir hukuk yoluna başvurma hakkı, denetim makamı tarafından bildirilen görüş veya bulunulan tavsiye gibi denetim makamları tarafından alınan ve hukuki bağlayıcılığı bulunmayan tedbirleri kapsamaz. Bir denetim makamına karşı açılacak davalar denetim makamının kurulu olduğu Üye Devlet'in mahkemelerinde açılmalıdır ve söz konusu Üye Devlet'in usul hukuku uyarınca yürütülmelidir. Bu mahkemeler, huzurlarına getirilen uyuşmazlıkla ilgili tüm maddi ve hukuki meselelerin incelenmesine yönelik yargı yetkisi de dâhil, tam yargı yetkisine sahip olmalıdır.

Bir şikâyetin denetim makamı tarafından reddedildiği veya geri çevrildiği durumlarda, şikâyet sahibi aynı Üye Devlet'te bulunan bir mahkemede dava açabilir. Bu Tüzük'ün uygulanması ile ilgili hukuk yolları kapsamında, kendi kararını vermek için konuya ilişkin bir karara gerek duyan ulusal mahkemeler, bu Tüzük dâhil, Birlik hukukunun yorumlanması için Adalet Divanından bir ön karar talebinde bulunabilir veya ABİA'nın 267. maddesinde öngörülen durumda, bulunmalıdır. Ayrıca, bir denetim makamının, Kurul'un bir kararını uygulayan kararına, bir ulusal mahkeme önünde itiraz edildiğinde ve Kurul'un kararının geçerliliği ihtilaf konusu olduğunda, söz konusu ulusal mahkemenin Kurul'un kararını hükümsüz ilan etme yetkisi yoktur fakat kararın hükümsüz olduğunu değerlendirmesi halinde, Adalet Divanı tarafından yorumlandığı şekliyle, ABİA'nın 267. maddesi uyarınca hükümsüzlük hususunda Adalet Divanı'na başvurmalıdır. Ancak ulusal mahkeme, özellikle söz konusu karar kendilerini doğrudan ve kişisel olarak ilgilendiriyorsa, bu kararın iptali için dava açma hakkı bulunan ancak ABİA'nın 263.

maddesinde belirtilen süre içinde dava açmamış olan gerçek veya tüzel kişilerin talebi üzerine, Kurul'un verdiği kararın hükümsüzlüğü hususunda bir başvuruda bulunamaz.

(144) Denetim makamı tarafından alınan bir karara karşı açılan bir davaya bakan mahkemenin, aynı veri sorumlusu veya veri işleyen tarafından gerçekleştirilen bir işleme faaliyeti bakımından aynı konu veya aynı dava sebebi gibi, aynı işleme faaliyetine ilişkin olarak başka bir Üye Devlet'in yetkili mahkemesinde de dava açıldığına inanmak için nedeni varsa, söz konusu ilgili davaların varlığını teyit etmek için bahse konu mahkeme ile iletişime geçmelidir. Başka bir Üye Devlet'te bulunan bir mahkeme önünde, ilişkili bir davanın derdest olması halinde, ilk davaya bakan mahkeme haricindeki bir mahkeme; yargılamayı durdurabilir veya taraflardan birinin talebi üzerine, ilk davaya bakan mahkemenin söz konusu davalara ilişkin yargı yetkisinin bulunması ve hukukunun, bu tür ilişkili davaların birleştirilmesine olanak tanıması halinde, ilk davaya bakan mahkeme lehine yetkisizlik kararı verebilir. Davaların, farklı davalar sonucunda bağdaşmayan kararların verilmesi riskini önlemek amacıyla bir arada görülmesi ve karara bağlanması uygun olacak kadar yakın bağlantılı olmaları halinde, birbirleriyle ilişkili oldukları kabul edilir.

(145) Bir veri sorumlusu veya veri işleyene karşı açılan davalarda davacı, veri sorumlusu bir Üye Devlet'te kamusal yetkilerini kullanan bir kamu makamı olmadığı sürece, davayı veri sorumlusu veya veri işleyenin kuruluşunun bulunduğu Üye Devlet mahkemelerinde mi yoksa veri öznesinin ikamet ettiği Üye Devlet mahkemelerinde mi açacağını seçebilmelidir.

(146) Veri sorumlusu veya veri işleyen, bu Tüzük'ü ihlâl eden işleme faaliyetinin sonucunda kişinin görebileceği zararı tazmin etmelidir. Zarardan hiçbir şekilde sorumlu olmadığını kanıtlaması hâlinde, veri sorumlusu veya veri işleyen, bu yükümlülükten muaf tutulmalıdır. Zarar kavramı, Adalet Divanı içtihadı doğrultusunda, bu Tüzük'ün amaçlarını tam olarak yansıtacak şekilde geniş olarak yorumlanmalıdır. Bu, Birlik veya Üye Devlet hukukunun diğer kurallarının ihlâlinden kaynaklanan herhangi bir tazminat talebine halel getirmez. Bu Tüzük'ü ihlâl eden işleme faaliyeti, bu Tüzük ve bu Tüzük'ün kurallarını detaylandıran Üye Devlet mevzuatı uyarınca kabul edilen yetki devrine dayanan tasarrufları ve uygulama tasarruflarını ihlâl eden işleme faaliyetini de kapsar. Veri özneleri, uğradıkları zarar için tam ve etkili bir tazminat almalıdırlar. Veri sorumluları veya veri işleyenler aynı işleme faaliyetine dâhil olduklarında, her veri sorumlusu veya veri işleyen zararın tamamından sorumlu tutulmalıdır. Bununla birlikte, Üye Devlet hukuku uyarınca, bunların aynı adli süreçlerde birlikte yer almaları durumunda, zarara uğrayan veri öznesine tam ve etkili tazminat verilmesinin sağlanması koşuluyla, işlemenin neden olduğu zarar için her bir veri sorumlusu veya veri işleyenin sorumluluğuna göre tazminat paylaştırılabilir. Tam tazminat ödemiş olan herhangi bir veri sorumlusu veya veri işleyen daha sonra, aynı işlemde yer alan diğer veri sorumluları veya veri işleyenler aleyhine rücu davası açabilir.

(147) Özellikle bir veri sorumlusu veya veri işleyen aleyhine tazminat dâhil olmak üzere bir hukuk yoluna başvuru süreçlerine ilişkin olarak, bu Tüzük'te yargı yetkisine ilişkin özel kuralların yer aldığı durumlarda, (AB) 1215/2012 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü'ndekiler[13] gibi yargı yetkisine ilişkin genel kurallar, bu tür özel kuralların uygulanmasına halel getirmemelidir.

[13] Hukuki ve ticari konularda yargılama ile mahkeme kararlarının tanınması ve tenfizi hakkında 12 Aralık 2012 tarihli ve (AB) 1215/2012 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ABRG L 351, 20.12.2012, s. 1).

(148) Bu Tüzük kurallarının uygulanmasını güçlendirmek için, bu Tüzük'ün herhangi bir şekilde ihlal edilmesi durumunda, bu Tüzük uyarınca denetim makamı tarafından alınan uygun tedbirlere ek olarak veya bunların yerine, idari para cezalarını da içeren cezalar verilmelidir. Hafif bir ihlâl durumunda veya verilmesi muhtemel para cezası bir gerçek kişiye orantısız bir yük teşkil edecekse, para cezası yerine kınama cezası verilebilir. Bununla birlikte, ihlâlin niteliği, ağırlığı ve süresi, ihlalin kasıt niteliği, uğranan zararı hafifletmek için yapılan işlemler, sorumluluğun derecesi veya daha önceki ilgili ihlâller, denetim makamının ihlâlden haberdar olma şekli, veri sorumlusu veya veri işleyene karşı alınan tedbirlere uyum, davranış kurallarına uyum ve diğer ağırlaştırıcı veya hafifletici etkenler dikkate alınmalıdır. İdari para cezaları dâhil olmak üzere ceza verilmesi, etkili yargısal koruma ve yargı süreci dâhil olmak üzere, Birlik hukukunun genel ilkeleri ve Şart uyarınca uygun usul güvencelerine tabi olmalıdır.

(149) Üye Devletler, bu Tüzük uyarınca ve bu Tüzük'ün sınırları dâhilinde kabul edilen ulusal kuralların ihlâlleri de dâhil olmak üzere, bu Tüzük'ün ihlâlleri ile ilgili cezalara ilişkin kuralları belirleyebilmelidirler. Bu cezalar, bu Tüzük'ün ihlâli yoluyla elde edilen kazançlardan mahrum bırakılmayı da mümkün kılabilir. Bununla birlikte, idari cezalar ve bu tür ulusal kuralların ihlâli nedeniyle adli cezalar verilmesi, Adalet Divanı tarafından yorumlandığı şekilde, *aynı suçtan dolayı iki kez yargılanmama* ilkesinin ihlâline yol açmamalıdır.

(150) Bu Tüzük'ün ihlâli hâlinde uygulanacak idari cezaları güçlendirmek ve uyumlaştırmak üzere her denetim makamının idari para cezası verme yetkisi olmalıdır. Bu Tüzük, özellikle ihlâlin ve sonuçlarının niteliği, ağırlığı ve süresi ile bu Tüzük kapsamındaki yükümlülüklere uyumu sağlamak ve ihlâlin sonuçlarını önlemek veya hafifletmek için alınan tedbirlere uygun olarak, özel durumun ilgili tüm koşulları göz önünde bulundurulmak suretiyle, ihlalleri ve her münferit olayda yetkili denetim makamı tarafından belirlenmesi gereken ilgili idari para cezalarını belirlemeye yönelik üst limit ile kriterleri öngörmelidir. Bir teşebbüse idari para cezası verilmesi halinde teşebbüsün, ABİA'nın 101 ve 102. maddeleri uyarınca, bu amaçlar doğrultusundaki bir teşebbüs olarak anlaşıldığı kabul edilmelidir. Bir teşebbüs olmayan kişilere idari para cezası verilmesi halinde denetim makamı, uygun para cezası miktarını değerlendirirken, o Üye Devlet'teki genel gelir düzeyini ve kişinin ekonomik durumunu dikkate almalıdır. Tutarlılık mekanizması, idari para cezalarının tutarlı bir şekilde uygulanmasını teşvik etmek için de kullanılabilir. Kamu makamlarının idari para cezalarına tabi olup olmayacaklarına ve ne ölçüde tabi olacaklarına Üye Devletler karar vermelidirler. İdari para cezası veya uyarı verilmesi, bu Tüzük kapsamında denetim makamlarının diğer yetkilerinin veya diğer cezaların uygulanmasını etkilemez.

(151) Danimarka ve Estonya'nın hukuk sistemleri, bu Tüzük'te belirtilen idari para cezalarına izin vermez. İdari para cezalarına ilişkin kurallar, Danimarka ve Estonya'daki uygulamaların, denetim makamları tarafından verilen idari para cezalarına eşdeğer bir etkiye sahip olması şartıyla, para cezasının Danimarka'da yetkili ulusal mahkemeler tarafından adli ceza olarak ve Estonya'da denetim makamı tarafından bir kabahat usulü çerçevesinde kesilmesi suretiyle uygulanması şeklinde gerçekleştirilebilir. Bu nedenle yetkili ulusal mahkemeler, para cezası için girişimde bulunan denetim makamının tavsiyesini dikkate almalıdır. Her halükarda, verilen para cezaları etkili, orantılı ve caydırıcı olmalıdır.

(152) Bu Tüzük'ün idari cezaları uyumlaştırmaması halinde veya ihtiyaç duyulan diğer hallerde, örneğin bu Tüzük'ün ağır ihlâlleri halinde, Üye Devletler etkili, orantılı ve

caydırıcı cezalar öngören bir sistem uygulamalıdırlar. Adli veya idari, söz konusu cezaların niteliği, Üye Devlet hukukuna göre belirlenmelidir.

(153) Üye Devletlerin mevzuatları bu Tüzük uyarınca, gazetecilikle ilgili, akademik, sanatsal ve/veya edebi ifadeler de dâhil olmak üzere, ifade ve bilgi edinme özgürlüğünü düzenleyen kurallar ile kişisel verilerin korunması hakkını birbiriyle bağdaştırmalıdırlar. Kişisel verilerin sadece gazetecilik amaçlarıyla veya akademik, sanatsal veya edebi ifade maksatlarıyla işlenmesi hakkında, kişisel verilerin korunması hakkı ile Şart'ın 11. maddesi kapsamında yer verilen ifade özgürlüğü hakkının ve özellikle de bilgi edinme ve açıklama haklarının birbiriyle bağdaştırılması bakımından gerekmesi halinde, bu Tüzük'ün belirli hükümlerinden derogasyon veya istisna sağlanmalıdır. Bu durum, özellikle kişisel verilerin görsel-işitsel alanda ve haber arşivlerinde ve basın kütüphanelerinde işlenmesi için geçerli olmalıdır. Bu nedenle Üye Devletler, bu temel hakların dengelenmesi amacıyla gerekli olan istisnaları ve derogasyonları ortaya koyan yasama tedbirlerini kabul etmelidirler. Üye Devletler; genel ilkeler, veri öznesinin hakları, veri sorumlusu ve veri işleyen, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması, bağımsız denetim makamları, işbirliği ve tutarlılık ve özel veri işleme durumlarına ilişkin olarak bu tür istisnalar ve derogasyonlar kabul etmelidirler. Bu tür istisnaların veya derogasyonların Üye Devletler arasında farklılık göstermesi halinde, veri sorumlusunun tabi olduğu Üye Devlet'in mevzuatı uygulanmalıdır. Her demokratik toplumda ifade özgürlüğü hakkının önemini dikkate almak için, gazetecilik gibi, bu özgürlüğe ilişkin kavramları geniş anlamda yorumlamak gerekir.

(154) Bu Tüzük, uygulanmasında resmi belgelere kamu erişimi ilkesinin de göz önünde tutulmasına imkân tanır. Kamunun resmi belgelere erişiminin kamu yararına olduğu düşünülebilir. Bir kamu makamı veya organı tarafından tutulan belgelerdeki kişisel veriler, Birlik hukukunda veya söz konusu kamu makamı veya organının tabi olduğu Üye Devlet hukukunda açıklanmalarının öngörülmesi durumunda, bu makam veya organ tarafından kamuya açıklanabilmelidir. Söz konusu mevzuat, resmi belgelere kamu erişimi ile kamu sektörü bilgilerinin yeniden kullanılmasını, kişisel verilerin korunması hakkı ile bağdaştırmalıdır ve böylelikle, bu Tüzük uyarınca kişisel verilerin korunması hakkı ile gerekli bağdaştırmayı öngörebilmelidir. Kamu makamları ve organlarına yapılan atıf, söz konusu bağlamda, belgelere kamu erişimiyle ilgili Üye Devlet mevzuatı kapsamında yer alan tüm makamları veya diğer organları kapsamalıdır. 2003/98/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi[14], kişisel verilerin işlenmesi bakımından gerçek kişilerin Birlik ve Üye Devlet hukuku hükümleri uyarınca korunma düzeyine dokunmaz ve bu düzeyi hiçbir şekilde etkilemez ve özellikle bu Tüzük'te belirtilen yükümlülükleri ve hakları değiştirmez. Özellikle söz konusu Direktif, kişisel verilerin korunması gerekçesiyle erişim rejimleri vasıtasıyla erişimin olmadığı veya kısıtlandığı belgelere ve belgelerin, tekrar kullanımlarının kişisel verilerin işlenmesi bakımından gerçek kişilerin korunmasına ilişkin mevzuata aykırı olduğu mevzuatla öngörülmüş kişisel verileri içeren ve söz konusu rejimler aracılığıyla erişilebilen kısımlarına uygulanmamalıdır.

(155) Üye Devlet hukuku veya "iş akitleri" de dahil olmak üzere toplu sözleşmeler; kişisel verilerin istihdam bağlamında çalışanın rızasına dayanılarak işlenebileceği koşullara; işe alım, mevzuatla ya da toplu sözleşme yoluyla belirtilen yükümlülüklerin sona ermesi de dâhil olmak üzere iş sözleşmesinin ifası, işin yönetimi, planlanması ve düzenlenmesi, iş yerinde eşitlik ve çeşitlilik, iş sağlığı ve güvenliği amaçları; istihdam ile ilgili olarak bireysel ya da toplu şekilde haklar ve menfaatlerin öne sürülmesi ve bunlardan

[14] Kamu sektöründeki bilgilerin tekrar kullanılması hakkında 17 Kasım 2003 tarihli ve 2003/98/AT sayılı Direktif (ABRG L 345, 31.12.2003, s. 90).

yararlanılması amaçları ve iş ilişkisinin sona erdirilmesi amacı doğrultusunda işlenmesine ilişkin kurallar başta olmak üzere, çalışanların kişisel verilerinin istihdam bağlamında işlenmesine ilişkin olarak spesifik kurallar öngörebilir.

(156) Kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla kişisel verilerin işlenmesi faaliyeti, bu Tüzük uyarınca veri öznesinin hakları ve özgürlükleri açısından uygun güvencelere tabi olmalıdır. Bu güvenceler ile özellikle veri minimizasyonu ilkesine uygun hareket edilmesinin sağlanması amacıyla teknik ve kurumsal tedbirlerin uygulamaya konulması sağlanmalıdır. Kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla kişisel verilerin daha fazla işlenmesi, uygun güvencelerin mevcut olması koşuluyla (örneğin, verilerde takma ad kullanılması), veri sorumlusunun, veri öznesinin kimliğinin belirlenmesine izin vermeyen veya artık izin vermeyen verileri işleyerek söz konusu amaçlara ulaşılıp ulaşılamayacağını değerlendirmiş olması halinde gerçekleştirilir. Üye Devletler, kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla kişisel verilerin işlenmesi faaliyeti için uygun güvenceler öngörmelidirler. Üye Devletlerin, belirli koşullar altında ve veri öznelerine yönelik uygun güvencelere tabi olarak, bilgi gerekliliklerivle ve düzeltme, kalıcı olarak silme, unutulma, işlemeyi kısıtlama, veri taşınabilirliği ve kişisel veriler kamu yararına arşivleme, bilimsel veya tarihsel araştırma veya istatistiki amaçlarla işlenirken itiraz etme haklarıyla ilgili olarak koşullar ve derogasyonlar öngörmesine izin verilmelidir. Söz konusu koşullar ve güvenceler, orantılılık ve gereklilik ilkeleri uyarınca, kişisel verilerin işlenmesini en aza indirmeyi amaçlayan teknik ve kurumsal tedbirlerin yanı sıra, spesifik işlemenin amaçları ışığında uygun olduğu takdirde, veri öznelerinin bu hakları kullanmaları için özel usulleri gerektirebilir. Kişisel verilerin bilimsel amaçlarla işlenmesi, klinik araştırmalar hakkındaki gibi diğer ilgili mevzuat ile de uyumlu olmalıdır.

(157) Araştırmacılar, kayıtlardan alınan bilgileri birleştirerek, kalp damar hastalıkları, kanser ve depresyon gibi yaygın tıbbi durumlarla ilgili çok değerli yeni bilgiler elde edebilirler. Kayıtlar daha geniş bir nüfus kitlesine dayalı olduğundan, araştırma sonuçları kayıtlardan yararlanılarak geliştirilebilir. Sosyal bilimlerde kayıtlara dayanılarak yapılan araştırma, araştırmacıların, işsizlik ve eğitim gibi bir dizi sosyal koşulun diğer yaşam koşullarıyla uzun vadeli ilişkisi hakkında temel bilgileri elde etmelerini sağlar. Kayıtlar aracılığıyla elde edilen araştırma sonuçları, bilgiye dayalı politikanın oluşturulması ve uygulanması için temel teşkil edebilecek güvenilir, yüksek kaliteli bilgi sağlar, birçok kişi için yaşam kalitesini iyileştirir ve sosyal hizmetlerin etkinliğini artırır. Bilimsel araştırmayı kolaylaştırmak için kişisel veriler, Birlik veya Üye Devlet mevzuatında belirtilen uygun şartlara ve güvencelere tabi olmak şartıyla, bilimsel araştırma amaçları doğrultusunda işlenebilir.

(158) Bu Tüzük'ün vefat etmiş kişilere uygulanmaması gerektiği akılda tutularak, kişisel verilerin arşivleme amaçları doğrultusunda işlenmesi halinde, bu Tüzük söz konusu işleme için de geçerli olmalıdır. Kamu yararına ilişkin kayıtları tutan kamu makamları ile kamu organları veya özel organlar, Birlik veya Üye Devlet mevzuatına göre, genel kamu yararı için değeri olan kayıtları edinme, koruma, değerlendirme, düzenleme, betimleme, iletme, tanıtma, yayma ve bu kayıtlara erişim sağlamaya yönelik yasal yükümlülüğü olan birimler olmalıdır. Üye Devletlerin ayrıca, örneğin eski totaliter devlet rejimleri sırasındaki siyasi davranışlar, soykırım, Holokost başta olmak üzere insanlığa karşı işlenen suçlar veya savaş suçları ile ilgili özel bilgilerin sağlanması bakımından, arşivleme amaçları doğrultusunda kişisel verilerin daha fazla işlenmesini öngörmelerine izin verilmelidir.

(159) Kişisel verilerin bilimsel araştırma amaçları doğrultusunda işlenmesi halinde, bu Tüzük söz konusu işleme için de uygulanmalıdır. Bu Tüzük'ün amaçları doğrultusunda, kişisel verilerin bilimsel araştırma amaçlarıyla işlenmesi, örneğin teknolojik gelişme ve gösteri, temel araştırma, uygulamalı araştırma ve özel olarak finanse edilen araştırma dâhil olmak üzere geniş bir şekilde yorumlanmalıdır. Buna ilave olarak, söz konusu işlemede, ABİA'nın 179(1) maddesi kapsamında yer alan Birlik'in bir Avrupa Araştırma Alanı oluşturma hedefi de dikkate alınmalıdır. Bilimsel araştırma amaçları, halk sağlığı alanında kamu yararına yapılan çalışmaları da içermelidir. Kişisel verilerin bilimsel araştırma amaçları doğrultusunda işlenmesinin belirliliğini sağlamak için, kişisel verilerin özellikle bilimsel araştırma amaçları bağlamında yayımlanması veya başka bir şekilde açıklanması bakımından özel koşullar uygulanmalıdır. Özellikle sağlık bağlamında olmak üzere, bilimsel araştırmanın sonucu, veri öznesinin yararına olacak ilave tedbirlerin alınması için gerekçe oluşturuyorsa, bu tedbirler bakımından bu Tüzük'ün genel kuralları uygulanmalıdır.

(160) Kişisel verilerin tarihi araştırma amaçları doğrultusunda işlenmesi halinde, bu Tüzük söz konusu işleme için de uygulanmalıdır. Bu işleme, bu Tüzük'ün vefat etmiş kişilere uygulanmaması gerektiği akılda tutularak, tarihi araştırma ve kalıtımsal amaçlar doğrultusunda yapılan araştırmaları da içermelidir.

(161) Klinik araştırmalarda bilimsel araştırma faaliyetlerine katılıma rıza verilmesi amacı doğrultusunda, (AB) 536/2014 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü'nün[15] ilgili hükümleri uygulanmalıdır.

(162) Kişisel verilerin istatistiki amaçlarla işlenmesi halinde, bu Tüzük hükümleri söz konusu işleme için uygulanmalıdır. Birlik veya Üye Devlet mevzuatı, bu Tüzük'ün sınırları dâhilinde, istatistiki içeriği, erişimin kontrolünü, kişisel verilerin istatistiki amaçlarla işlenmesine yönelik koşulları ve veri öznesinin hak ve özgürlüklerini güvence altına almak ve istatistiki gizliliği sağlamak amacıyla uygun tedbirleri belirlemelidir. İstatistiki amaçlar, istatistiki anketler veya istatistiki sonuçların üretimi için gerekli olan kişisel verilerin toplanması ve işlenmesine yönelik her türlü işlemdir. Bu istatistiki sonuçlar, bilimsel bir araştırma amacı dâhil olmak üzere, farklı amaçlar için de kullanılabilir. İstatistiki amaç, istatistiki amaçlarla işlemeden elde edilen sonucun kişisel veri değil, toplulaştırılmış veril olduğuna ve bu sonucun veya kişisel verilerin belirli bir gerçek kişiye ilişkin tedbirleri veya kararları desteklemek için kullanılmadığına işaret eder.

(163) Birlik ve ulusal istatistik makamları tarafından resmi Avrupa istatistiklerinin ve resmi ulusal istatistiklerin üretimi için toplanan gizli bilgiler korunmalıdır. Avrupa istatistiklerinin, ABİA'nın 338(2) maddesinde belirtilen istatistiki ilkelere uygun olarak geliştirilmesi, üretilmesi ve yayılması, ulusal istatistiklerin de Üye Devlet mevzuatına uygun olması gerekir. (AT) 223/2009 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü'nde[16], Avrupa istatistiklerine yönelik istatistiki gizlilik hakkında daha fazla açıklama öngörülmüştür.

---

[15] 2001/20/AT sayılı Direktif'i yürürlükten kaldıran ve beşeri tıbbi ürünler üzerindeki klinik denemeler hakkında 16 Nisan 2014 tarihli ve (AB) 536/2014 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ABRG L 158, 27.5.2014, s. 1).

[16] İstatistiki gizliliğe tabi verilerin Avrupa Toplulukları İstatistik Ofisine iletilmesi hakkında (AT, Euratom) 1101/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü'nü, Topluluk İstatistikleri hakkında (AT) 322/97 sayılı Konsey Tüzüğü'nü ve Avrupa Toplulukları İstatistik Programları Komitesini tesis eden 89/382/AET, Euratom sayılı Konsey Kararı'nı değiştiren ve Avrupa istatistikleri hakkında 11 Mart 2009 tarihli ve (AT) 223/2009 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ABRG L 87, 31.3.2009, s. 164).

(164) Denetim makamlarının, veri sorumlusu veya veri işleyenden, kişisel verilere erişim veya tesislere erişim elde etmelerine ilişkin yetkileriyle ilgili olarak Üye Devletler, bu Tüzük'ün sınırları dâhilinde, kişisel verilerin korunması hakkının mesleki sır saklama yükümlülüğüyle bağdaştırılması için gerektiği ölçüde, mesleki veya dengi diğer sır saklama yükümlülüklerini güvence altına almak amacıyla mevzuatla özel kurallar kabul edebilirler. Bu durum, Üye Devletlerin, Birlik hukukunun gerektirdiği durumlarda mesleki sır saklama ile ilgili kuralları kabul etme yönünde mevcut olan yükümlülüklerine halel getirmez.

(165) Bu Tüzük, ABİA'nın 17. maddesinde tanındığı şekilde, Üye Devletlerdeki kiliselerin ve dini birliklerin veya toplulukların mevcut anayasal hukuk çerçevesindeki statülerine saygı gösterir ve halel getirmez.

(166) Bu Tüzük'ün hedeflerinin gerçekleştirilmesi amacıyla, diğer bir deyişle, gerçek kişilerin temel hak ve özgürlüklerinin ve özellikle bunların kişisel verilerinin korunması hakkının korunması ve kişisel verilerin Birlik içinde serbest dolaşımının sağlanması için, ABİA'nın 290. maddesi uyarınca tasarruflar kabul etme yetkisi Komisyona devredilmelidir. Özellikle, belgelendirme mekanizmalarına ilişkin kriterler ve gereklilikler, standartlaştırılmış simgelerle sunulacak bilgiler ve bu tür simgelerin sağlanmasına yönelik usuller açısından yetki devrine dayanan tasarruflar kabul edilmelidir. Komisyonun, hazırlık çalışmaları sırasında, uzman seviyesindekiler de dâhil olmak üzere, uygun istişarelerde bulunması özellikle önemlidir. Komisyon, yetki devrine dayanan tasarrufları hazırlarken ve düzenlerken, ilgili belgelerin Avrupa Parlamentosuna ve Konseye eşzamanlı olarak, gecikmeden ve uygun bir şekilde iletilmesini sağlamalıdır.

(167) Bu Tüzük'ün uygulanmasına yönelik olarak yeknesak koşulların sağlanması amacıyla, bu Tüzük'te öngörülmesi halinde Komisyona uygulama yetkileri tanınmalıdır. Bu yetkiler, (AB) 182/2011 sayılı Tüzük'e uygun olarak kullanılmalıdır. Söz konusu bağlamda Komisyon, mikro, küçük ve orta ölçekli işletmelere yönelik özel tedbirleri değerlendirmelidir.

(168) İnceleme prosedürü, veri sorumluları ve veri işleyenler arasındaki ve veri işleyenlerin aralarındaki standart sözleşme hükümlerine ilişkin uygulama tasarruflarının; davranış kurallarının; belgelendirmeye ilişkin teknik standartların ve mekanizmaların; bir üçüncü ülke, üçüncü ülke içindeki bir bölge veya belirli bir sektör ya da bir uluslararası kuruluş tarafından sağlanan yeterli koruma düzeyinin; standart koruma hükümlerinin; bağlayıcı şirket kuralları için veri sorumluları, veri işleyenler ve denetim makamları arasında elektronik yollarla bilgi alışverişine ilişkin formatların ve usullerin; karşılıklı yardımın ve denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin düzenlemelerin kabul edilmesi için kullanılmalıdır.

(169) Komisyon, mevcut kanıtlarla, bir üçüncü ülke, üçüncü ülke içindeki bir bölge veya belirli bir sektörün ya da bir uluslararası kuruluşun uygun koruma düzeyini temin etmediğinin ortaya çıkması halinde ve aciliyet açısından gerekmesi hâlinde tatbik edilecek uygulama tasarruflarını gecikmesizin kabul etmelidir.

(170) Bu Tüzük'ün, Birlik içinde gerçek kişilerin ve kişisel verilerin serbest akışının eşdeğer düzeyde korunmasını sağlamak olan hedefine, Üye Devletler tarafından yeterli düzeyde ulaşılamayacağından ve bahse konu eylemin ölçek veya etkileri dikkate alınarak bu hedefe Birlik düzeyinde daha iyi şekilde ulaşılabilecek olması gerekçesiyle Birlik, Avrupa Birliği Antlaşması'nın (ABA) 5. maddesinde belirtilen katmanlı yetki ilkesine uygun olarak tedbirler kabul edebilir. Söz konusu maddede belirtilen orantılılık ilkesi uyarınca, bu Tüzük, söz konusu hedefe ulaşmak için gerekli olanın ötesine geçmez.

(171) 95/46/AT sayılı Direktif bu Tüzük ile yürürlükten kaldırılmalıdır. Bu Tüzük'ün uygulanma tarihinde hâlihazırda devam etmekte olan işleme faaliyetleri, bu Tüzük'ün yürürlüğe girdiği tarihten itibaren iki yıl içinde bu Tüzük'e uygun hale getirilmelidir. İşlemenin 95/46/AT sayılı Direktif uyarınca rızaya dayalı olarak gerçekleştirildiği hâllerde, veri sorumlusunun bu Tüzük'ün uygulama tarihten sonra bu tür işleme faaliyetine devam etmesine izin vermek amacıyla, rızanın verilme şekli bu Tüzük şartlarına uygun ise, veri öznesinin rızasının tekrar alınması gerekmez. 95/46/AT sayılı Direktif'e dayanılarak kabul edilen Komisyon kararları ve denetim makamları tarafından verilen izinler, değiştirilmediği, yenilenmediği veya yürürlükten kaldırılmadığı sürece yürürlükte kalmaya devam eder.

(172) (AT) 45/2001 sayılı Tüzük'ün 28(2) maddesi uyarınca Avrupa Veri Koruma Denetçisine danışılmış ve 7 Mart 2012 tarihinde görüşü[17] alınmıştır .

(173) Bu Tüzük, veri sorumlusunun yükümlülükleri ve gerçek kişilerin hakları da dâhil olmak üzere 2002/58/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde belirtilen hedefe yönelik spesifik yükümlülüklere konu olmayan kişisel veri işleme karşısında temel hak ve özgürlüklerin korunmasıyla ilgili tüm meselelere uygulanmalıdır. Bu Tüzük ile 2002/58/AT sayılı Direktif[18] arasındaki ilişkiyi açıklığa kavuşturmak için, söz konusu Direktif'te bu doğrultuda değişiklik yapılmalıdır. Bu Tüzük kabul edildikten sonra, 2002/58/AT sayılı Direktif özellikle bu Tüzük ile tutarlılığı sağlamak amacıyla gözden geçirilmelidir.

İŞBU TÜZÜK'Ü KABUL ETMİŞTİR:

BÖLÜM I

Genel Hükümler

Madde 1

Konu ve amaçlar

1. Bu Tüzük gerçek kişilerin, kişisel verilerin işlenmesiyle ilgili olarak korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kuralları belirler.

2. Bu Tüzük, gerçek kişilerin temel hak ve özgürlükleri ile özellikle, kişisel verilerin korunmasına ilişkin haklarını korur.

3. Kişisel verilerin Birlik içinde serbest dolaşımı, kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ile bağlantılı sebeplerle kısıtlanmaz ve yasaklanmaz.

Madde 2

Maddi kapsam

[17] ABRG C 192, 30.6.2012, s.7.

[18] Elektronik iletişim sektöründe kişisel verilerin işlenmesi ve özel hayatın korunmasına ilişkin 12 Temmuz 2002 tarihli ve 2002/58/AT sayılı Direktif (Özel hayatın gizliliği ve elektronik iletişim Direktifi) (ATRG L 201, 31.7.2002, s.37).

1. Bu Tüzük, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan kişisel verilerin otomatik yollar haricinde işlenmesine uygulanır.

2. Bu Tüzük:

(a) Birlik hukuku kapsamına girmeyen bir faaliyet esnasında;

(b) ABA'nın V. Başlığının 2. Bölümü kapsamına giren faaliyetler gerçekleştirilirken Üye Devletler tarafından;

(c) tamamen kişisel veya hane içi bir faaliyet esnasında bir gerçek kişi tarafından;

(d) kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi amacıyla yetkili makamlar tarafından kişisel verilerin işlenmesine uygulanmaz.

3. Kişisel verilerin, Birlik kurumları, organları, ofisleri ve ajansları tarafından işlenmesi için (AT) 45/2001 sayılı Tüzük uygulanır. (AT) 45/2001 sayılı Tüzük ve kişisel verilerin bu şekilde işlenmesine uygulanan Birlik'in diğer hukuki tasarrufları, 98. madde uyarınca bu Tüzük'te yer alan ilke ve kurallara uyarlanır.

4. Bu Tüzük, 2000/31/AT sayılı Direktif'in uygulanmasına ve aynı Direktif'in özellikle aracı hizmet sağlayıcıların yükümlülüklerine ilişkin 12 ilâ 15. maddelerinde yer alan kurallara halel getirmez.

Madde 3

Bölgesel kapsam

1. Bu Tüzük, işlemenin Birlik içinde gerçekleşip gerçekleşmediğine bakılmaksızın, kişisel verilerin, Birlik içindeki bir veri sorumlusunun veya veri işleyenin kuruluşunun faaliyetleri bağlamında işlenmesine uygulanır.

2. Bu Tüzük, işleme faaliyetlerinin aşağıdaki hususlarla ilgili olması halinde, Birlik içinde bulunan veri öznelerinin kişisel verilerinin Birlik içinde kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesine uygulanır:

(a) veri öznesinin ödeme yapmasına gerek olup olmadığına bakılmaksızın, Birlik içindeki söz konusu veri öznelerine mal veya hizmetlerin sunulması veya

(b) Davranışları Birlik içinde gerçekleştiği ölçüde, davranışlarının izlenmesi.

3. Bu Tüzük kişisel verilerin, Birlik içinde kurulu bulunmayan, ancak Üye Devlet hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde bir veri sorumlusu tarafından işlenmesine uygulanır.

Madde 4

Tanımlar

Bu Tüzük'ün amaçları doğrultusunda:

(1) "kişisel veri" kimliği belirlenmiş veya belirlenebilir bir gerçek kişiye (“veri öznesi”) ilişkin her türlü bilgidir; kimliği belirlenebilir bir gerçek kişi, özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı gibi bir tanımlayıcıya ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak belirlenmiş bir kişidir.

(2) "işleme" otomatik yollarla olsun veya olmasın, kişisel veriler veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri getirme, danışma, kullanma, iletim yoluyla açıklama, yayma veya bir başka şekilde kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, kalıcı olarak silme veya yok etme gibi herhangi bir işlem veya işlem setidir.

(3) "işlemenin kısıtlanması" depolanan kişisel verilerin gelecekte işlenmelerinin sınırlanması amacıyla işaretlenmesidir.

(4) "profilleme" kişisel verilerin, bir gerçek kişiyle ilgili bazı kişisel özellikleri değerlendirmek, özellikle söz konusu gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususları analiz etmek veya tahmin etmek amacıyla kişisel verilerin kullanılmasını içeren her türlü otomatik işlenmesi biçimidir.

(5) "takma ad kullanımı" ek bilgilerin ayrı tutulması ve kişisel verilerin kimliği belirlenmiş veya belirlenebilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacıyla teknik ve düzenlemeye ilişkin tedbirlere tabi olması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın belirli bir veri öznesiyle artık ilişkilendirilemeyecek şekilde işlenmesidir.

(6) "dosyalama sistemi" işlevsel veya coğrafi bir temelde, merkezi, merkezi olmayan veya dağınık olmasına bakılmaksızın, belirli kriterlere göre erişilebilen yapılandırılmış kişisel veri setidir.

(7) "veri sorumlusu" yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve yollarını belirleyen gerçek veya tüzel kişi, kamu makamı, kamu kurumu veya diğer organlardır; söz konusu işlemenin amaçları ve yollarının Birlik ya da Üye Devlet hukukuna göre belirlenmesi halinde, veri sorumlusu veya veri sorumlusunun tayinine özgü kriterler Birlik ya da Üye Devlet hukukuna göre öngörülebilir.

(8) "veri işleyen" veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu makamı, kamu kurumu veya diğer organlardır.

(9) "alıcı" üçüncü kişi olsun veya olmasın, kişisel verilerin açıklandığı gerçek ya da tüzel kişi, kamu makamı, kamu kurumu veya diğer organlardır. Ancak kişisel verileri, Birlik veya Üye Devlet hukuku uyarınca belirli bir sorgulama çerçevesinde alabilen kamu makamları alıcı olarak nitelendirilmez; bu verilerin söz konusu kamu makamları tarafından işlenmesi, işleme amaçlarına göre geçerli veri koruma kurallarına uygun olarak yapılır.

(10) "üçüncü kişi" veri öznesi, veri sorumlusu, veri işleyen ve veri sorumlusu ya da veri işleyenin doğrudan otoritesi altında, kişisel verileri işleme yetkisi bulunan kişiler haricindeki bir gerçek veya tüzel kişi, kamu makamı, kamu kuruluşu veya organıdır.

(11) veri öznesinin "rızası" veri öznesinin, bir beyanla ya da açık bir onay eylemiyle kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini belirttiği, özgür bir şekilde, spesifik, bilinçli ve açıkça ifade edilen istekleridir.

(12) "kişisel veri ihlâli" iletilen, depolanan veya başka bir şekilde işlenen kişisel verilerin kazara veya hukuk dışı yollarla yok edilmesi, kaybı, değiştirilmesi, izinsiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlâlidir.

(13) "genetik veri" bir gerçek kişinin fizyoloji veya sağlığı ile ilgili benzersiz bilgiler sağlayan ve özellikle, söz konusu gerçek kişiden alınan bir biyolojik numunenin analizi ile ortaya çıkan, gerçek kişinin kalıtsal veya edinilmiş genetik özellikleri ile ilgili kişisel verilerdir.

(14) "biyometrik veri" yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin kimliğinin benzersiz şekilde belirlenmesini sağlayan veya bunu teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak belirli teknik işleme ile ortaya çıkan kişisel verilerdir.

(15) "sağlık verileri" sağlık hizmetlerinin sağlanması da dâhil olmak üzere, bir gerçek kişinin sağlık durumuyla ilgili bilgileri açığa çıkaran, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel verilerdir.

(16) "ana kuruluş":

(a) birden fazla Üye Devlet'te kuruluşu bulunan bir veri sorumlusu ile ilgili olarak, kişisel verilerin işlenmesine ilişkin amaçlar ve yollara yönelik kararların veri sorumlusunun Birlik içindeki diğer bir kuruluşunda alınmaması ve bu diğer kuruluşun söz konusu kararları uygulatma yetkisinin bulunmaması durumunda, ki bunların gerçekleşmesi hâlinde, söz konusu kararları alan kuruluş asıl kuruluş olarak kabul edilir, Birlik içindeki merkezi idare yeridir.

(b) birden fazla Üye Devlet'te kuruluşu bulunan bir veri işleyen ile ilgili olarak, Birlik içindeki merkezi idare yeridir veya veri işleyenin Birlik içinde merkezi bir idare yerinin bulunmaması hâlinde, veri işleyenin kuruluşunun faaliyetleri bağlamındaki temel işleme faaliyetlerinin, veri işleyenin bu Tüzük kapsamındaki belirli yükümlülüklere tabi olduğu ölçüde gerçekleştiği Birlik içindeki kuruluşudur.

(17) "temsilci" 27. madde uyarınca veri sorumlusu veya veri işleyen tarafından yazılı olarak belirlenen, bu Tüzük kapsamındaki yükümlülükleri bakımından veri sorumlusu veya veri işleyeni temsil eden ve Birlik içinde kurulmuş olan, gerçek veya tüzel kişidir.

(18) "işletme" düzenli olarak bir ekonomik faaliyetle iştigal eden ortaklıklar veya birlikler de dâhil olmak üzere, hukuki biçimine bakılmaksızın, bir ekonomik faaliyetle iştigal eden gerçek veya tüzel kişidir.

(19) "teşebbüsler grubu" bir idare eden teşebbüs ve onun idare ettiği teşebbüsleridir.

(20) "bağlayıcı şirket kuralları" teşebbüsler grubu veya ortak bir ekonomik faaliyette bulunan işletmeler grubu içinde bir veya daha fazla sayıda üçüncü ülkedeki bir veri sorumlusuna veya veri işleyene kişisel veri aktarımları veya aktarım setiyle ilgili olarak, Üye Devletlerden birinin topraklarında kurulmuş olan bir veri sorumlusu veya veri işleyen tarafından uyulan kişisel veri koruma politikalarıdır.

(21) "denetim makamı" 51. madde uyarınca bir Üye Devlet tarafından kurulan bağımsız bir kamu makamıdır.

(22) "ilgili denetim makamı" aşağıdaki sebeplerden dolayı kişisel verilerin işlenmesiyle ilgili olan bir denetim makamıdır:

(a) veri sorumlusu veya veri işleyenin, söz konusu denetim makamının bulunduğu Üye Devleti'in topraklarında kurulmuş olması;

(b) söz konusu denetim makamının bulunduğu Üye Devlet'te ikamet eden veri öznelerinin işlemeden kayda değer biçimde etkilenmesi veya kayda değer biçimde etkilenme ihtimalinin bulunması veya

(c) söz konusu denetim makamına bir şikâyette bulunulması;

(23) "sınır ötesi işleme":

(a) veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te kurulu olması hâlinde, kişisel verilerin, söz konusu veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te bulunan kuruluşlarının faaliyetleri bağlamında işlenmesidir veya

(b) bir veri sorumlusu veya veri işleyenin Birlik içinde bulunan tek bir kuruluşunun faaliyetleri bağlamında gerçekleşen, ancak birden fazla Üye Devlet'teki veri öznelerini kayda değer ölçüde etkileyen veya kayda değer ölçüde etkileme ihtimali bulunan kişisel veri işlemesidir.

(24) "yerinde ve gerekçeli itiraz" bir taslak karar açısından bu Tüzük ile ilgili bir ihlâl olup olmadığına veya veri sorumlusu veya veri işleyen ile ilgili olarak öngörülen eylemin bu Tüzük'e uygun olup olmadığına yönelik olarak yapılan ve taslak kararın veri öznelerinin temel hakları ve özgürlükleri ve uygun olduğu hâllerde, kişisel verilerin Birlik içinde akışı açısından teşkil ettiği risklerin önemini açık bir şekilde gösteren itirazdır.

(25) "bilgi toplumu hizmeti" (AB) 2015/1535 sayılı Avrupa Parlamentosu ve Konsey Direktifi'nin[19] 1(1) maddesinin (b) bendinde tanımlanan hizmettir;

(26) "uluslararası kuruluş" uluslararası kamu hukuku ile düzenlenen bir kuruluş ve söz konusu kuruluşa bağlı organlar veya iki ya da daha fazla sayıda ülke arasındaki bir anlaşma ile veya böyle bir anlaşmaya dayanılarak kurulan diğer organlardır.

BÖLÜM II

İlkeler

Madde 5

Kişisel verilerin işlenmesine ilişkin ilkeler

1. Kişisel veriler:

(a) veri öznesi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir ("hukuka uygunluk, adalet ve şeffaflık");

(b) belirtilen, açık ve meşru amaçlarla toplanır ve bu amaçlara uygun olmayacak şekilde sonradan işlenmez; kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları veya istatistiki amaçlarla sonraki işleme, 89(1) maddesi uyarınca, baştaki amaçlara uygun olmadığı yönünde değerlendirilmez ("amacın sınırlandırılması");

(c) işlenme amaçlarına uygun, işlenme amaçlarıyla ilgili ve bunlarla sınırlı olmalıdır. ("veri minimizasyonu");

[19] Bilgi Toplumu hizmetlerine ilişkin teknik düzenlemeler ve kurallar alanında bilgi sağlanmasına yönelik usulü belirleyen 9 Eylül 2015 tarihli ve (AB) 2015/1535 sayılı Avrupa Parlamentosu ve Konsey Direktifi (ABRG L 241, 17.9.2015, s.1).

(d) doğrudur ve gerektiğinde güncel tutulur; işlenme amaçları göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeksizin kalıcı olarak silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır (“doğruluk”);

(e) veri öznelerinin, yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece kimliğinin belirlenmesini sağlayan bir şekilde tutulur; kişisel veriler, veri öznesinin hakları ve özgürlüklerinin güvence altına alınması için bu Tüzük’ün gerektirdiği uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanmasına tabi olmak kaydıyla, 89(1) maddesi uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece, daha uzun sürelerle depolanabilir (“depolamanın sınırlandırılması”);

(f) izinsiz veya hukuka aykırı işlemeye karşı ve kazara kayba, yok etmeye veya tahribe karşı koruma da dâhil olmak üzere, teknik veya düzenlemeye ilişkin uygun tedbirler kullanılarak kişisel verilerin uygun bir biçimde güvenliğini sağlayacak şekilde işlenir ("bütünlük ve gizlilik").

2. Veri sorumlusu, 1. paragrafa uygunluktan sorumludur ve bunu gösterebilmelidir ("hesap verebilirlik").

Madde 6

İşlemenin hukuka uygunluğu

1. İşleme, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve geçerli olduğu ölçüde hukuka uygundur:

(a) veri öznesinin, kişisel verilerinin bir ya da daha fazla spesifik amaca yönelik olarak işlenmesine rıza vermesi;

(b) veri öznesinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri öznesinin talebiyle adımlar atılması için işlemenin gerekli olması;

(c) veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyulması amacıyla işlemenin gerekli olması;

(d) veri öznesinin veya diğer bir gerçek kişinin hayati menfaatlerinin korunması amacıyla işlemenin gerekli olması;

(e) kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için işlemenin gerekli olması;

(f) özellikle veri öznesinin çocuk olması hâlinde, kişisel verilerin korunmasını gerektiren, veri öznesinin menfaatleri veya temel hak ve özgürlüklerinin bir veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu meşru menfaatler doğrultusunda işlemenin gerekli olması.

Birinci alt paragrafın (f) bendi, kamu makamlarının, görevlerini yerine getirirken veri işlemelerinde uygulanmaz.

3. 1. paragrafın (c) ve (e) bentlerinde belirtilen işlemenin dayanağı

(a) Birlik hukuku veya

(b)veri sorumlusunun tabi olduğu Üye Devlet hukuku ile ortaya konur.

İşleme amacı, söz konusu yasal dayanakta belirlenir veya 1. paragrafın (e) bendinde atıfta bulunulan işleme faaliyeti ile ilgili olarak, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için gereklidir. Söz konusu yasal dayanak, diğerlerinin yanı sıra, bu Tüzük kurallarının tatbik edilmesinin uyarlanmasına yönelik şu tür özel hükümler içerebilir: veri sorumlusu tarafından gerçekleştirilen işlemenin hukuka uygunluğunu düzenleyen genel koşullar; işlemeye tabi veri türleri; ilgili veri özneleri; kişisel verilerin açıklanabileceği teşekküller ve açıklanma amaçları; amacın sınırlandırılması; depolama süreleri ve IX. Bölümde belirtilen diğer spesifik işleme durumlarına yönelik tedbirler gibi hukuka uygun ve adil işlemenin sağlanmasına yönelik tedbirler de dâhil olmak üzere, işleme faaliyetleri ve işleme usulleri. Birlik veya Üye Devlet hukuku, kamu yararı amacını karşılar ve gözetilen meşru amaçla orantılıdır.

4. Kişisel verilerin toplanma amacı dışında bir amaca yönelik işlenmesinin, veri öznesinin rızasına veya 23(1) maddede atıfta bulunulan amaçların güvence altına alınması amacıyla demokratik bir toplumda gerekli ve orantılı bir tedbir teşkil eden Birlik veya Üye Devlet mevzuatına dayanmaması durumunda, veri sorumlusu, başka bir amaca yönelik işlemenin kişisel verilerin asıl toplanma amacına uygun olup olmadığını değerlendirmek üzere, diğerlerinin yanı sıra, aşağıdaki hususları dikkate alır:

(a) kişisel verilerin toplanma amaçları ile planlanan sonraki işleme amaçları arasındaki herhangi bir bağlantı;

(b) özellikle, veri özneleri ve veri sorumlusu arasındaki ilişki bakımından, kişisel verilerin toplandığı bağlam;

(c) 9. madde uyarınca özel kategorilerdeki kişisel verilerin işlenip işlenmediği veya 10. madde uyarınca mahkûmiyet kararları ve suçlara ilişkin kişisel verilerin işlenip işlenmediği başta olmak üzere, kişisel verilerin mahiyeti;

(d) planlanan sonraki işlemenin veri özneleri bakımından olası sonuçları;

(e) şifreleme veya takma ad kullanımı da içerebilecek uygun güvencelerin mevcut olması.

Madde 7

Rıza koşulları

1. İşlemenin rızaya dayandığı hâllerde, veri sorumlusu veri öznesinin kişisel verilerinin işlenmesine rıza vermiş olduğunu kanıtlayabilmelidir.

2. Veri öznesinin, rızasını diğer hususlarla da ilgili olan yazılı bir beyan biçiminde vermesi durumunda rıza talebi, diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir şekilde, açık ve sade bir dil kullanılarak sunulur. Söz konusu beyanın, bu Tüzük açısından ihlal teşkil eden hiçbir kısmı bağlayıcı değildir.

3. Veri öznesi, istediği zaman rızasını geri alma hakkına sahiptir. Rızanın geri çekilmesi, geri alma işleminden önce rızaya dayalı olarak yapılan işlemenin hukuka uygunluğunu etkilemez. Veri öznesine, rıza vermeden önce, bu hususta bilgi verilir. Rızanın geri çekilmesi rıza vermek kadar kolaydır.

4. Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, diğerlerinin yanı sıra, bir hizmetin sağlanması da dâhil olmak üzere, bir sözleşmenin ifasının, söz konusu sözleşmenin ifası için gerekli olmayan kişisel verilerin işlenmesine rıza verilmesine bağlı olup olmadığı azami ölçüde dikkate alınır.

Madde 8

Bilgi toplumu hizmetleri ile ilgili olarak çocuğun rızasına uygulanacak koşullar

1. 6(1) maddesinin (a) bendinin uygulanması durumunda, bilgi toplumu hizmetlerinin doğrudan bir çocuğa sağlanması ile ilgili olarak, çocuğun en az 16 yaşında olması hâlinde çocuğun kişisel verilerinin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması hâlinde, söz konusu işleme, ancak çocuk üzerinde velayet sorumluluğu bulunan kişi tarafından rıza veya izin verilmesi hâlinde ve rıza veya izin verildiği ölçüde hukuka uygundur.

Üye Devletler, bu amaçlara yönelik olarak, 13 yaştan küçük olmamak kaydıyla, mevzuatla daha küçük bir yaş belirleyebilir.

2. Bu durumlarda veri sorumlusu, mevcut teknolojiyi dikkate alarak, çocuk üzerinde velayet sorumluluğu bulunan kişi tarafından rıza veya izin verildiğini doğrulamak için makul çaba sarf eder.

3. 1. paragraf, bir çocuk ile ilgili bir sözleşmenin geçerliliği, oluşturulması veya etkisine ilişkin kurallar gibi Üye Devletlerin genel sözleşme hukukunu etkilemez.

Madde 9

Özel kategorilerdeki kişisel verilerin işlenmesi

1. Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğini açığa çıkaran kişisel verilerin işlenmesi ve bir gerçek kişinin kimliğini benzersiz bir şekilde belirleyen genetik veriler ile biyometrik verilerinin işlenmesi, sağlık verilerinin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.

2. 1. paragraf aşağıdakilerden birinin geçerli olması hâlinde uygulanmaz:

(a) Birlik veya Üye Devlet hukukunun 1. paragrafta belirtilen yasağın veri öznesi tarafından kaldırılamayacağını öngörmesi haricinde, veri öznesinin, belirtilen bir veya daha fazla amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık rıza vermesi;

(b) Birlik veya Üye Devlet hukuku çerçevesinde ya da veri öznesinin temel hak ve menfaatlerine yönelik uygun güvencelerin öngörüldüğü Üye Devlet hukuku uyarınca yapılan bir toplu sözleşme çerçevesinde izin verildiği sürece, veri sorumlusunun veya veri öznesinin istihdam ve sosyal güvenlik ile sosyal koruma hukuku alanındaki yükümlülüklerinin yerine getirilmesi ve spesifik haklarının kullanılması amacıyla işlemenin gerekli olması;

(c) veri öznesinin fiziksel veya hukuken rıza gösteremeyecek durumda olması hâlinde, veri öznesinin veya diğer bir gerçek kişinin hayati menfaatlerinin korunması için işlemenin gerekli olması;

(d) işlemenin; uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında, siyasi, felsefi, dini veya sendikal amaçlı bir vakıf, birlik veya kâr amacı gütmeyen başka bir müessese tarafından ve yalnızca müessesenin üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak müesseseyle düzenli olarak temas hâlinde bulunan kişilerle ilgili olması ve kişisel verilerin veri öznelerinin rızası olmaksızın söz konusu müessese dışında açıklanmaması koşuluyla gerçekleştirilmesi;

(e) işlemenin, veri öznesi tarafından açık bir biçimde alenileştirilen kişisel verilerle ilgili olması;

(f) hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması için veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ederken işlemenin gerekli olması;

(g) gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri öznesinin temel hak ve menfaatlerinin güvence altına alınması için uygun ve spesifik tedbirler öngören Birlik veya Üye Devlet hukuku temelinde esaslı kamu yararına yönelik nedenlerden dolayı işlemenin gerekli olması;

(h) işlemenin, koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da Üye Devlet hukuku temelinde veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi amacıyla gerekli olması;

(i) işlemenin; mesleki sır saklama başta olmak üzere, veri öznesinin hak ve özgürlüklerinin güvenceye alınması için uygun ve spesifik tedbirler öngören Birlik veya Üye Devlet hukuku temelinde, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartlarının tesis edilmesi gibi halk sağlığı alanında kamu yararı nedeniyle gerekli olması;

(j) işlemenin, gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri öznesinin temel hak ve menfaatlerinin güvence altına alınmasına uygun ve spesifik tedbirler öngören Birlik veya Üye Devlet hukuku temelinde, 89(1) madde uyarınca kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda gerekli olması.

3. 1. paragrafta atıfta bulunulan kişisel veriler, Birlik ya da Üye Devlet hukuku veya ulusal yetkili organlar tarafından tesis edilen kurallar kapsamında mesleki sır saklama yükümlülüğüne tabi bir profesyonel tarafından veya söz konusu profesyonelin sorumluluğu altında veya Birlik ya da Üye Devlet hukuku veya ulusal yetkili organlar tarafından tesis edilen kurallar kapsamında sır saklama yükümlülüğüne tabi başka bir kişi tarafından işlendiğinde, 2. paragrafın (h) bendinde atıfta bulunulan amaçlar doğrultusunda işlenebilir.

4. Üye Devletler, genetik veriler, biyometrik veriler veya sağlık verileri bakımından sınırlamalar dâhil olmak üzere, ilave koşulları uygulamaya devam edebilir ya da tesis edebilir.

Madde 10

Mahkûmiyet kararlarına ve suçlara ilişkin kişisel verilerin işlenmesi

Mahkûmiyet kararlarına ve suçlara ya da ilgili güvenlik tedbirlerine ilişkin kişisel verilerin 6(1) maddesi temelinde işlenmesi, ancak resmi bir makamın kontrolü altında veya veri öznelerinin hak ve özgürlüklerine yönelik uygun güvenceler sağlayan Birlik veya Üye Devlet hukuku çerçevesinde işlemeye izin verildiğinde gerçekleştirilir. Mahkûmiyet kararlarına ilişkin kapsamlı herhangi bir kayıt, yalnızca resmi makamın kontrolü altında tutulur.

Madde 11

Kimlik belirlenmesini gerektirmeyen işleme

1. Bir veri sorumlusunun kişisel veri işleme amaçlarının, veri sorumlusu tarafından bir veri öznesinin kimliğinin belirlenmesini gerektirmemesi veya artık buna gerek kalmaması halinde, veri sorumlusu, yalnızca bu Tüzük'e uyum sağlamak amacıyla veri öznesinin kimliğini belirlemek üzere ek bilgi tutmak, elde etmek veya işlemek zorunda değildir.

2. Bu maddenin 1. paragrafında atıfta bulunulan hâllerde, veri sorumlusunun veri öznesinin kimliğini belirleyecek bir konumda bulunmadığını kanıtlayabilmesi durumunda, veri sorumlusu mümkünse veri öznesine bilgi verir. Bu durumlarda, 15 ilâ 20. maddeler, veri öznesinin bu maddelerden kaynaklanan haklarını kullanmak amacıyla kimliğinin belirlenmesine olanak tanıyan ek bilgiler sağlaması haricinde uygulanmaz.

BÖLÜM III

Veri öznesinin hakları

Kesim 1

Şeffaflık ve yöntemler

Madde 12

Veri öznesinin haklarının kullanımına ilişkin şeffaf bilgi, bilgilendirme ve yöntemler

1. Veri sorumlusu spesifik olarak bir çocuğa yönelik her türlü bilgi başta olmak üzere işleme faaliyeti ile ilgili olarak 13 ve 14. maddelerde atıfta bulunulan her türlü bilgi ile 15 ilâ 22. ve 34. maddeler kapsamındaki her türlü bilgilendirmeyi kısa ve öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak veri öznesine sağlamak üzere uygun tedbirleri alır. Bilgiler yazılı olarak veya uygun olduğu hâllerde, elektronik yollar da dâhil olmak üzere diğer yollarla sağlanır. Veri öznesi tarafından talep edilmesi durumunda, veri öznesinin kimliğinin diğer yollarla doğrulanması koşuluyla, bilgiler sözlü olarak sağlanabilir.

2. Veri sorumlusu veri öznesinin 15 ilâ 22. maddeler kapsamındaki haklarının kullanılmasında kolaylık sağlar. 11(2) maddesinde atıfta bulunulan hâllerde, veri sorumlusunun veri öznesinin kimliğini belirleyecek bir konumda bulunmadığını göstermemesi hâlinde, veri sorumlusu veri öznesinin 15 ilâ 22. maddeler kapsamındaki haklarının kullanılması yönündeki talebini işleme koymayı reddetmez.

3. Veri sorumlusu 15 ilâ 22. maddeler kapsamındaki bir taleple ilgili olarak gerçekleştirilen işleme ilişkin bilgileri fazla gecikmeksizin ve her halükarda talebin alınmasından itibaren bir ay içinde veri öznesine sağlar. Bu süre, gerektiğinde, taleplerin karmaşıklığı ve sayısı dikkate alınarak iki ay daha uzatılabilir. Veri sorumlusu talebin alınmasından itibaren bir ay içinde söz konusu süre uzatımıyla birlikte gecikme sebepleri hakkında veri öznesine bilgi verir. Veri öznesinin talebini elektronik yollarla iletmesi hâlinde ve veri öznesi tarafından aksi talep edilmedikçe, bilgiler mümkün olduğunca elektronik yollarla sağlanır.

4. Veri sorumlusunun veri öznesinin talebi ile ilgili işlem yapmaması durumunda, veri sorumlusu işlem yapmama sebepleri ve bir denetim makamına şikâyette bulunma ve yargı yoluna başvurma olanağı ile ilgili olarak gecikmeksizin ve talebin alınmasından itibaren en geç bir ay içinde veri öznesine bilgi verir.

5. 13 ve 14. maddelerde sağlanan bilgiler ile 15 ilâ 22. ve 34. maddeler çerçevesinde yapılan her türlü bilgilendirme ve gerçekleştirilen her türlü işlem ücretsiz olarak sağlanır. Özellikle mükerrer niteliği nedeniyle bir veri öznesinin talepleri açık bir şekilde asılsız veya ölçüsüz ise, veri sorumlusu aşağıdakilerden birini gerçekleştirebilir:

(a) bilgiler veya bilgilendirme sağlanması veya talep edilen işlemin gerçekleştirilmesine ilişkin idari masrafları dikkate alarak makul bir ücret talep edebilir veya

(b) taleple ilgili işlem yapmayı reddedebilir.

Veri sorumlusu talebin açık bir şekilde asılsız veya ölçüsüz olduğunu gösterme yükümlülüğünü taşır.

6. 11. maddeye halel gelmeksizin, veri sorumlusunun 15 ilâ 21. maddelerde atıfta bulunulan talepte bulunan gerçek kişinin kimliği ile ilgili makul şüphelerinin bulunduğu hâllerde, veri sorumlusu veri öznesinin kimliğinin teyit edilmesi için gereken ek bilgilerin sağlanmasını talep edebilir.

7. 13 ve 14. maddeler uyarınca veri öznelerine sağlanacak bilgiler, planlanan işlemeye yönelik anlamlı bir genel bakışın kolayca görülebilir, anlaşılabilir ve okunaklı bir biçimde sunulması amacıyla standart simgelerle bir arada sağlanabilir. Simgelerin elektronik olarak sunulduğu hâllerde, simgeler makine tarafından okunabilecek şekilde sağlanır.

8. Komisyon simgelerle sunulacak bilgilerin ve standart simgeler sağlanmasına yönelik usullerin belirlenmesi amacıyla 92. madde uyarınca yetki devrine dayanan tasarruflar kabul etmeye yetkilidir.

Kesim 2

Bilgiler ve kişisel verilere erişim

Madde 13

Kişisel verilerin veri öznesinden toplandığı hâllerde sağlanacak bilgiler

1. Bir veri öznesine ilişkin kişisel verilerin veri öznesinden toplanması durumunda, veri sorumlusu kişisel verilerin elde edildiği anda aşağıdaki bilgilerin tamamını veri öznesine sağlar:

(a) veri sorumlusunun ve uygun olduğu hâllerde, veri sorumlusunun temsilcisinin kimlik ve irtibat bilgileri;

(b) uygun olduğu hâllerde, veri koruma görevlisinin irtibat bilgileri;

(c) kişisel verilerin planlanan işlenme amaçlarının yanı sıra işlemenin yasal dayanağı;

(d) işlemenin 6(1) maddesinin (f) bendine dayanması durumunda, veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatler;

(e) varsa, kişisel verilerin alıcıları veya alıcı kategorileri;

(f) uygun olduğu hâllerde, veri sorumlusunun kişisel verileri, bir üçüncü ülke veya uluslararası kuruluşa aktarmayı amaçladığı ve Komisyon tarafından bir yeterlilik kararı verilip verilmediği ya da 46 veya 47. maddelerde veya 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması hâlinde, uygun veya yerinde güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede sağlandığı.

2. 1. paragrafta atıfta bulunulan bilgilere ek olarak, veri sorumlusu kişisel verilerin elde edildiği anda adil ve şeffaf bir işleme faaliyeti için gereken aşağıdaki ek bilgileri veri öznesine sağlar:

(a) kişisel verilerin depolanacağı süre veya bunun mümkün olmaması hâlinde, bu sürenin belirlenmesi amacıyla kullanılan kriterler;

(b) veri sorumlusundan kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da kalıcı olarak silinmesini veya veri öznesi ile ilgili işlemenin kısıtlanmasını talep etme ya da işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının varlığı;

(c) işlemenin 6(1) maddesinin (a) bendine veya 9(2) maddesinin (a) bendine dayandığı hâllerde, rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işlemenin hukuka uygunluğu etkilenmeksizin, her zaman rızayı geri alma hakkının varlığı;

(d) denetim makamına şikâyette bulunma hakkı;

(e) kişisel verilerin sağlanmasının yasal ya da sözleşmeye bağlı bir gereklilik mi yoksa sözleşme yapılabilmesi için aranan bir gereklilik mi olduğu ve ayrıca, veri öznesinin kişisel verileri sağlamak zorunda olup olmadığı ve söz konusu verilerin sağlanmamasının muhtemel sonuçları;

(f) profillemede dâhil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar almanın varlığı ve en azından bu hâllerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçları.

3. Veri sorumlusunun kişisel verileri bu verilerin toplanma amacı dışında bir amaçla sonradan işlemeyi planladığı hâllerde, veri sorumlusu söz konusu sonraki işlemeden önce diğer amaca ilişkin bilgileri ve 2. paragrafta atıfta bulunulan diğer ilgili bilgileri veri öznesine sağlar.

4. Veri öznesinin hâlihazırda bu bilgilere sahip olduğu hâllerde ve ölçüde 1, 2 ve 3. paragraflar uygulanmaz.

Madde 14

Kişisel verilerin veri öznesinden alınmadığı hâllerde sağlanacak bilgiler

1. Kişisel verilerin veri öznesinden alınmaması durumunda, veri sorumlusu veri öznesine aşağıdaki bilgileri sağlar:

(a) veri sorumlusunun ve uygun olduğu hâllerde, veri sorumlusunun temsilcisinin kimlik ve irtibat bilgileri;

(b) uygun olduğu hâllerde, veri koruma görevlisinin irtibat bilgileri;

(c) kişisel verilerin planlanan işlenme amaçlarının yanı sıra işlemenin yasal dayanağı;

(d) ilgili kişisel veri kategorileri;

(e) varsa, kişisel verilerin alıcıları veya alıcı kategorileri;

(f) uygun olduğu hâllerde, veri sorumlusunun kişisel verileri bir üçüncü ülke veya uluslararası kuruluşa aktarmayı amaçladığı ve Komisyon tarafından bir yeterlilik kararı verilip verilmediği ya da 46 veya 47. maddelerde veya 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması hâlinde, uygun veya yerinde güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede sağlandığı.

2. 1. paragrafta atıfta bulunulan bilgilere ek olarak, veri sorumlusu veri öznesi açısından adil ve şeffaf bir işlemenin sağlanması için gereken aşağıdaki bilgileri veri öznesine sağlar:

(a) kişisel verilerin depolanacağı süre veya bunun mümkün olmaması hâlinde, bu sürenin belirlenmesi amacıyla kullanılan kriterler;

(b) işlemenin 6(1) maddesinin (f) bendine dayanması durumunda, veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatler;

(c) veri sorumlusundan kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da kalıcı olarak silinmesini veya veri öznesi ile ilgili işlemenin kısıtlanmasını talep etme hakkı ile işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının varlığı;

(d) işlemenin 6(1) maddesinin (a) bendine veya 9(2) maddesinin (a) bendine dayandığı hâllerde, rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işlemenin hukuka uygunluğu etkilenmeksizin, her zaman rızayı geri alma hakkının varlığı;

(e) denetim makamına şikâyette bulunma hakkı;

(f) kişisel verilerin hangi kaynaktan alındığı, ve uygun hâllerde, kişisel verilerin kamunun erişebileceği kaynaklardan gelip gelmediği;

(g) profilleme de dâhil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar almanın varlığı ve en azından bu hâllerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçları.

3. Veri sorumlusu 1 ve 2. paragraflarda atıfta bulunulan bilgileri şu şekilde sağlar:

(a) kişisel verilerin elde edilmesinden itibaren makul bir süre içinde, ancak kişisel verilerin işlendiği spesifik koşullar göz önünde tutularak, en geç bir ay içinde;

(b) kişisel verilerin veri öznesi ile bilgilendirme amacıyla kullanılacak olması durumunda, en geç söz konusu veri öznesi ile ilk kez iletişime geçildiği zaman veya

(c) başka bir alıcıya açıklamanın öngörülmesi hâlinde, en geç kişisel veriler ilk kez açıklandığı zaman.

4. Veri sorumlusunun kişisel verileri bu verilerin elde edilme amacı dışında bir amaçla sonradan işlemeyi planladığı hâllerde, veri sorumlusu söz konusu sonraki işlemeden önce diğer amaca ilişkin bilgileri ve 2. paragrafta atıfta bulunulan diğer ilgili bilgileri veri öznesine sağlar.

5. 1 ilâ 4. paragraflar aşağıdaki hâllerde ve ölçüde uygulanmaz:

(a) veri öznesinin hâlihazırda bilgisinin olması;

(b) 89(1) maddesinde atıfta bulunulan koşullara ve güvencelere tabi olarak kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar başta olmak üzere söz konusu bilgilerin sağlanmasının imkânsız olduğunun ortaya konulması veya ölçüsüz bir çaba gerektirmesi hâlinde ya da bu maddenin 1. paragrafında atıfta bulunulan yükümlülüğün söz konusu işleme amaçlarına ulaşılmasını imkânsız hâle getirmesi veya bu amaçlara ulaşılmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde. Böyle durumlarda, veri sorumlusu bilginin kamu erişimine açılması da dâhil olmak üzere veri öznesinin hakları ile özgürlüklerinin ve meşru menfaatlerinin korunması amacıyla uygun tedbirleri alır;

(c) elde etme veya açıklamanın, veri sorumlusunun tabi olduğu ve veri öznesinin meşru menfaatlerini korumak üzere uygun tedbirler öngören Birlik veya Üye Devlet hukukunda açıkça belirtilmesi veya

(d) kişisel verilerin yasadan kaynaklanan bir sır saklama yükümlülüğü de dâhil olmak üzere Birlik ya da Üye Devlet hukuku ile düzenlenen mesleki bir sır saklama yükümlülüğüne tabi olarak gizli kalmasının gerekmesi.

Madde 15

Veri öznesinin erişim hakkı

1. Veri öznesinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme ve işlemenin söz konusu olması hâlinde kişisel verilere ve aşağıdaki bilgilere erişim sağlama hakkı bulunur:

(a) işleme amaçları;

(b) ilgili kişisel veri kategorileri;

(c) üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri;

(d) mümkün olması hâlinde, kişisel verilerin depolanması için öngörülen süre veya bunun mümkün olmaması hâlinde, bu sürenin belirlenmesi amacıyla kullanılan kriterler;

(e) veri sorumlusundan veri öznesine ilişkin kişisel verilerin düzeltilmesi veya kalıcı olarak silinmesini ya da söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işlemeye itiraz etme hakkının varlığı;

(f) denetim makamına şikâyette bulunma hakkı;

(g) kişisel verilerin veri öznesinden toplanmaması hâlinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;

(h) profilleme de dâhil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar almanın varlığı ve en azından bu hâllerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçları.

2. Kişisel verilerin bir üçüncü ülke ya da bir uluslararası kuruluşa aktarılması durumunda, veri öznesinin aktarımla ilgili olarak 46. madde uyarınca uygun güvenceler hususunda bilgilendirilme hakkı bulunur.

3. Veri sorumlusu işlenen kişisel verilerin bir nüshasını temin eder. Veri öznesi tarafından talep edilen diğer nüshalarla ilgili olarak, veri sorumlusu idari masraflara istinaden makul bir ücret talep edebilir. Veri öznesinin talebini elektronik yollarla iletmesi hâlinde ve veri öznesi tarafından aksi talep edilmedikçe, bilgiler yaygın kullanılan bir elektronik yolla sağlanır.

4. 3. paragrafta atıfta bulunulan bir nüsha alma hakkı başkalarının hak ve özgürlüklerini olumsuz yönde etkilemez.

Kesim 3

Düzeltme ve kalıcı olarak silme

Madde 16

Düzeltme hakkı

Veri öznesinin kendisiyle ilgili doğru olmayan kişisel verilerin fazla gecikmeksizin düzeltilmesini veri sorumlusundan temin etme hakkı bulunur. İşleme amaçları dikkate alınarak, veri öznesinin, ek beyan yoluyla yapılması da dâhil olmak üzere, eksik kişisel verileri tamamlatma hakkı bulunur.

Madde 17

Kalıcı olarak silme hakkı ("unutulma hakkı")

1. Veri öznesinin kendisi ile ilgili kişisel verilerin fazla gecikmeksizin kalıcı olarak silinmesini veri sorumlusundan temin etme hakkı bulunur ve aşağıdaki hâllerden birinin geçerli olması

durumunda, veri sorumlusu kişisel verileri fazla gecikmeksizin kalıcı olarak silmekle yükümlüdür:

(a) kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması;

(b) veri öznesinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendine göre işlemenin dayandığı rızayı geri alması ve işlemeyle ilgili başka bir hukuki dayanak bulunmaması;

(c) veri öznesinin 21(1) maddesi uyarınca işlemeye itirazda bulunması ve işlemeye yönelik ağır basan meşru bir dayanak bulunmaması ya da veri öznesinin 21(2) maddesi uyarınca işlemeye itirazda bulunması;

(d) kişisel verilerin hukuka aykırı biçimde işlenmiş olması;

(e) veri sorumlusunun tabi olduğu Birlik veya Üye Devlet hukukundaki bir yasal yükümlülüğe uyum sağlanması amacıyla kişisel verilerin kalıcı olarak silinmesinin zorunlu olması;

(f) kişisel verilerin 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sunulması ile ilgili toplanmış olması.

2. Veri sorumlusunun kişisel verileri kamuya açıklamış olduğu ve 1. paragraf uyarınca kişisel verileri kalıcı olarak silmek zorunda olduğu hâllerde, veri sorumlusu, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri öznesinin talep ettiği kişisel verileri işleyen veri sorumlularına söz konusu kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının söz konusu veri sorumlularınca kalıcı olarak silinmesi hususunda bilgi vermek üzere teknik tedbirler de dâhil olmak üzere makul adımları atar.

3. İşleme aşağıdaki amaçlar doğrultusunda gerekli olduğu ölçüde 1 ve 2. paragraflar uygulanmaz:

(a) ifade özgürlüğü ve bilgi edinme hakkının kullanılması;

(b) veri sorumlusunun tabi olduğu Birlik veya Üye Devlet hukuku çerçevesinde işleme gerektiren bir yasal yükümlülüğe uyulması veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması;

(c) 9(2) maddesinin (h) ve (i) bentlerinin yanı sıra 9(3) maddesi uyarınca halk sağlığı alanındaki kamu yararı sebeplerinden dolayı;

(d) 1. paragrafta atıfta bulunulan hakkın işleme amaçlarına ulaşılmasını imkânsız hale getirmesi veya bu amaçlara ulaşılmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, 89(1) maddesi uyarınca kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya

(e) hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması açısından.

Madde 18

İşlemeyi kısıtlama hakkı

1. Aşağıdaki durumlardan birinin geçerli olması hâlinde, veri öznesinin veri sorumlusundan işlemenin kısıtlanmasını temin etme hakkı bulunur:

(a) veri sorumlusunun kişisel verilerin doğruluğunu teyit etmesine imkân veren sürede, veri öznesinin kişisel verilerin doğruluğuna itiraz etmesi;

(b) işlemenin hukuka aykırı olması ve veri öznesinin kişisel verilerin kalıcı olarak silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi;

(c) veri sorumlusunun işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması ancak veri öznesinin, hak talepleri oluşturma, hakkın yerine getirilmesi veya savunulması amacıyla söz konusu verilere ihtiyaç duyması;

(d) veri sorumlusunun meşru gerekçelerinin veri öznesinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar, veri öznesinin 21(1) maddesi uyarınca işlemeye itiraz etmesi.

2. İşleme faaliyetinin 1. paragraf kapsamında kısıtlanmış olduğu hâllerde, söz konusu kişisel veriler, depolama haricinde, yalnızca veri öznesinin rızasıyla veya hak taleplerinin oluşturulması, hakkın yerine getirilmesi ya da savunulmasına yönelik olarak ya da başka bir gerçek veya tüzel kişinin haklarının korunması amacıyla ya da Birlik veya bir Üye Devlet'in esaslı kamu yararı sebebiyle işlenir.

3. 1. paragraf uyarınca işlemenin kısıtlanmasını temin eden veri öznesine, işlemeye ilişkin kısıtlama kaldırılmadan önce, veri sorumlusu tarafından bilgi verilir.

Madde 19

Kişisel verilerin düzeltilmesine ya da kalıcı olarak silinmesine ya da işlemenin kısıtlanmasına ilişkin bildirim yükümlülüğü

Veri sorumlusu, imkânsız olduğunun ortaya konulmaması veya ölçüsüz bir çaba gerektirmemesi hâlinde, 16. madde, 17(1) maddesi ve 18. madde uyarınca gerçekleştirilen her türlü kişisel veri düzeltme veya kalıcı olarak silme işlemi ya da işlemenin kısıtlanması hakkında kişisel verilerin açıklandığı her alıcı bilgilendirilir. Veri öznesinin bu yönde bir talebinin bulunması hâlinde, veri sorumlusu veri öznesine bu alıcılar hakkında bilgi verir.

Madde 20

Veri taşınabilirliği hakkı

1. Aşağıdaki hâllerde, veri öznesinin kendisi ile ilgili olarak bir veri sorumlusuna sağladığı kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı bulunur ve kişisel verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın bu verileri başka bir veri sorumlusuna iletme hakkı bulunur:

(a) işlemenin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendi uyarınca bir rızaya veya 6(1) maddesinin (b) bendi uyarınca bir sözleşmeye dayanması ve

(b) işlemenin otomatik yollarla yapılması.

2. 1. paragraf uyarınca veri taşınabilirliği hakkını kullanırken veri öznesinin, teknik açıdan uygulanabilir olması hâlinde, kişisel verileri doğrudan bir veri sorumlusundan diğerine ilettirme hakkı bulunur.

3. Bu maddenin 1. paragrafında atıfta bulunulan hakkın kullanımı 17. maddeye halel getirmez. Söz konusu hak kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması için gereken işlemelere uygulanmaz.

4. 1. paragrafta atıfta bulunulan hak, başkalarının hak ve özgürlüklerini olumsuz yönde etkilemez.

İtiraz hakkı ve otomatik münferit karar alma

Madde 21

İtiraz hakkı

1. Veri öznesinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, (6)1 maddesinin (e) veya (f) bentlerine istinaden, profilleme de dâhil olmak üzere, bu bentlere dayanarak kendisi ile ilgili kişisel verilerin işlenmesine her zaman itiraz etme hakkı bulunur. Veri sorumlusu veri öznesinin menfaatleri, hakları ve özgürlüklerine veya hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulmasına ağır basan zorlayıcı meşru bir dayanak göstermediği sürece artık kişisel verileri işleyemez.

2. Kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, veri öznesinin doğrudan söz konusu pazarlamayla ilgili olduğu ölçüde profilleme de dâhil olmak üzere, kendisiyle ilgili kişisel verilerin söz konusu doğrudan pazarlama amacıyla işlenmesine her zaman itiraz etme hakkı bulunur.

3. Veri öznesinin doğrudan pazarlama amaçlarına yönelik işlemeye itiraz etmesi halinde, kişisel veriler artık bu amaçlarla işlenmez.

4. En geç veri öznesi ile ilk kez iletişime geçildiği zaman, 1 ve 2. paragraflarda atıfta bulunulan hak açık bir şekilde veri öznesine bildirilir ve diğer bilgilerden açık ve ayrı bir şekilde sunulur.

5. Bilgi toplumu hizmetlerinin kullanımı bağlamında ve 2002/58/AT sayılı Direktif'e bağlı olmaksızın, veri öznesi teknik özellikleri kullanmak suretiyle otomatik yollarla itiraz hakkını kullanabilir.

6. Kişisel verilerin 89(1) maddesi uyarınca bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlenmesi durumunda, işleme kamu yararı sebebiyle gerçekleştirilen bir görevin yürütülmesi için gerekli olmadığı sürece, veri öznesinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, kendisi ile ilgili kişisel verilerin işlenmesine itiraz hakkı bulunur.

Madde 22

Profilleme de dâhil olmak üzere otomatik münferit karar alma

1. Veri öznesinin kendisiyle ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen, profilleme de dâhil olmak üzere yalnızca otomatik işlemeye dayalı bir karara tabi olmama hakkı bulunur.

2. Kararın aşağıdaki özellikleri taşıması hâlinde, 1. paragraf uygulanmaz:

(a) veri öznesi ve bir veri sorumlusu arasında bir sözleşme yapılması veya söz konusu sözleşmenin uygulanması için gerekli olması;

(b) veri sorumlusunun tabi olduğu ve veri öznesinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği Birlik veya Üye Devlet hukuku tarafından verilen yetkiye dayanması veya

(c) veri öznesinin açık rızasına dayanması.

3. 2. paragrafın (a) ve (c) bentlerinde atıfta bulunulan hâllerde, asgari olarak, veri sorumlusunun müdahalesini temin hakkı başta olmak üzere, veri öznesinin kendi görüşünü ifade etme ve

karara karşı çıkma yönündeki hak ve özgürlükleri ile meşru menfaatlerini güvence altına almak için veri sorumlusu uygun tedbirleri uygular.

4. 2. paragrafta atıfta bulunulan kararlar, 9(2) maddesinin (a) veya (g) bendinin uygulandığı ve veri öznesinin hak ve özgürlükleri ile meşru menfaatlerini güvence altına almak üzere uygun tedbirlerin alındığı durumlar hariç, 9(1) maddesinde atıfta bulunulan özel kategorilerdeki kişisel verilere dayandırılmaz.

Kesim 5

Kısıtlamalar

Madde 23

Kısıtlamalar

1. Veri sorumlusu veya veri işleyenin tabi olduğu Birlik veya Üye Devlet hukuku, bir yasama tedbiri vasıtasıyla, temel hak ve özgürlüklerin esasına riayet etmesi ve demokratik bir toplumda aşağıdaki hususların güvence altına alınması açısından gerekli ve orantılı bir tedbir teşkil etmesi durumunda, 12 ilâ 22. maddeler ve 34. maddede öngörülen yükümlülük ve hakların kapsamını, ayrıca 5. madde hükümleri 12 ilâ 22. maddelerde öngörülen hak ve yükümlülüklere karşılık geldiği sürece 5. maddenin kapsamını kısıtlayabilir:

(a) milli güvenlik;

(b) savunma;

(c) kamu güvenliği;

(d) kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi;

(e) Birlik'in veya bir Üye Devlet'in önemli ekonomik veya mali çıkarı başta olmak üzere, parasal hususlar ile bütçe ve vergilendirmeye ilişkin hususlar, halk sağlığı ve sosyal güvenlik de dâhil, Birlik ya da bir Üye Devlet'in genel kamu yararına yönelik diğer önemli amaçlar;

(f) yargı bağımsızlığının ve yargısal süreçlerin korunması;

(g) düzenlenmiş mesleklere ilişkin etik kuralların ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması;

(h) nadiren olsa dahi, (a) ilâ (e) ve (g) bentlerinde atıfta bulunulan durumlarda resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi;

(i) veri öznesinin veya başkalarının hak ve özgürlüklerinin korunması;

(j) medeni hukuktan kaynaklanan hak iddialarına ilişkin kararların icrası.

2. Özellikle, 1. paragrafta atıfta bulunulan bir yasama tedbiri, ilgili olduğunda, asgari aşağıdaki hususlara ilişkin spesifik hükümleri içerir:

(a) işlemenin veya işleme kategorilerinin amaçları;

(b) kişisel veri kategorileri;

(c) getirilen kısıtlamaların kapsamı;

(d) kötüye kullanımın veya hukuka aykırı yollarla erişimin veya aktarımın engellenmesine yönelik güvenceler;

(e) veri sorumlusunun veya veri sorumlusu kategorilerinin belirlenmesi;

(f) işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak depolama süreleri ve uygulanabilir güvenceler;

(g) veri öznelerinin hak ve özgürlüklerine yönelik riskler ve

(h) kısıtlama amacına halel getirmemesi durumunda, veri öznelerinin kısıtlamayla ilgili bilgi sahibi olma hakkı.

BÖLÜM IV

Veri sorumlusu ve veri işleyen

Kesim 1

Genel yükümlülükler

Madde 24

Veri sorumlusunun sorumluluğu

1.Veri sorumlusu, işlemenin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra, gerçek kişilerin hak ve özgürlükleri açısından değişen olasılık ve ağırlıktaki riskleri dikkate alarak, işlemenin bu Tüzük'e uygun olarak gerçekleştirilmesini ve bunun gösterebilmesini temin etmek için uygun teknik ve kurumsal tedbirleri uygular. Bu tedbirler gözden geçirilir ve gerektiğinde, güncellenir.

2. İşleme faaliyetleriyle orantılı olması halinde, 1. paragrafta atıfta bulunulan tedbirler veri sorumlusu tarafından uygun veri koruma politikalarının uygulanmasını kapsar.

3. 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmalarına riayet edilmesi, veri sorumlusunun yükümlülüklerine uygunluğunun gösterilmesine yönelik bir unsur olarak kullanılabilir.

Madde 25

Tasarımdan itibaren ve varsayılan olarak veri koruma

1. Veri sorumlusu, son teknoloji, uygulama maliyeti ve işlemenin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra, işlemenin gerçek kişilerin hak ve özgürlüklere yönelik, değişen olasılık ve ağırlıktaki riskleri dikkate alarak, verilerin minimizasyonu gibi veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzük'ün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin işlemeye entegre edilmesi amacıyla tasarlanan takma ad

kullanımı gibi uygun teknik ve kurumsal tedbirleri hem işleme yönteminin belirlenmesi hem de işleme esnasında uygular ve veri öznelerinin haklarını korur.

2. Veri sorumlusu, varsayılan olarak, yalnızca her bir özel işleme amacı için gereken kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve kurumsal tedbirleri uygular. Söz konusu yükümlülük, toplanan kişisel veri miktarı, bunların işlenme derecesi, depolanma süresi ve erişilebilirliğine uygulanır. Söz konusu tedbirler özellikle, bireyin müdahalesi olmaksızın kişisel verilerin belirsiz sayıda gerçek kişinin erişimine varsayılan olarak açılmamasını sağlar.

3. 42. madde uyarınca onaylı bir belgelendirme mekanizması bu maddenin 1 ve 2. paragraflarında ortaya konulan gerekliliklere uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.

Madde 26

Birlikte veri sorumluları

1. İşleme amaçlarını ve yöntemlerini iki ya da daha fazla veri sorumlusunun ortak bir şekilde belirlediği hallerde, bu veri sorumluları birlikte veri sorumlularıdır. Birlikte veri sorumluları, veri sorumlularının ilgili sorumlulukları, veri sorumlularının tabi olduğu Birlik veya Üye Devlet hukuku çerçevesinde belirlenmedikçe ve belirlendiği ölçüde, özellikle veri öznesinin haklarının kullanımı ve 13 ve 14. maddelerde atıfta bulunulan bilgileri sağlama görevleri ile ilgili olarak bu Tüzük kapsamındaki yükümlülüklere uygunluğa ilişkin sorumluluklarını aralarındaki bir düzenleme vasıtasıyla şeffaf bir şekilde belirler. Düzenleme çerçevesinde veri öznelerine yönelik bir temas noktası belirlenebilir.

2. 1. paragrafta atıfta bulunulan düzenleme, birlikte veri sorumlularının veri özneleriyle karşılıklı rolleri ve ilişkilerini uygun şekilde yansıtır. Düzenlemenin mahiyeti, veri öznesinin erişimine sunulur.

3. 1. paragrafta atıfta bulunulan düzenlemenin koşullarına bakılmaksızın, veri öznesi bu Tüzük kapsamındaki haklarını her veri sorumlusu açısından ve her veri sorumlusuna karşı kullanabilir.

Madde 27

Birlik içinde kurulu olmayan veri sorumlularının veya veri işleyenlerin temsilcileri

1. 3(2) maddesinin uygulandığı hallerde, veri sorumlusu veya veri işleyen Birlik içinde yazılı olarak bir temsilci belirler.

2. Bu maddenin 1. paragrafında belirtilen yükümlülük aşağıdaki durumlara uygulanmaz:

(a) nadiren gerçekleşen, 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verilerin işlenmesini veya 10. maddede atıfta bulunulan mahkûmiyet kararları ve suçlar ile ilgili kişisel verilerin işlenmesini büyük çaplı olarak içermeyen ve işlemenin mahiyeti, bağlamı, kapsamı ve amaçları dikkate alındığında, gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebep olması muhtemel olmayan bir işleme veya

(b) bir kamu makamı veya organı.

3. Temsilci, kişisel verileri kendilerine mal veya hizmetlerin sağlanması ile ilgili olarak işlenen veya davranışı izlenen veri öznelerinin bulunduğu Üye Devletlerin birinde kurulur.

4. Temsilci, işleme faaliyeti ile ilgili tüm hususlarda, bu Tüzük'e uygunluk sağlanması amacıyla, özellikle denetim makamları ve veri özneleri tarafından veri sorumlusu veya veri işleyene ek olarak veya bunlar yerine muhatap kabul edilmek üzere, veri sorumlusu veya veri işleyen tarafından yetkilendirilir.

5. Veri sorumlusu veya veri işleyen tarafından bir temsilci belirlenmesi, veri sorumlusuna veya veri işleyene karşı başlatılabilecek yasal işlemlere halel getirmez.

Madde 28

Veri İşleyen

1. İşlemenin bir veri sorumlusu adına gerçekleştirileceği hallerde, veri sorumlusu, ancak işlemenin bu Tüzük'ün gerekliliklerinin yerine getirilmesini ve veri öznesinin haklarının korunmasını sağlayacak biçimde uygun teknik ve kurumsal tedbirler uygulama hususunda yeterli güvenceleri sağlayan veri işleyenler kullanır.

2. Veri işleyen, veri sorumlusunun önceden verdiği spesifik veya genel yazılı izin olmaksızın başka bir veri işleyen çalıştıramaz. Genel yazılı izin halinde, veri işleyen diğer veri işleyenlerin eklenmesi veya değiştirilmesi ile ilgili planlanan değişiklikler hususunda veri sorumlusuna söz konusu değişikliklere itiraz etme olanağı tanıyarak bilgi verir

3. Bir veri işleyen tarafından işlemenin gerçekleştirilmesi, veri sorumlusu ile ilgili olarak veri işleyen açısından bağlayıcı olan ve işlemenin konusu ve süresi, işlemenin mahiyeti ve amacı, kişisel verilerin türü ve veri öznelerinin kategorileri ile veri sorumlularının yükümlülükleri ve haklarının ortaya konulduğu, Birlik veya Üye Devlet hukuku çerçevesinde düzenlenen bir sözleşme veya diğer hukuki tasarruflar ile düzenlenir. Söz konusu sözleşme veya diğer hukuki tasarruflarda özellikle veri işleyenin aşağıdaki yükümlülükleri belirtilir:

(a) bir üçüncü ülkeye veya bir uluslararası kuruluşa kişisel veri aktarımları ile ilgili olanlar da dâhil olmak üzere, kişisel verileri yalnızca veri sorumlusunun verdiği belgelendirilmiş talimatlar doğrultusunda işler, veri işleyenin tabi olduğu Birlik veya Üye Devlet hukuku çerçevesinde aksi yönde bir gereklilik bulunan haller bunun dışındadır, ki bu hallerde, mevzuat çerçevesinde söz konusu bilgilendirme kamu yararına ilişkin önemli gerekçelerle yasaklanmadıkça, veri işleyen veri sorumlusuna işleme öncesinde bu hukuki gereklilik hakkında bilgi verir;

(b) kişisel verileri işleme yetkisi bulunan kişilerin gizlilik taahhüt etmelerini veya uygun bir yasal gizlilik yükümlülüğü altında bulunmalarını sağlar;

(c) 32. madde uyarınca gerekli tüm tedbirleri alır;

(d) başka bir veri işleyenle çalışılması amacıyla 2 ve 4. paragraflarda atıfta bulunulan koşullara riayet eder;

(e) işlemenin mahiyetinin dikkate alınması suretiyle, veri sorumlusunun, veri öznesinin III. Bölümde belirtilen haklarının kullanımına ilişkin taleplere yanıt verme yükümlülüğünün yerine getirilmesine yönelik olarak, uygun teknik ve kurumsal tedbirler vasıtasıyla, veri sorumlusuna mümkün olduğunca yardımcı olur;

(f) işlemenin mahiyetini ve veri işleyene sağlanan bilgileri dikkate alarak, 32 ila 36. maddeler uyarınca yükümlülüklere uygun hareket edilmesinin sağlanmasında veri sorumlusuna yardımcı olur;

(g) veri sorumlusunun tercihine bağlı olarak, işlemeyle ilgili hizmetlerin sağlanmasından sonra tüm kişisel verileri siler veya veri sorumlusuna iade eder ve Birlik ya da Üye Devlet hukuku çerçevesinde kişisel verilerin depolanmasının gerekli olmaması durumunda, mevcut nüshaları siler;

(h) bu maddede ortaya konulan yükümlülüklere uygunluğun gösterilmesi için gereken tüm bilgileri veri sorumlusuna sağlar ve teftişler de dâhil olmak üzere, veri sorumlusu tarafından

ya da veri sorumlusunca yetkilendirilen başka bir denetçi tarafından gerçekleştirilen denetimlere izin verir ve katkıda bulunur.

İlk alt paragrafın (h) bendi ile ilgili olarak, veri işleyen, bir talimatın bu Tüzük veya Birlik ya da Üye Devlet'in diğer veri koruma hükümlerini ihlal ettiğini düşünmesi halinde, veri sorumlusuna ivedilikle bilgi verir.

4. Bir veri işleyenin veri sorumlusu adına belirli işleme faaliyetlerinin gerçekleştirilmesine yönelik olarak diğer bir veri işleyen çalıştırdığı durumlarda, 3. paragrafta atıfta bulunulan veri sorumlusu ve veri işleyen arasındaki sözleşme veya başka bir hukuki tasarrufta ortaya konulan veri koruma yükümlülükleri, özellikle işlemenin bu Tüzük'ün gerekliliklerinin yerine getirilmesini sağlayacak şekilde uygun teknik ve kurumsal tedbirlerin uygulanması için yeterli güvenceleri sağlayan bir sözleşme ya da Birlik veya Üye Devlet hukuku kapsamındaki başka bir hukuki tasarruf yoluyla diğer veri işleyene de uygulanır. Diğer veri işleyenin veri koruma yükümlülüklerini yerine getiremediği hallerde, ilk veri işleyen, diğer veri işleyenin yükümlülüklerinin ifası konusunda veri sorumlusuna karşı tamamen sorumlu olmaya devam eder.

5. Bir veri işleyenin 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmalarına uygun hareket etmesi, bu maddenin 1 ve 4. paragraflarında atıfta bulunulan yeterli güvencelerin gösterilmesine ilişkin bir unsur olarak kullanılabilir.

6. Veri sorumlusu ve veri işleyen arasındaki münferit bir sözleşmeye halel gelmeksizin, bu maddenin 3 ve 4. paragraflarında atıfta bulunulan sözleşme ya da başka bir hukuki tasarruf, 42 ve 43. maddeler uyarınca veri sorumlusuna veya veri işleyene sağlanan bir belgelendirmenin parçası olmaları durumu da dâhil olmak üzere, tamamen veya kısmen, bu maddenin 7 ve 8. paragraflarında atıfta bulunulan standart sözleşme hükümlerine dayanabilir.

7. Komisyon bu maddenin 3 ve 4. paragraflarında atıfta bulunulan hususlara yönelik olarak ve 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca standart sözleşme hükümleri oluşturabilir.

8. Bir denetim makamı bu maddenin 3 ve 4. paragraflarında atıfta bulunulan hususlara yönelik olarak ve 63. maddede atıfta bulunulan tutarlılık mekanizması uyarınca standart sözleşme hükümleri kabul edebilir.

9. 3 ve 4. paragraflarda atıfta bulunulan sözleşme veya diğer hukuki tasarruflar elektronik format da dâhil olmak üzere, yazılı olarak hazırlanır.

10. 82, 83 ve 84. maddelere halel gelmeksizin, bir veri işleyenin işleme amaçlarını ve yöntemlerini belirleyerek bu Tüzük'ü ihlal etmesi durumunda, veri işleyen bu işleme açısından veri sorumlusu olarak değerlendirilir.

Madde 29

Veri sorumlusunun veya veri işleyenin otoritesi altında işleme

Veri işleyen ile veri sorumlusunun ya da veri işleyenin otoritesi altında hareket eden ve kişisel verilere erişimi bulunan hiç kimse, Birlik ya da Üye Devlet hukuku çerçevesinde bu yönde hareket etmesi gerekmedikçe, veri sorumlusundan aldığı talimatlar haricinde bu verileri işlemez.

Madde 30

İşleme faaliyetlerinin kayıtları

1. Her veri sorumlusu ve uygun olduğu hâllerde, veri sorumlusunun temsilcisi, kendi sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutar. Bu kayıt aşağıdaki bilgilerin tamamını ihtiva eder:

(a) veri sorumlusu ve uygun olduğu hâllerde, birlikte veri sorumlusu, veri sorumlusu temsilcisi ve veri koruma görevlisinin isim ve irtibat bilgileri;

(b) işleme amaçları;

(c) veri öznesi kategorileri ve kişisel veri kategorileriyle ilgili bir açıklama;

(d) üçüncü ülkelerdeki veya uluslararası kuruluşlardaki alıcılar da dâhil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri;

(e) uygun olduğu hâllerde, bir üçüncü ülkenin veya bir uluslararası kuruluşun tanımlanması ve 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun güvencelere ilişkin belgelendirme de dâhil olmak üzere, kişisel verilerin söz konusu üçüncü ülke veya uluslararası kuruluşa aktarılması;

(f) mümkün olması hâlinde, farklı kategorilerdeki verilerin kalıcı olarak silinmesi için öngörülen süre sınırları;

(g) mümkün olması hâlinde, 32(1) maddesinde atıfta bulunulan teknik ve kurumsal güvenlik tedbirlerine yönelik genel bir açıklama.

2. Her veri işleyen ve uygun olduğu hâllerde, veri işleyenin temsilcisi, bir veri sorumlusu adına gerçekleştirilen tüm kategorilerdeki işleme faaliyetlerine ilişkin olarak aşağıdakileri ihtiva eden bir kayıt tutar:

(a) Veri işleyenin veya işleyenlerin ve veri işleyenin adına hareket ettiği her bir veri sorumlusunun ve uygun olduğu hâllerde, veri sorumlusu ya da veri işleyenin temsilcisinin ve veri koruma görevlisinin isim ve irtibat bilgileri;

(b) her bir veri sorumlusu adına gerçekleştirilen işleme kategorileri;

(c) uygun olduğu hâllerde, bir üçüncü ülkenin veya bir uluslararası kuruluşun tanımlanması ve 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun güvencelere ilişkin belgelendirme de dâhil olmak üzere, kişisel verilerin söz konusu üçüncü ülke veya uluslararası kuruluşa aktarılması;

(d) mümkün olması hâlinde, 32(1) maddesinde atıfta bulunulan teknik ve kurumsal güvenlik tedbirlerine yönelik genel bir açıklama.

3. 1 ve 2. paragraflarda atıfta bulunulan kayıtlar elektronik format da dâhil olmak üzere, yazılı olarak tutulur.

4. Veri sorumlusu ve veri işleyen ile uygun olduğu hâllerde, veri sorumlusunun veya veri işleyenin temsilcisi, talep üzerine, kayıtları denetim makamına sağlar.

5. Gerçekleştirdiği işlemenin veri öznelerinin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması, işlemenin nadiren gerçekleştirilmemesi veya işlemenin 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verileri ya da 10. maddede atıfta bulunulan mahkûmiyet kararları ve suçlara ilişkin kişisel verileri kapsamaması durumunda, 1 ve 2. paragraflarda atıfta bulunulan yükümlülükler 250'den az kişi istihdam eden bir işletme veya organizasyona uygulanmaz.

Madde 31

Denetim makamıyla iş birliği

Veri sorumlusu ve veri işleyen ile uygun olduğu hâllerde, bunların temsilcileri, talep üzerine, görevlerinin yürütülmesi ile ilgili olarak denetim makamı ile iş birliği yapar.

Kesim 2

Kişisel verilerin güvenliği

Madde 32

İşleme güvenliği

1. Veri sorumlusu ve veri işleyen, son teknoloji, uygulama maliyetleri ve işlemenin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra, gerçek kişilerin hakları ve özgürlükleri açısından değişen olasılık ve ağırlıktaki riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, diğer hususların yanı sıra, uygun olduğu hâllerde, aşağıdakiler de dâhil olmak üzere uygun teknik ve kurumsal tedbirler uygular:

(a) kişisel verilerde takma ad kullanımı ve şifreleme;

(b) işleme sistemlerinin ve hizmetlerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve mukavemetini sürekli olarak sağlama kabiliyeti;

(c) fiziksel veya teknik bir olay durumunda, kişisel verilerin kullanılabilirliğinin ve kişisel verilere erişimin vakitlice yeniden sağlanma kabiliyeti;

(d) işlemenin güvenliliğinin sağlanmasına yönelik olarak teknik ve kurumsal tedbirlerin etkililiğinin düzenli olarak sınanmasına, ölçülmesine ve değerlendirilmesine ilişkin süreç.

2. Uygun güvenlik seviyesi değerlendirilirken, iletilen, depolanan veya işlenen kişisel verilerin kazara veya hukuka aykırı olarak yok edilmesi, kaybı, değiştirilmesi, izinsiz şekilde açıklanması veya bunlara erişim başta olmak üzere, özellikle işlemenin yol açtığı riskler göz önünde bulundurulur.

3. 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmasına uygun hareket edilmesi, bu maddenin 1. paragrafında ortaya konulan gerekliliklere uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.

4. Veri sorumlusu ve veri işleyen, veri sorumlusunun ya da veri işleyenin otoritesi altında hareket eden ve kişisel verilere erişimi bulunan her gerçek kişinin, Birlik ya da Üye Devlet hukuku çerçevesinde aksi öngörülmedikçe, veri sorumlusundan aldığı talimatlar haricinde bu verileri işlememesini sağlamak üzere adımlar atar.

Madde 33

Kişisel veri ihlalinin denetim makamlarına bildirilmesi

1. Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmadığı haller dışında, veri sorumlusu, fazla gecikmesizin ve uygun olması hâlinde, ihlalden haberdar olduktan itibaren en geç 72 saat içinde, kişisel veri ihlalini 55. madde uyarınca yetkili denetim makamına bildirir. Denetim makamına yönelik bildirimin 72 saat içinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir.

2. Veri işleyen, bir kişisel veri ihlalinden haberdar olduktan sonra, fazla gecikmeksizin, veri sorumlusuna bildirimde bulunur.

3. 1. paragrafta atıfta bulunulan bildirimde asgari olarak:

(a) uygun olduğu hâllerde, ilgili veri öznesi kategorileri ve yaklaşık sayısı ile ilgili kişisel veri kaydı kategorileri ve yaklaşık sayısı da dâhil olmak üzere, kişisel veri ihlalinin mahiyeti açıklanır;

(b) veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgileri iletilir;

(c) kişisel veri ihlalinin olası sonuçları açıklanır;

(d) uygun olduğu hâllerde, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dâhil olmak üzere, kişisel veri ihlalinin ele alınması için veri sorumlusu tarafından alınan veya alınması önerilen tedbirler açıklanır.

4. Bilgilerin aynı zamanda sağlanmasının mümkün olmadığı hâllerde ve ölçüde, bilgiler daha fazla gecikmeksizin aşamalı olarak sağlanabilir.

5. Veri sorumlusu kişisel veri ihlallerini, kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirir. Bu belgelendirme, denetim makamının bu maddeye uygunluğu doğrulamasını sağlar.

Madde 34

Kişisel veri ihlali hakkında veri öznesinin bilgilendirilmesi

1. Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hâllerde, veri sorumlusu kişisel veri ihlali hakkında fazla gecikmeksizin, veri öznesini bilgilendirir.

2. Bu maddenin 1. paragrafında atıfta bulunulan veri öznesine yönelik bilgilendirmede kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanır ve asgari olarak, 33(3) maddesinin (b), (c) ve (d) bentlerinde atıfta bulunulan bilgiler ve tedbirlere yer verilir.

3. Aşağıdaki koşulların herhangi birinin yerine getirilmesi durumunda, 1. paragrafta atıfta bulunulan veri öznesine yönelik bilgilendirme gerekmez:

(a) veri sorumlusunun uygun teknik ve kurumsal koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim izni bulunmayan hiç kimse tarafından anlaşılamaz hale getiren şifreleme gibi tedbirler başta olmak üzere, bu tedbirlerin kişisel veri ihlalinden etkilenen kişisel verilere uygulanmış olması;

(b) veri sorumlusunun 1. paragrafta atıfta bulunulan veri öznelerinin hak ve özgürlüklerine ilişkin yüksek riskin gerçeğe dönüşmesinin artık muhtemel olmamasını sağlayan ek tedbirler alması;

(c) bilgilendirmenin orantısız bir çaba gerektirecek olması. Bu durumda, veri öznesinin bilgilendirilmesi yerine, veri öznelerine aynı etkililikle bilgi verilen kamuya yönelik bir bilgilendirme veya benzeri bir tedbir uygulanır.

4. Veri sorumlusunun kişisel veri ihlali hakkında veri öznesini hâlihazırda bilgilendirmediği durumda, denetim makamı, kişisel veri ihlalinin yüksek bir riske sebebiyet verme olasılığını değerlendirdikten sonra, veri sorumlusunun bu bilgilendirmeyi yapmasını şart koşabilir veya 3. paragrafta atıfta bulunulan koşullardan herhangi birinin karşılandığına karar verebilir.

Kesim 3

Veri koruma etki değerlendirmesi ve ön istişare

Madde 35

Veri koruma etki değerlendirmesi

1. Özellikle yeni teknolojiler kullanılırken ve işlemenin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hâllerde, veri sorumlusu, işleme öncesinde, öngörülen işleme faaliyetlerinin kişisel verilerin korunması üzerindeki etkisine ilişkin bir değerlendirme yapar. Tek bir değerlendirmede benzeri yüksek riskler taşıyan bir dizi benzer işleme faaliyeti ele alınabilir.

2. Veri sorumlusu, veri koruma etki değerlendirmesi gerçekleştirirken, belirlenmiş olması hâlinde, veri koruma görevlisinin tavsiyesine başvurur.

3. 1. paragrafta atıfta bulunulan veri koruma etki değerlendirmesi aşağıdaki durumlarda özellikle gereklidir:

(a) Profilleme de dâhil olmak üzere, otomatik işlemeye dayanan ve gerçek kişilerle ilgili hukuki sonuçlar doğuran veya benzeri biçimde, gerçek kişileri önemli ölçüde etkileyen kararların dayandığı, gerçek kişilerle ilgili kişisel özelliklerin sistematik ve kapsamlı bir değerlendirmesi;

(b) 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verilerin veya 10. maddede atıfta bulunulan mahkûmiyet kararlarına ve suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi veya

(c) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi.

4. Denetim makamı 1. paragraf uyarınca bir veri koruma etki değerlendirmesi gerekliliğine tabi olan işleme faaliyetlerinin türüne ilişkin bir liste oluşturur ve bu listeyi kamuya açıklar.1. Denetim makamı, bu listeleri 68. maddede atıfta bulunulan Kurula iletir.

5. Denetim makamı bir veri koruma etki değerlendirmesinin gerekli olmadığı işleme faaliyetlerinin türüne ilişkin bir liste oluşturabilir ve bu listeyi kamuya açıklayabilir. Denetim makamı bu listeleri Kurula iletir.

6. Yetkili denetim makamı, 4 ve 5. paragraflarda atıfta bulunulan listelerin kabulünden önce, söz konusu listelerin veri öznelerine çeşitli Üye Devletlerde mal veya hizmetlerin sağlanması ya da veri öznelerinin davranışlarının izlenmesi ile ilgili olan veya kişisel verilerin Birlik içinde serbest dolaşımını kayda değer ölçüde etkileyebilecek işleme faaliyetlerine yer verildiği hâllerde, 63. maddede atıfta bulunulan tutarlılık mekanizmasını uygular.

7. Değerlendirme asgari olarak aşağıdaki hususları içerir:

(a) uygun olduğu hâllerde, veri sorumlusu tarafından gözetilen meşru menfaat de dâhil olmak üzere öngörülen işleme faaliyetleri ve işleme amaçlarına ilişkin sistematik bir açıklama;

(b) işleme faaliyetlerinin amaçlarla ilişkili olarak gerekliliği ve orantılılığına ilişkin bir değerlendirme;

(c) 1. paragrafta atıfta bulunulduğu üzere veri öznelerinin hak ve özgürlüklerine yönelik risklere ilişkin bir değerlendirme ve

(d) veri öznelerinin ve ilgili diğer kişilerin hakları ve meşru menfaatleri dikkate alınarak, kişisel verilerin korunmasının sağlanmasıyla ve bu Tüzük'e uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dâhil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler.

8. Veri sorumluları veya veri işleyenler tarafından özellikle bir veri koruma etki değerlendirmesi amaçlarına yönelik olarak gerçekleştirilen işleme faaliyetlerinin etkisinin değerlendirilmesi bakımından, ilgili veri sorumluları veya veri işleyenler tarafından 40. maddede atıfta bulunulan onaylı davranış kurallarına uyum sağlanması dikkate alınır.

9. Uygun olduğu hâllerde, veri sorumlusu, ticari menfaatlerin veya kamu menfaatlerinin korunmasına ya da işleme faaliyetlerinin güvenliğine halel gelmeksizin, veri öznelerinin veya temsilcilerinin amaçlanan işlemeye ilişkin görüşlerini alır.

10. 6(1) maddesinin (c) veya (e) bendi uyarınca gerçekleştirilen bir işlemenin Birlik hukukunda veya veri sorumlusunun tabi olduğu Üye Devlet'in mevzuatında hukuki bir dayanağının bulunduğu, söz konusu mevzuatın belirli bir işleme faaliyetini veya bir dizi faaliyeti düzenlediği ve bir veri koruma etki değerlendirmesinin söz konusu hukuki dayanağın kabulü bağlamında genel bir etki değerlendirmesinin parçası olarak zaten gerçekleştirilmiş olduğu hâllerde, Üye Devletler işleme faaliyetlerinden önce böylesi bir değerlendirme yapılmasını gerekli görmedikçe, 1 ila 7. paragraflar uygulanmaz.

11. Gerekmesi hâlinde, en azından işleme faaliyetlerinin teşkil ettiği risk açısından bir değişiklik meydana geldiğinde, veri sorumlusu, işlemenin veri koruma etki değerlendirmesi uyarınca gerçekleştirilip gerçekleştirilmediğini değerlendirmek üzere bir gözden geçirme gerçekleştirir.

Madde 36

Ön istişare

1. 35. madde kapsamındaki bir veri koruma etki değerlendirmesinin, veri sorumlusu tarafından riskin azaltılması hususunda tedbir alınmadığı takdirde işlemenin yüksek bir riske sebebiyet vereceğini gösterdiği hâllerde, veri sorumlusu işleme öncesinde denetim makamına danışır.

2. Veri sorumlusunun riski yeterli şekilde belirlemediği veya azaltmadığı hâller başta olmak üzere, denetim makamının, 1. paragrafta atıfta bulunulan amaçlanan işleme faaliyetinin bu Tüzük'ü ihlal edeceğini düşündüğü hâllerde, denetim makamı, istişare talebinin alınmasından itibaren sekiz haftalık bir süre içinde, veri sorumlusuna ve uygun olduğunda, veri işleyene yazılı tavsiyede bulunur ve 58. maddede atıfta bulunulan yetkilerinden herhangi birini kullanabilir. Bu süre, amaçlanan işlemenin karmaşıklığı dikkate alınarak, altı hafta uzatılabilir. Denetim makamı, istişare talebinin alınmasından itibaren bir ay içinde veri sorumlusuna ve uygun olduğu hâllerde, veri işleyene gecikmenin sebepleri ile birlikte bu tür bir süre uzatımı ile ilgili olarak bilgi verir. Bu süreler, denetim makamı istişare amacıyla talep etmiş olduğu bilgileri elde edene kadar askıya alınabilir.

3. 1. paragraf uyarınca denetim makamına danışılırken, veri sorumlusu denetim makamına şunları sağlar:

(a) uygun olduğu hâllerde, veri sorumlusunun, birlikte veri sorumlularının ve işlemeye dahil olan veri işleyenlerin, özellikle bir teşebbüsler grubu dahilindeki işlemeye yönelik sorumlulukları;

(b) planlanan işleme amaçları ve yöntemleri;

(c) veri öznelerinin haklarının ve özgürlüklerinin korunması amacıyla bu Tüzük uyarınca sağlanan tedbirler ve güvenceler;

(d) uygun olduğu hâllerde, veri koruma görevlisinin irtibat bilgileri;

(e) 35. maddede belirtilen veri koruma etki değerlendirmesi ve

(f) denetim makamının talep ettiği diğer bilgiler.

4. Üye Devletler, bir ulusal parlamento tarafından kabul edilecek bir yasama tedbiri teklifinin veya böylesi bir yasama tedbirine dayanan işlemeye ilişkin bir düzenleyici tedbirinin hazırlanması esnasında denetim makamına danışır.

5. 1. paragrafa bakılmaksızın, Üye Devlet hukuku, sosyal koruma ve halk sağlığına ilişkin işlemeler de dâhil olmak üzere, veri sorumlusu tarafından kamu yararına gerçekleştirilen bir görevin yürütülmesine yönelik olarak bir veri sorumlusu tarafından gerçekleştirilen işleme hususunda veri sorumlularının denetim makamına danışmasını ve ön izin almasını gerektirebilir.

Kesim 4

Veri koruma görevlisi

Madde 37

Veri koruma görevlisinin belirlenmesi

1. Veri sorumlusu ve veri işleyen aşağıdaki durumlarda bir veri koruma görevlisi belirler:

(a) işlemenin, kendi yargı yetkisi çerçevesinde hareket eden mahkemeler haricindeki bir kamu makamı veya organı tarafından gerçekleştirilmesi;

(b) veri sorumlusunun veya veri işleyenin temel faaliyetlerinin niteliği, kapsamı ve/veya amaçları itibarıyla veri öznelerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya

(c) veri sorumlusunun veya veri işleyenin temel faaliyetlerinin 9. madde uyarınca özel kategorilerdeki verilerin ve 10. maddede atıfta bulunulan mahkûmiyet kararlarına ve suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi.

2. Bir teşebbüsler grubu, veri koruma görevlisine her kuruluştan kolay bir şekilde erişilebilmesi koşuluyla, tek bir veri koruma görevlisi belirleyebilir.

3. Veri sorumlusunun veya veri işleyenin bir kamu makamı ya da organı olduğu hâllerde, kurumsal yapıları ve büyüklükleri dikkate alınarak, bu tür kamu makam veya organlarının birden fazlası için tek bir veri koruma görevlisi belirlenebilir.

4. 1. paragrafta atıfta bulunulanlar haricindeki durumlarda, veri sorumlusu veya veri işleyen veya birlikler ya da veri sorumlusu veya veri işleyen kategorilerini temsil eden diğer organlar bir veri koruma görevlisi belirleyebilirler veya Birlik ya da Üye Devlet hukukunun gerektirdiği hâllerde, bir veri koruma görevlisi belirlerler. Veri koruma görevlisi, veri sorumlularını ve veri işleyenleri temsil eden bu tür birlikler ve diğer organlar adına hareket edebilir.

5. Veri koruma görevlisi mesleki nitelikler ve özellikle veri koruma hukukuna ve uygulamalarına ilişkin uzmanlık bilgisi ile 39. maddede atıfta bulunulan görevleri yerine getirme kabiliyetine dayalı olarak belirlenir.

6. Veri koruma görevlisi veri sorumlusunun veya veri işleyenin bir çalışanı olabilir veya görevlerini bir hizmet sözleşmesine dayalı olarak yerine getirebilir.

7. Veri sorumlusu veya veri işleyen veri koruma görevlisinin irtibat bilgilerini yayımlar ve denetim makamına iletir.

Madde 38

Veri koruma görevlisinin konumu

1. Veri sorumlusu ve veri işleyen, veri koruma görevlisinin kişisel verilerin korunmasına ilişkin tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlar.

2. Veri sorumlusu ve veri işleyen, 39. maddede atıfta bulunulan görevlerin ifasında veri koruma görevlisine, bu görevlerin yerine getirilmesi, kişisel verilere ve işleme faaliyetlerine erişim sağlaması ve uzmanlık bilgisini muhafaza etmesi için gerekli kaynakları sağlamak suretiyle destek verir.

3. Veri sorumlusu ve veri işleyen veri koruma görevlisinin bu görevlerin yerine getirilmesi ile ilgili olarak hiçbir talimat almamasını sağlar. Veri koruma görevlisi, görevlerini yerine getirmesi nedeniyle veri sorumlusu veya veri işleyen tarafından işten çıkarılamaz ya da cezalandırılamaz. Veri koruma görevlisi, veri sorumlusunun veya veri işleyenin en üst yönetim kademesine doğrudan rapor verir.

4. Veri özneleri kişisel verilerinin işlenmesi ve bu Tüzük kapsamındaki haklarının kullanımı ile ilgili tüm hususlarla alakalı olarak veri koruma görevlisiyle irtibata geçebilir.

5. Veri koruma görevlisi, Birlik veya Üye Devlet hukuku uyarınca, görevlerinin yerine getirilmesi ile ilgili olarak sır saklama veya gizlilik ilkeleri ile bağlıdır.

6. Veri koruma görevlisi, başka görevleri ve sorumlulukları da yerine getirebilir. Veri sorumlusu veya veri işleyen, söz konusu görev ve sorumlulukların bir çıkar çatışmasına neden olmamasını sağlar.

Madde 39

Veri koruma görevlisinin görevleri

1. Veri koruma görevlisinin asgari olarak aşağıdaki görevleri bulunur:

(a) veri sorumlusu veya veri işleyen ile işlemeyi gerçekleştiren çalışanlara, bu Tüzük ve Birlik ya da Üye Devletlerin diğer veri koruma hükümleri uyarınca yükümlülükleri hususunda bilgi verilmesi ve onlara tavsiyede bulunulması;

(b) sorumlulukların tahsisi, işleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ve ilgili denetimler de dâhil olmak üzere, bu Tüzük'e, diğer Birlik veya Üye Devletlerin veri koruma hükümlerine ve veri sorumlusu veya veri işleyenin kişisel verilerin korunmasına ilişkin politikalarına uyumun izlenmesi;

(c) talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyelerde bulunulması ve 35. madde uyarınca bu değerlendirmenin ifasının izlenmesi;

(d) denetim makamıyla iş birliği yapılması;

(e) 36. maddede atıfta bulunulan ön istişare de dâhil olmak üzere, işlemeye ilişkin konularda denetim makamı için bir temas noktası olarak hareket edilmesi ve uygun olduğu hâllerde, diğer her türlü konu ile ilgili olarak istişarede bulunulması.

2. Veri koruma görevlisi, görevlerini yerine getirirken, işlemenin mahiyeti, kapsamı, bağlamı ve amaçlarını dikkate alarak, işleme faaliyetleri ile ilişkili riski gerektiği şekilde göz önünde bulundurur.

Davranış kuralları ve belgelendirme

Madde 40

Davranış kuralları

1. Üye Devletler, denetim makamları, Kurul ve Komisyon, çeşitli işleme sektörlerinin belirli özelliklerini ve mikro, küçük ve orta büyüklükteki işletmelerin özel ihtiyaçlarını dikkate alarak, bu Tüzük'ün düzgün bir şekilde uygulanmasına katkıda bulunmayı amaçlayan davranış kurallarının hazırlanmasını teşvik ederler.

2. Birlikler ve veri sorumlusu veya veri işleyen kategorilerini temsil eden diğer organlar, bu Tüzük'ün aşağıdaki hususlarla ilgili olarak uygulanmasını detaylandırmak amacıyla davranış kuralları hazırlayabilir veya bu kuralları değiştirebilir ya da bunların kapsamını genişletebilir:

(a) adil ve şeffaf işleme;

(b) veri sorumluları tarafından spesifik bağlamlarda gözetilen meşru menfaatler;

(c) kişisel verilerin toplanması;

(d) kişisel verilerde takma ad kullanımı;

(e) kamuya ve veri öznelerine sağlanan bilgiler;

(f) veri öznelerinin haklarının kullanımı;

(g) çocuklara sağlanan bilgiler ve çocukların korunması ve çocuklar üzerinde velayet hakkına sahip olanların rızasının alınma şekli;

(h) 24 ve 25. maddelerde atıfta bulunulan tedbirler ve usuller ile 32. maddede atıfta bulunulan işlemenin güvenliğinin sağlanmasına yönelik tedbirler.

(i) kişisel veri ihlallerinin denetim makamlarına bildirilmesi ve bu tür kişisel veri ihlalleri hakkında veri öznelerinin bilgilendirilmesi;

(j) kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması veya

(k) 77 ve 79. maddeler uyarınca veri öznelerinin haklarına halel gelmeksizin, veri sorumluları ve veri işleyenler arasında uyuşmazlıkların çözümüne yönelik mahkeme dışı usuller ve diğer uyuşmazlık çözüm yolları.

3. Bu Tüzük'e tabi veri sorumluları veya veri işleyenlerin uygun hareket etmesine ek olarak, 46(2) maddesinin (e) bendinde atıfta bulunulan koşullar çerçevesinde üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları çerçevesinde uygun güvenceler sağlanması amacıyla, bu maddenin 5. paragrafı uyarınca onaylanan ve bu maddenin 9. paragrafı uyarınca genel geçerliliğe sahip davranış kurallarına, 3. madde uyarınca bu Tüzük'e tabi olmayan veri sorumluları veya veri işleyenler tarafından da uyulabilir. Söz konusu veri sorumluları veya veri işleyenler, veri öznelerinin hakları ile ilgili olanlar da dâhil olmak üzere, uygun güvenceleri uygulamak amacıyla sözleşmeden doğan veya hukuken bağlayıcı diğer belgeler vasıtasıyla bağlayıcı ve uygulanabilir taahhütlerde bulunur.

4. Bu maddenin 2. paragrafında atıfta bulunulan davranış kuralları, 55 veya 56. maddeler uyarınca yetkili denetim makamlarının görev ve yetkilerine halel gelmeksizin, 41(1) maddesinde atıfta bulunulan organın, davranış kurallarını uygulamayı üstlenen veri sorumluları veya veri işleyenler tarafından söz konusu hükümlere uygunluğun zorunlu olarak izlenmesini sağlayan mekanizmaları içerir.

5. Bu maddenin 2. paragrafında atıfta bulunulan ve davranış kuralları hazırlamayı veya mevcut kuralları değiştirmeyi ya da mevcut kuralların kapsamını genişletmeyi amaçlayan birlikler ve

diğer organlar, taslak kuralları, kurallarda yapılan değişikliği veya kapsamı genişletilmiş kuralları 55. madde uyarınca yetkili denetim makamına sunar. Denetim makamı, taslağın, değişikliğin veya kapsamı genişletilmiş kuralların bu Tüzük ile uyumlu olup olmadığı konusunda bir görüş sunar ve yeterli uygun güvenceleri sağladığını tespit etmesi durumunda, söz konusu taslağı, değişikliği veya kapsamı genişletilmiş kuralları onaylar.

6. Taslağın veya değişikliğin ya da kapsamı genişletilmiş kuralların 5. paragraf uyarınca onaylandığı hâllerde ve ilgili davranış kurallarının çeşitli Üye Devletlerdeki işleme faaliyetleri ile ilgili olmadığı hâllerde, denetim makamı kuralları tescil eder ve yayımlar.

7. Davranış kurallarına ilişkin bir taslağın çeşitli Üye Devletlerdeki işleme faaliyetleri ile ilgili olduğu hâllerde, 55. madde uyarınca yetkili denetim makamı, taslağı, değişikliği ya da kapsamı genişletilmiş kuralları onaylamadan önce, söz konusu taslağın, değişikliğin veya kapsamın genişletilmesinin bu Tüzük ile uyumlu olup olmadığına veya bu maddenin 3. paragrafında atıfta bulunulan durumda uygun güvenceler sağlayıp sağlamadığına ilişkin bir görüş sunan taslağı Kurula 63. maddede atıfta bulunulan usul çerçevesinde ibraz eder.

8. 7. paragrafta atıfta bulunulan görüşün, taslak kuralların, değişikliğin veya kapsamı genişletilmiş kuralların bu Tüzük ile uyumlu olduğunu veya 3. paragrafta atıfta bulunulan durumda uygun güvenceler sağladığını teyit ettiği hâllerde, Kurul görüşünü Komisyona sunar.

9. Komisyon, bu maddenin 8. paragrafı uyarınca kendisine sunulan onaylı davranış kurallarının, kurallarda yapılan değişikliğin veya kapsamı genişletilmiş kuralların Birlik içinde genel geçerliliğe sahip olduğuna uygulama tasarrufları vasıtasıyla karar verebilir. Bu uygulama tasarrufları, 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

10. Komisyon 9. paragraf uyarınca genel geçerliliği olduğuna karar verilen onaylı kuralların uygun şekilde ilan edilmesini sağlar.

11. Kurul, onaylı tüm davranış kurallarını, kurallarda yapılan değişiklikleri ve kapsamı genişletilmiş kuralları bir sicilde toplar ve uygun yollarla kamunun erişimine açar.

Madde 41

Onaylı davranış kurallarının izlenmesi

1. Yetkili denetim makamının 57 ve 58. maddeler kapsamındaki görev ve yetkilerine halel gelmeksizin, 40. madde uyarınca davranış kurallarına uyumun izlenmesi, kuralların konusu ile ilgili uygun düzeyde uzmanlığa sahip olan ve bu amaca yönelik olarak yetkili denetim makamı tarafından akredite edilen bir organ tarafından gerçekleştirilebilir.

2. 1. paragrafta atıfta bulunulan bir organ, aşağıdaki özellikleri taşıması hâlinde, davranış kurallarına uyumun izlenmesi amacıyla akredite edilebilir:

(a) kuralların konusuna ilişkin bağımsızlığını ve uzmanlığını yetkili denetim makamını tatmin edecek şekilde göstermiş olması;

(b) ilgili veri sorumlularının ve veri işleyenlerin davranış kurallarını uygulama konusundaki yeterliliklerini değerlendirmesine, bu kuralların hükümlerine uyumun izlenmesine ve kuralların işleyişini düzenli olarak gözden geçirmesine olanak tanıyan usulleri tesis etmesi;

(c) kuralların ihlaline veya bir veri sorumlusu ya da veri işleyen tarafından uygulanma şekline ilişkin şikayetlerin ele alınması ve söz konusu usullerin ve yapıların veri öznelerine ve kamuya şeffaf hale getirilmesi hususunda usuller ve yapılar oluşturmuş olması ve

(d) görev ve sorumlulukların bir çıkar çatışmasına neden olmadığını yetkili denetim makamını tatmin edecek şekilde göstermiş olması.

3. Yetkili denetim makamı, bu maddenin 1. paragrafında atıfta bulunulan bir organın akreditasyonuna ilişkin taslak kriterleri, 63. maddede atıfta bulunulan tutarlılık mekanizması uyarınca Kurula sunar.

4. Yetkili denetim makamının görev ve yetkileri ile VIII. Bölümün hükümlerine halel gelmeksizin, bu maddenin 1. paragrafında atıfta bulunulan bir organ, kuralların bir veri sorumlusu veya veri işleyen tarafından ihlal edilmesi halinde, uygun güvencelere tabi olarak, ilgili veri sorumlusu veya veri işleyenin kurallardan geçici olarak uzaklaştırılması veya çıkarılması da dâhil olmak üzere uygun adımları atar. Söz konusu organ, bu tür eylemler ve bunların gerçekleştirilme sebepleri konusunda yetkili denetim makamına bilgi verir.

5. Akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmeyeceği durumlarda ya da organ tarafından gerçekleştirilen eylemlerin bu Tüzük'ü ihlal ettiği hâllerde, yetkili denetim makamı 1. paragrafta atıfta bulunulduğu üzere bir organın akreditasyonunu iptal eder.

6. Bu madde, kamu makamları ve organları tarafından gerçekleştirilen işlemeye uygulanmaz.

Madde 42

Belgelendirme

1. Üye Devletler, denetim makamları, Kurul ve Komisyon, veri sorumluları ve veri işleyenler tarafından gerçekleştirilen işleme faaliyetlerinin bu Tüzük'e uygunluğunu göstermek amacıyla, özellikle Birlik düzeyinde, veri koruma belgelendirme mekanizmalarının ve veri koruma mühürleri ve işaretlerinin oluşturulmasını teşvik ederler. Mikro, küçük ve orta ölçekli işletmelerin özel ihtiyaçları dikkate alınır.

2. Bu Tüzük'e tabi veri sorumluları veya veri işleyenlerin uygun hareket etmesine ek olarak, bu maddenin 5. paragrafı uyarınca onaylanan veri koruma belgelendirme mekanizmaları, mühürler ya da işaretler, 46(2) maddesinin (f) bendinde atıfta bulunulan koşullar uyarınca üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları çerçevesinde, 3. madde uyarınca bu Tüzük'e tabi olmayan veri sorumluları veya veri işleyenler tarafından sağlanan uygun güvencelerin mevcut olduğunun gösterilmesi amacıyla oluşturulabilir. Söz konusu veri sorumluları veya veri işleyenler, veri öznelerinin hakları ile ilgili olanlar da dâhil olmak üzere, uygun güvenceleri uygulamak üzere sözleşmeden doğan veya hukuken bağlayıcı diğer belgeler vasıtasıyla bağlayıcı ve uygulanabilir taahhütlerde bulunur.

3. Belgelendirme, gönüllülük esasına dayanır ve şeffaf bir süreç vasıtasıyla sağlanır.

4. Bu madde uyarınca sağlanan bir belgelendirme, veri sorumlusu ya da veri işleyenin bu Tüzük'e uyma sorumluluğunu azaltmaz ve 55 veya 56. madde uyarınca yetkili denetim makamlarının görevleri ve yetkilerine halel getirmez.

5. Bu madde uyarınca sağlanan bir belgelendirme, 43. maddede atıfta bulunulan belgelendirme organları veya yetkili denetim makamı tarafından, 58(3) madde uyarınca söz konusu yetkili denetim makamı veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere dayalı olarak sağlanır. Kriterlerin Kurul tarafından onaylandığı hâllerde, ortak bir belgelendirme olan Avrupa Veri Koruma Mührü verilebilir.

6. İşlemeyi, belgelendirme mekanizmasına sunan veri sorumlusu veya veri işleyen, belgelendirme usulünün yürütülmesi için gereken tüm bilgileri ve işleme faaliyetlerine erişimi, 43. maddede atıfta bulunulan belgelendirme organına veya uygun olduğu hâllerde, yetkili denetim makamına sağlar.

7. Belgelendirme, bir veri sorumlusu veya veri işleyene azami üç yıllık bir süre için sağlanır ve ilgili gerekliliklerin karşılanmasına devam edilmesi şartıyla, aynı koşullar altında, yenilenebilir.

Belgelendirme gerekliliklerinin karşılanmadığı veya daha fazla karşılanmadığı durumda, belgelendirme, uygun olduğu hâllerde, 43. maddede atıfta bulunulan belgelendirme organları veya yetkili denetim makamı tarafından geri çekilir.

8. Kurul, tüm belgelendirme mekanizmaları ve veri koruma mühürleri ile işaretlerini bir sicilde toplar ve uygun yollarla kamuya açık hale getirir.

Madde 43

Belgelendirme organları

1. Yetkili denetim makamının 57 ve 58. maddeler kapsamındaki görev ve yetkilerine halel gelmeksizin, veri koruma ile ilgili uygun bir uzmanlık seviyesine sahip olan belgelendirme organları, denetim makamını, gerektiğinde 58(2) maddesinin (h) bendi uyarınca yetkilerini kullanmasını sağlamak üzere bilgilendirdikten sonra, belgelendirme sağlar ve belgelendirmeyi yeniler. Üye Devletler, bu belgelendirme organlarının aşağıdakilerin biri veya her ikisi tarafından akredite edilmesini sağlarlar:

(a) 55 veya 56. maddeler uyarınca yetkili denetim makamı;

(b) EN-ISO/IEC 17065/2012'ye uygun olarak (AT) 765/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü[20] uyarınca ve 55 ya da 56. maddeler uyarınca yetkili olan denetim makamı tarafından belirlenen ek gerekliliklere göre belirlenen ulusal akreditasyon organı.

2. 1. paragrafta atıfta bulunulan belgelendirme organları ancak aşağıdaki özellikleri taşımaları hâlinde, söz konusu paragraf uyarınca akredite edilir:

(a) belgelendirme konusuna ilişkin bağımsızlıkları ve uzmanlıklarını yetkili denetim makamını tatmin edecek şekilde göstermiş olmaları;

(b) 42(5) maddesinde atıfta bulunulan ve 55 veya 56. maddeler uyarınca yetkili olan denetim makamı tarafından veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere riayet etmeyi taahhüt etmiş olmaları;

(c) veri koruma belgelendirmesi, mühürleri ve işaretlerinin verilmesi, düzenli aralıklarla gözden geçirilmesi ve geri çekilmesine ilişkin usuller oluşturmuş olmaları;

(d) belgelendirmeye ilişkin ihlallere veya veri sorumlusunun ya da veri işleyenin belgelendirmeyi uygulama şekline yönelik şikayetlerin ele alacak ve söz konusu usullerin ve yapıların veri özneleri ile kamuoyu bakımından şeffaf hale getirecek usul ve yapıları tesis etmeleri ve

(e) görev ve sorumluluklarının bir çıkar çatışmasına neden olmadığını yetkili denetim makamını tatmin edecek şekilde göstermiş olmaları.

3. Bu maddenin 1 ve 2. paragraflarında atıfta bulunulduğu üzere, belgelendirme organlarının akreditasyonu 55 veya 56. maddeler uyarınca yetkili olan denetim makamı tarafından veya 63. madde uyarınca Kurul tarafından onaylanan kriterlere dayalı olarak gerçekleşir. Bu maddenin 1. paragrafının (b) bendi uyarınca akreditasyon yapılması hâlinde, bu gereklilikler (AT)

[20] (AET) 339/93 sayılı Tüzük'ü yürürlükten kaldıran ve ürünlerin pazarlanması ile ilgili akreditasyon ve piyasa gözetimi gerekliliklerini belirleyen 9 Temmuz 2008 tarihli ve (AT) 765/2008 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ABRG L 218, 13.8.2008, s.30).

765/2008 sayılı Tüzük'te öngörülen gereklilikleri ve belgelendirme organlarının yöntem ve usullerinin açıklandığı teknik kuralları tamamlar.

4. 1. paragrafta atıfta bulunulan belgelendirme organları, veri sorumlusu veya veri işleyenin bu Tüzük'e uyma sorumluluğuna halel gelmeksizin, belgelendirmeye veya belgelendirmenin geri çekilmesine yol açan uygun bir değerlendirmeden sorumludur. Akreditasyon, azami beş yıllık bir süre için verilir ve belgelendirme organının bu maddede belirtilen gereklilikleri yerine getirmesi şartıyla, aynı koşullar altında, yenilenebilir.

5. 1. paragrafta atıfta bulunulan belgelendirme organları, talep edilen belgelendirmenin verilmesi veya geri çekilmesine ilişkin sebepleri yetkili denetim makamına sağlar.

6. Bu maddenin 3. paragrafında atıfta bulunulan gereklilikler ve 42(5) maddesinde atıfta bulunulan kriterler, denetim makamı tarafından kolayca erişilebilecek bir şekilde kamuya açıklanır. Denetim makamları bu gereklilikleri ve kriterleri Kurula da iletir. Kurul, tüm belgelendirme mekanizmalarını ve veri koruma mühürlerini bir sicilde toplar ve uygun yollarla kamuoyuna açıklar.

7. VIII. Bölüme halel gelmeksizin, akreditasyon koşullarının yerine getirilmediği veya artık yerine getirilmeyeceği durumlarda veya bir belgelendirme organı tarafından gerçekleştirilen eylemlerin bu Tüzük'ü ihlal ettiği hâllerde, yetkili denetim makamı veya ulusal akreditasyon organı, bu maddenin 1. paragrafı uyarınca bir belgelendirme organının akreditasyonunu iptal eder.

8. Komisyon, 42(1) maddesinde atıfta bulunulan veri koruma belgelendirme mekanizmaları için dikkate alınacak gerekliliklerin belirtilmesi amacıyla 92. madde uyarınca yetki devrine dayanan tasarrufları kabul etme yetkisine sahiptir.

9. Komisyon, belgelendirme mekanizmaları ve veri koruma mühürleri ve işaretleri ile bu belgelendirme mekanizmaları, mühürleri ve işaretlerinin tanıtılması ve tanınmasıyla ilgili mekanizmalara ilişkin teknik standartları belirleyen uygulama tasarrufları kabul edebilir. Bu uygulama tasarrufları, 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

BÖLÜM V

Üçüncü ülkeler veya uluslararası kuruluşlara kişisel veri aktarımları

Madde 44

Aktarımlar için genel ilke

İşlenmekte olan veya bir üçüncü ülkeye veya bir uluslararası kuruluşa aktarılmasının ardından işlenmesi amaçlanan kişisel verilerin aktarılması, üçüncü ülkeden veya bir uluslararası kuruluştan başka bir üçüncü ülke veya başka bir uluslararası kuruluşa yönelik tekrar aktarımlar da dâhil olmak üzere, ancak bu Tüzük'ün diğer hükümleri saklı kalmak kaydıyla bu Bölümde belirtilen koşullara veri sorumlusu ve veri işleyen tarafından uyulması halinde gerçekleşir. Bu Bölümdeki tüm hükümler, bu Tüzük ile güvence altına alınan gerçek kişilerin korunma düzeyine zarar verilmemesini sağlamak amacıyla uygulanır.

Madde 45

Bir yeterlilik kararına dayalı olarak yapılan aktarımlar

1. Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dâhilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma

sağladığına karar verdiği hâllerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir. Böylesi bir aktarım için, herhangi bir özel onay gerekmez.

2. Komisyon koruma düzeyinin yeterliliğini değerlendirirken, özellikle aşağıdaki hususları dikkate alır:

(a) hukukun üstünlüğü, insan haklarına ve temel özgürlüklere saygı, kamu güvenliği, savunma, milli güvenlik ve ceza hukuku ile kamu makamlarının kişisel verilere erişimi de dâhil olmak üzere, ilgili genel ve sektörel mevzuatın yanı sıra, söz konusu mevzuatın uygulanması, kişisel verilerin başka bir üçüncü ülke veya uluslararası kuruluşa tekrar aktarımı hakkında o ülke veya uluslararası kuruluşta riayet edilen kurallar da dâhil olmak üzere, veri koruma kuralları, mesleki kurallar ve güvenlik tedbirleri, içtihat, etkili ve uygulanabilir veri öznesi hakları ile kişisel verileri aktarılan veri öznelerine yönelik etkili idari ve adli şikayet;

(b) üçüncü ülkede bulunan veya bir uluslararası kuruluşun tabi olduğu, yeterli uygulama yetkileri de dâhil olmak üzere veri koruma kuralları ile uyumluluğu sağlamak ve uygulamak, haklarının kullanılması hususunda veri öznelerine destek olmak ve tavsiyede bulunmak ve Üye Devletlerin denetim makamları ile iş birliği yapmakla sorumlu olan bir veya daha fazla sayıda bağımsız denetim makamının varlığı ve etkili bir şekilde işleyişi; ve

(c) ilgili üçüncü ülke veya uluslararası kuruluşun üstlendiği uluslararası taahhütler veya hukuken bağlayıcı sözleşmeler veya belgelerin yanı sıra, kişisel verilerin korunması ile ilgili olanlar başta olmak üzere çok taraflı veya bölgesel sistemlere katılımından kaynaklanan diğer yükümlülükler.

3. Komisyon, koruma düzeyinin yeterliliğini değerlendirdikten sonra, uygulama tasarrufu vasıtasıyla, bir üçüncü ülkenin, bir üçüncü ülke içindeki bir bölgenin veya bir ya da daha fazla belirli sektörün ya da bir uluslararası kuruluşun bu maddenin 2. paragrafı bağlamında yeterli bir koruma düzeyi sağladığına karar verebilir. Uygulama tasarrufu, en az dört yılda bir olmak üzere, üçüncü ülke veya uluslararası kuruluştaki ilgili tüm gelişmeleri dikkate alacak bir periyodik gözden geçirme mekanizması öngörür. Uygulama tasarrufunda bunun bölgesel ve sektörel uygulaması belirtilir ve uygun olduğu hallerde, bu maddenin 2. paragrafının (b) bendinde atıfta bulunulan denetim makamı veya makamları tanımlanır. Bu uygulama tasarrufu, 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

4. Komisyon, bu maddenin 3. paragrafı uyarınca kabul edilen kararların ve 95/46/AT sayılı Direktif'in 25(6) maddesi çerçevesinde kabul edilen kararların işleyişini etkileyebilecek olan, üçüncü ülkelerdeki ve uluslararası kuruluşlardaki gelişmeleri sürekli olarak izler.

5. Özellikle bu maddenin 3. paragrafında atıfta bulunulan gözden geçirmenin ardından, mevcut bilgilerin bir üçüncü ülkenin, bir üçüncü ülke içindeki bir bölgenin veya bir ya da daha fazla belirli sektörün ya da bir uluslararası kuruluşun, bu maddenin 2. paragrafı bağlamında artık yeterli bir koruma düzeyi sağlamadığını göstermesi durumunda, Komisyon geriye dönük etkisi olmayan uygulama tasarrufları vasıtasıyla bu maddenin 3. paragrafında atıfta bulunulan kararı gereken ölçüde yürürlükten kaldırır, değiştirir veya askıya alır. Bu uygulama tasarrufları, 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

Usulüne uygun şekilde gerekçelendirilmiş zorunlu acil gerekçelerle, Komisyon 93(3) maddesinde atıfta bulunulan usule uygun olarak gecikmeksizin uygulanabilir uygulama tasarruflarını kabul eder.

6. Komisyon, 5. paragraf uyarınca alınan karara yol açan durumun düzeltilmesi amacıyla üçüncü ülke veya uluslararası kuruluşla istişarelerde bulunur.

7. Bu maddenin 5. paragrafı uyarınca verilen bir karar, kişisel verilerin üçüncü ülkeye, söz konusu üçüncü ülke dâhilindeki bir bölgeye veya belirli bir ya da daha fazla sektöre ya da uluslararası kuruluşa 46 ila 49. maddeler uyarınca aktarılmasına halel getirmez.

8. Komisyon, yeterli düzeyde koruma sağlandığına veya artık sağlanmadığına karar verdiği üçüncü ülkeleri, bir üçüncü ülke içindeki bölgeleri ve belirli sektörleri ve uluslararası kuruluşları içeren bir listeyi *Avrupa Birliği Resmi Gazetesi* ve internet sitesinde yayımlar.

9. 95/46/AT sayılı Direktif'in 25(6) maddesine dayalı olarak Komisyon tarafından kabul edilen kararlar, bu maddenin 3 veya 5. paragrafı uyarınca kabul edilen bir Komisyon Kararı ile tadil edilene, yerine yenisi alınana veya yürürlükten kaldırılana kadar yürürlükte kalır.

Madde 46

Uygun güvencelere tabi olarak yapılan aktarımlar

1. 45(3) maddesi uyarınca bir kararın bulunmaması hâlinde, ancak veri sorumlusu veya veri işleyenin uygun güvenceler sağlamış olması hâlinde ve uygulanabilir veri öznesi haklarının ve veri öznelerine yönelik etkili hukuk yollarının mevcut olması koşuluyla, söz konusu veri sorumlusu veya veri işleyen bir üçüncü ülke veya bir uluslararası kuruluşa kişisel veri aktarabilir.

2. 1. paragrafta atıfta bulunulan uygun güvenceler, bir denetim makamından özel izin alınmasına gerek olmaksızın, aşağıdaki yollarla sağlanabilir:

(a) kamu makamları veya organları arasında hukuki bağlayıcılığı bulunan ve uygulanabilir bir belge;

(b) 47. madde uyarınca bağlayıcı şirket kuralları;

(c) 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca Komisyon tarafından kabul edilen standart veri koruma hükümleri;

(d) 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma hükümleri;

(e) 40. madde uyarınca onaylı davranış kuralları ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin, veri öznesinin hakları ile ilgili olanlar da dâhil olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri veya

(f) 42. madde uyarınca onaylı bir belgelendirme mekanizması ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin, veri öznesinin hakları ile ilgili olanlar da dâhil olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri.

3. Yetkili denetim makamından alınan izne tabi olarak, 1. paragrafta atıfta bulunulan uygun güvenceler, özellikle aşağıdakilerle de sağlanabilir:

(a) Veri sorumlusu veya veri işleyen ile üçüncü ülke ya da uluslararası kuruluştaki veri sorumlusu, veri işleyen ya da kişisel verilerin alıcısı arasındaki sözleşme hükümleri veya

(b) kamu makamları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri öznesi hakları içeren hükümler.

4. Denetim makamı, bu maddenin 3. paragrafında atıfta bulunulan hallerde 63. maddede atıfta bulunulan tutarlılık mekanizmasını uygular.

5. 95/46/AT sayılı Direktif'in 26(2) maddesine dayalı olarak bir Üye Devlet veya denetim makamı tarafından verilen izinler, gerektiğinde söz konusu denetim makamı tarafından tadil edilene, yerine yenisi alınana veya yürürlükten kaldırılana kadar geçerliliğini korur. 95/46/AT

sayılı Direktif'in 26(4) maddesine dayalı olarak Komisyon tarafından kabul edilen kararlar, gerektiğinde bu maddenin 2. paragrafı uyarınca kabul edilen bir Komisyon Kararı ile tadil edilene, yerine yenisi alınana veya yürürlükten kaldırılana kadar yürürlükte kalır.

Madde 47

Bağlayıcı şirket kuralları

1. 63. maddede yer alan tutarlılık mekanizması uyarınca, yetkili denetim makamı, bağlayıcı şirket kurallarını, aşağıdaki koşulları sağlamaları şartıyla, onaylar:

(a) yasal bağlayıcılığının olması ve çalışanları da dâhil olmak üzere, teşebbüsler grubunun veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun ilgili her üyesi için uygulanması ve bu üyeler tarafından yürütülmesi;

(b) veri öznelerine kişisel verilerinin işlenmesi ile ilgili olarak açık bir şekilde uygulanabilir haklar vermesi ve

(c) 2. paragrafta belirtilen gereklilikleri yerine getirmesi.

2. 1. paragrafta atıfta bulunulan bağlayıcı şirket kurallarında asgari aşağıdakiler belirlenir:

(a) teşebbüsler grubunun veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun ve bu grupların her üyesinin yapısı ve irtibat bilgileri;

(b) kişisel veri kategorileri, işleme türü ve amaçları, etkilenen veri öznelerinin türü ve söz konusu üçüncü ülke veya ülkelerin belirlenmesi de dâhil olmak üzere veri aktarımları veya aktarım seti;

(c) bunların hem içeride hem de dışarda hukuki olarak bağlayıcı niteliği;

(d) amaç sınırlaması, veri minimizasyonu, sınırlı depolama süreleri, veri kalitesi, tasarımdan itibaren ve varsayılan olarak veri koruma, işlemeye yönelik yasal dayanak, özel kategorilerdeki kişisel verilerin işlenmesi, veri güvenliğinin sağlanmasına ilişkin tedbirler ve bağlayıcı şirket kurallarıyla bağlı bulunmayan organlara tekrar aktarımlara ilişkin gerekliliklerin uygulanması başta olmak üzere genel veri koruma ilkeleri;

(e) 22. madde uyarınca profilleme de dâhil olmak üzere yalnızca otomatik işlemeye dayalı kararlara tabi olmama hakkı, 79. madde uyarınca yetkili denetim makamına ve Üye Devletlerin yetkili mahkemelerine şikâyette bulunma ve bağlayıcı şirket kurallarına ilişkin bir ihlalden dolayı şikâyet hakkı ve uygun olduğu hallerde tazminat hakkı da dâhil olmak üzere veri öznelerinin işlemeye ilişkin hakları ve bu hakları kullanma yöntemleri;

(f) Birlik içinde yerleşik olmayan herhangi bir üye tarafından bağlayıcı şirket kuralların ihlalinde bir Üye Devlet'in topraklarında yerleşik veri sorumlusu veya veri işleyenin sorumluluğu üstüne alması; veri sorumlusu veya veri işleyen, yalnızca söz konusu üyenin zarara neden olan olaydan sorumlu olmadığını kanıtlaması durumunda, bu sorumluluktan tamamen veya kısmen muaf tutulur;

(g) 13 ve 14. maddelere ek olarak, bu paragrafın (d), (e) ve (f) bentlerinde atıfta bulunulan hükümler başta olmak üzere bağlayıcı şirket kurallarına ilişkin bilgilerin veri öznelerine nasıl sağlandığı;

(h) eğitim ile şikâyetlerin ele alınmasının izlenmesi dâhil olmak üzere, 37. madde uyarınca belirlenen veri koruma görevlilerinin ya da teşebbüsler grubu veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun bağlayıcı şirket kurallarına uyumunun izlenmesinden sorumlu olan diğer kişilerin veya teşekküllerin görevleri;

(i) şikâyet usulleri;

(j) teşebbüsler grubu veya ortak bir ekonomik faaliyette bulunan işletmeler grubu içinde bağlayıcı şirket kurallarına uyumun doğrulanmasının sağlanmasına yönelik mekanizmalar. Söz konusu mekanizmalar, veri öznesinin haklarının korunmasına yönelik düzeltici eylemlerin sağlanmasına ilişkin veri koruma denetimlerini ve yöntemlerini kapsar. Bu doğrulamanın sonuçları, (h) bendinde atıfta bulunulan kişi veya teşekküle ve bir teşebbüsler grubunun veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun idare eden teşebbüsünün yönetim kuruluna iletilmeli ve yetkili denetim makamına, talebi üzerine sunulmalıdır;

(k) kurallara ilişkin değişikliklerin raporlanması ve kaydedilmesine ve bu değişikliklerin denetim makamına raporlanmasına ilişkin mekanizmalar;

(l) özellikle (j) bendinde atıfta bulunulan tedbirlere ilişkin doğrulamaların sonuçlarının denetim makamına sunulması suretiyle, teşebbüsler grubunun veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun herhangi bir üyesi tarafından uyumun sağlanması amacıyla denetim makamı ile kurulan iş birliği mekanizması;

(m) teşebbüsler grubunun veya ortak bir ekonomik faaliyette bulunan işletmeler grubunun bir üyesinin bir üçüncü ülkede tabi olduğu ve bağlayıcı şirket kurallarının sağladığı teminatlar açısından kayda değer bir olumsuz etki yaratması muhtemel olan yasal gerekliliklerin yetkili denetim makamına raporlanmasına ilişkin mekanizmalar ve

(n) kişisel verilere kalıcı veya düzenli olarak erişimi bulunan personele yönelik uygun veri koruma eğitimi.

3. Komisyon, bu madde çerçevesinde veri sorumluları, veri işleyenler ve denetim makamları arasında bağlayıcı şirket kurallarına yönelik bilgi alışverişine ilişkin format ve usulleri belirtebilir. Bu uygulama tasarrufları, 93(2) maddesinde atıfta bulunulan inceleme usulüne uygun olarak kabul edilir.

Madde 48

Birlik hukuku çerçevesinde izin verilmeyen aktarımlar veya açıklamalar

Bir veri sorumlusunun veya veri işleyenin kişisel verileri aktarmasının veya açıklamasının istendiği, bir üçüncü ülkenin herhangi bir mahkeme veya heyet kararı ve idari bir makamının herhangi bir kararı, bu Bölüm uyarınca diğer aktarım sebeplerine halel gelmeksizin, ancak talepte bulunan üçüncü ülke ile Birlik ya da bir Üye Devlet arasında yürürlükte bulunan bir karşılıklı hukuki yardım antlaşması gibi bir uluslararası anlaşmaya dayanması hâlinde, herhangi bir şekilde tanınabilir veya uygulanabilir.

Madde 49

Özel durumlara yönelik derogasyonlar

1. 45(3) maddesi uyarınca bir yeterlilik kararının veya bağlayıcı şirket kuralları da dâhil olmak üzere 46. madde uyarınca uygun güvencelerin olmaması durumunda, kişisel verilerin bir üçüncü ülkeye veya bir uluslararası kuruluşa aktarılması veya aktarım seti ancak aşağıdaki şartlardan biriyle gerçekleşir:

(a) veri öznesinin, bir yeterlilik kararı ve uygun güvencelerin bulunmaması nedeniyle, söz konusu aktarımların, kendisine yönelik olası riskleri hususunda bilgilendirilmesinin ardından, önerilen aktarıma açık bir şekilde rıza vermesi;

(b) aktarımın veri öznesi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya veri öznesinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması açısından gerekli olması;

(c) aktarımın veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında veri öznesi yararına yapılan bir sözleşmenin imzalanması veya ifası açısından gerekli olması;

(d) aktarımın kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması;

(e) aktarımın hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması açısından gerekli olması;

(f) veri öznesinin fiziksel veya hukuki olarak rıza gösteremeyecek durumda olması hâlinde, aktarımın veri öznesi veya diğer kişilerin hayati menfaatlerinin korunması açısından gerekli olması;

(g) Aktarımın, Birlik veya Üye Devlet hukukuna göre kamuya bilgi sağlanmasının amaçlandığı ve genel olarak kamunun veya meşru bir menfaati bulunan herhangi bir kişinin, fakat Birlik veya Üye Devlet hukuku çerçevesinde müracaata yönelik olarak ortaya konan koşullar ilgili durumda yerine getirildiği ölçüde, müracaatına açık olan bir sicilden yapılması.

Bir aktarımın bağlayıcı şirket kurallarına ilişkin hükümler de dâhil olmak üzere 45 veya 46. maddedeki bir hükme dayanmadığı ve bu paragrafın ilk alt paragrafında atıfta bulunulan özel bir duruma ilişkin derogasyonların herhangi birinin uygulanabilir olmadığı hallerde, ancak; aktarımın yinelemeli olmaması, yalnızca sınırlı sayıda veri öznesini ilgilendirmesi, veri sorumlusu tarafından gözetilen ve karşısında veri öznesinin menfaatleri veya hakları ile özgürlüklerinin ağır basmadığı zorlayıcı meşru menfaatler doğrultusunda gerekli olması ve veri sorumlusunun veri aktarımı ile ilgili tüm koşulları değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olması durumunda, bir üçüncü ülke veya bir uluslararası kuruluşa yönelik bir aktarım gerçekleşebilir. Veri sorumlusu, denetim makamını aktarım hususunda bilgilendirir. Veri sorumlusu, 13 ve 14. maddelerde atıfta bulunulan bilgilerin sağlanmasına ek olarak, veri öznesini aktarım ve gözetilen zorlayıcı meşru menfaatler hususunda bilgilendirir.

2. 1. paragrafın ilk alt paragrafının (g) bendi uyarınca yapılacak bir aktarımda sicilde bulunan tüm kişisel verilere veya tüm kişisel veri kategorilerine yer verilmez. Sicilin, meşru bir menfaati bulunan kişilerin müracaatı amacıyla oluşturulduğu durumlarda, aktarım yalnızca bu kişilerin talebi üzerine veya bu kişilerin alıcı olması hâlinde yapılır.

3. 1. paragrafın ilk alt paragrafının (a), (b) ve (c) bentleri ve ikinci alt paragrafı kamu yetkilerinin kullanılmasında kamu makamları tarafından gerçekleştirilen faaliyetlere uygulanmaz.

4. 1. paragrafın ilk alt paragrafının (d) bendinde atıfta bulunulan kamu yararı, Birlik hukukunda veya veri sorumlusunun tabi olduğu Üye Devlet hukukunda tanınır.

5. Bir yeterlilik kararı olmaması durumunda, kamu yararına ilişkin önemli sebepler nedeniyle, Birlik veya Üye Devlet hukukunda belirli kategorilerdeki kişisel verilerin bir üçüncü ülkeye veya bir uluslararası kuruluşa aktarılmasına ilişkin sınırlar açık bir şekilde konabilir. Üye Devletler söz konusu hükümleri Komisyona bildirir.

6. Veri sorumlusu veya veri işleyen bu maddenin 1. paragrafının ikinci alt paragrafında atıfta bulunulan değerlendirmeyi ve uygun güvenceleri 30. maddede atıfta bulunulan kayıtlarda belgelendirir.

Madde 50

Kişisel verilerin korunmasına yönelik uluslararası iş birliği

Üçüncü ülkeler ve uluslararası kuruluşlar ile ilgili olarak, Komisyon ve denetim makamları şunlara yönelik uygun adımları atar:

(a) kişisel verilerin korunmasına yönelik mevzuatın etkili bir şekilde uygulanmasının kolaylaştırılması için uluslararası iş birliği mekanizmalarının geliştirilmesi;

(b) kişisel verilerin ve diğer temel haklar ile özgürlüklerin korunmasına yönelik uygun güvencelere tabi olarak; bildirimle, şikâyet yönlendirmeyle, soruşturma desteğiyle ve bilgi alışverişi yoluyla dâhil, kişisel verilerin korunmasına yönelik mevzuatın uygulanması hususunda karşılıklı uluslararası yardım sağlanması;

(c) ilgili paydaşların, kişisel verilerin korunmasına yönelik mevzuatın uygulanmasında uluslararası iş birliğinin ilerletilmesini amaçlayan görüşmelere ve faaliyetlere dâhil edilmesi;

(d) üçüncü ülkelerle yargı yetkisine ilişkin ihtilaflar da dâhil olmak üzere kişisel veri koruma mevzuatı ve uygulamasının paylaşımı ve belgelendirmesinin teşvik edilmesi.

BÖLÜM VI

Bağımsız denetim makamları

Kesim 1

Bağımsız statü

Madde 51

Denetim makamı

1. Her Üye Devlet, gerçek kişilerin işleme ile ilgili temel hakları ve özgürlüklerini korumak ve Birlik içinde kişisel verilerin serbest akışını kolaylaştırmak üzere, bir ya da daha fazla sayıda bağımsız kamu makamının bu Tüzük'ün uygulamasının izlenmesinden sorumlu olmasını sağlar ("denetim makamı").

2. Her denetim makamı bu Tüzük'ün Birlik içinde tutarlı bir şekilde uygulanmasına katkıda bulunur. Bu amaç doğrultusunda, denetim makamları VII. Bölüm uyarınca birbirleriyle ve Komisyon ile iş birliği yapar.

3. Bir Üye Devlet'te birden fazla denetim makamının bulunduğu hallerde, söz konusu Üye Devlet bu makamları Kurulda temsil edecek denetim makamını belirler ve diğer makamların 63. maddede atıfta bulunulan tutarlılık mekanizmasına ilişkin kurallara uyumluluğunu sağlayacak mekanizmayı belirler.

4. Her Üye Devlet bu Bölüm uyarınca kabul ettiği mevzuat hükümlerini 25 Mayıs 2018 tarihine kadar ve bunları etkileyen sonraki değişiklikleri, gecikmeksizin, Komisyona bildirir.

Madde 52

Bağımsızlık

1. Her denetim makamı, bu Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsız olarak hareket eder.

2. Her denetim makamının üyesi veya üyeleri, bu Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken, doğrudan veya dolaylı dış etkilerden bağımsız hareket eder ve hiç kimseden talimat talebinde bulunmaz veya talimat almaz.

3. Her denetim makamının üyesi veya üyeleri görevlerine uygun olmayan eylemlerden kaçınır ve görev süreleri boyunca, maddi getirisi olsun ya da olmasın, bu göreve uygun olmayan hiçbir işle iştigal etmez.

4. Her Üye Devlet karşılıklı yardım, iş birliği ve Kurula katılım bağlamında gerçekleştirilecek olanlar da dâhil olmak üzere, görevlerini etkili bir şekilde yerine getirebilmeleri ve yetkilerini etkili bir şekilde kullanabilmeleri için gereken insan kaynağı, teknik ve mali kaynaklar, binalar ve altyapının her denetim makamına sağlanmasını temin eder.

5. Her Üye Devlet, her denetim makamının, ilgili denetim makamı üyesi veya üyelerinin münhasır yönlendirmesine tabi olacak personeli seçmesini ve haiz olmasını temin eder.

6. Her Üye Devlet her denetim makamının bağımsızlığını etkilemeyen bir mali kontrole tabi olmasını ve genel devlet bütçesi veya ulusal bütçenin parçası olabilecek ayrı yıllık kamu bütçelerinin bulunmasını sağlar.

Madde 53

Denetim makamının üyeleriyle ilgili genel koşullar

1. Üye Devletler, denetim makamlarının her üyesinin aşağıdaki taraflarca şeffaf bir usul vasıtasıyla atanmasını sağlar:

— parlamentoları;

— hükümetleri;

— Devlet başkanları veya

— Üye Devlet hukuku çerçevesinde atama yetkisi verilen bağımsız bir organ.

2. Her üye, özellikle kişisel verilerin korunması alanında, görevlerinin yerine getirilmesi ve yetkilerinin kullanılması için gereken nitelikler, deneyim ve becerilere sahiptir.

3. Bir üyenin görevleri, ilgili Üye Devlet hukuku uyarınca görev süresinin sona ermesi, istifa etmesi veya emekli edilmesi hâlinde sona erer.

4. Bir üye ancak ağır suiistimal hallerinde veya görevlerinin yerine getirilmesi için gereken koşulları artık sağlamaması durumunda görevden alınır.

Madde 54

Denetim makamının kurulmasına ilişkin kurallar

1. Her Üye Devlet, aşağıdakilerin tamamını mevzuatla belirler:

(a) her denetim makamının kurulması;

(b) her denetim makamının üyesi olarak atanmak için gereken nitelikler ve uygunluk koşulları;

(c) her denetim makamının üyesi veya üyelerinin atanmasına ilişkin kurallar ve usuller;

(d) aşamalı bir atama usulü vasıtasıyla denetim makamının bağımsızlığının korunması için gerekmesi durumunda, 24 Mayıs 2016 tarihinden sonra yapılacak ve bir kısmı daha kısa bir süre boyunca geçerli olabilecek ilk atama haricinde, dört yıldan az olmayacak şekilde her denetim makamının üyesi veya üyelerinin görev süresi;

(e) her denetim makamının üyesi veya üyelerinin yeniden atanıp atanamayacağı ve atanmaları halinde, kaç dönem atanabileceği;

(f) her denetim makamının üyesi veya üyeleri ile personelinin yükümlülüklerini düzenleyen koşullar, görev süresi esnasında ve sonrasında görevle bağdaşmayan eylemler, iştigal ve menfaatlere ilişkin yasaklar ve göreve son verilmesini düzenleyen kurallar.

2. Her denetim makamının üyesi veya üyeleri ile personeli, Birlik veya Üye Devlet hukuku uyarınca, hem görev süreleri esnasında hem de sonrasında, görevlerinin yerine getirilmesi veya yetkilerinin kullanımı esnasında öğrendikleri gizli bilgiler ile ilgili olarak bir mesleki gizlilik yükümlülüğüne tabi olur. Görev süreleri boyunca, söz konusu mesleki gizlilik yükümlülüğü özellikle bu Tüzük'e ilişkin yapılan ihlallerin gerçek kişiler tarafından rapor edilmesi için uygulanır.

Kesim 2

Yetkinlik, görevler ve yetkiler

Madde 55

Yetkinlik

1. Her denetim makamı, bu Tüzük uyarınca kendisine verilen görevlerin yerine getirilmesi ve yetkilerin kullanımı hususunda kendi Üye Devlet topraklarında yetkilidir.

2. İşleme faaliyetinin 6(1) maddesinin (c) veya (e) bendine dayalı olarak hareket eden kamu makamları veya özel organlar tarafından gerçekleştirildiği hallerde, ilgili Üye Devlet'in denetim makamı yetkilidir. Bu hallerde, 56. madde uygulanmaz.

3. Denetim makamları kendi yargı yetkileri çerçevesinde hareket eden mahkemelerin işleme faaliyetlerini denetlemeye yetkili değildir.

Madde 56

Baş denetim makamının yetkinliği

1. 55. maddeye halel gelmeksizin, veri sorumlusunun veya veri işleyenin ana kuruluşunun veya tek kuruluşunun denetim makamı söz konusu veri sorumlusu veya veri işleyen tarafından gerçekleştirilen sınır ötesi işlemeye yönelik olarak 60. maddede öngörülen usul uyarınca baş denetim makamı şeklinde hareket etmeye yetkilidir.

2. 1. paragrafa istisna olarak, her denetim makamı, konunun yalnızca kendi Üye Devleti'ndeki bir kuruluşuyla ilgili olması veya yalnızca kendi Üye Devleti'ndeki veri öznelerini kayda değer ölçüde etkilemesi hâlinde, kendisine yapılan bir şikâyetin veya bu Tüzük'e ilişkin olası bir ihlalin ele alınması hususunda yetkilidir.

3. Bu maddenin 2. paragrafında atıfta bulunulan hallerde, denetim makamı, baş denetim makamını bu konuyla ilgili olarak gecikmeksizin bilgilendirir. Baş denetim makamı, bilgilendirildikten itibaren üç haftalık bir süre içinde, kendisini bilgilendiren denetim

makamının Üye Devlet'inde veri sorumlusunun veya veri işleyenin bir kuruluşunun bulunup bulunmadığını dikkate alarak, meseleyi 60. maddede öngörülen usul uyarınca ele alıp almayacağına karar verir.

4. Baş denetim makamının meseleyi ele almaya karar verdiği hallerde, 60. maddede öngörülen usul uygulanır. Baş denetim makamını bilgilendiren denetim makamı bir karar taslağını baş denetim makamına sunabilir. Baş denetim makamı, 60(3) maddesinde atıfta bulunulan karar taslağını hazırlarken, bu taslağı önemle göz önünde bulundurur.

5. Baş denetim makamının meseleyi ele almamaya karar verdiği hallerde, baş denetim makamını bilgilendiren denetim makamı bu hususu 61 ve 62. maddeler uyarınca ele alır.

6. Baş denetim makamı, veri sorumlusu veya veri işleyen tarafından gerçekleştirilen sınır ötesi işlemeye yönelik olarak söz konusu veri sorumlusu veya veri işleyenin tek muhatabıdır.

Madde 57

Görevler

1. Bu Tüzük çerçevesinde ortaya konan diğer görevlere halel gelmeksizin, her denetim makamı kendi topraklarında:

(a) bu Tüzük'ün uygulanmasını izler ve yürütür;

(b) kamunun işleme ile ilgili riskler, kurallar, güvenceler ve haklara yönelik farkındalığını ve anlayışını geliştirir. Özellikle çocuklara yönelik faaliyetlere özel alaka gösterilir;

(c) Üye Devlet hukuku uyarınca, işleme ile ilgili olarak gerçek kişilerin hakları ve özgürlüklerinin korunmasına ilişkin yasal ve idari tedbirler hususunda ulusal parlamento, hükümet ve diğer kuruluşlar ile organlara tavsiyede bulunur;

(d) bu Tüzük kapsamındaki yükümlülükleri hususunda veri sorumlularının ve veri işleyenlerin farkındalığını artırır;

(e) talep üzerine, her veri öznesine bu Tüzük kapsamındaki haklarının kullanımı hususunda bilgi sağlar ve uygun olduğu hallerde, bu amaçla diğer Üye Devletlerdeki denetim makamları ile iş birliği yapar.

(f) 80. madde uyarınca bir veri öznesi veya bir organ, organizasyon ya da bir birlik tarafından yapılan şikâyetleri ele alır ve şikâyetin konusunu, uygun olduğu ölçüde, soruşturur ve özellikle daha ayrıntılı soruşturma ya da başka bir denetim makamı ile koordinasyonun gerekmesi durumunda, şikâyet sahibini soruşturmanın ilerlemesi ve sonucu konusunda makul bir süre içinde bilgilendirir;

(g) bu Tüzük'ün uygulanması ve yürütülmesine ilişkin tutarlılık sağlanması amacıyla, diğer denetim makamlarıyla bilgi paylaşımı ve diğer denetim makamlarına karşılıklı destek sağlama da dâhil olmak üzere iş birliği yapar;

(h) başka bir denetim makamı veya başka bir kamu makamından alınan bilgilere dayalı olanlar dâhil, bu Tüzük'ün uygulanmasına ilişkin soruşturmalar yürütür;

(i) kişisel verilerin korunmasına bir etkileri bulunduğu sürece, bilgi ve iletişim teknolojileri ve ticari uygulamaların gelişimi başta olmak üzere ilgili gelişmeleri izler;

(j) 28(8) maddesinde ve 46(2) maddesinin (d) bendinde atıfta bulunulan standart sözleşme hükümlerini kabul eder;

(k) 35(4) maddesi uyarınca veri koruma etki değerlendirmesi gerekliliği ile ilgili olarak bir liste oluşturur ve bu listeyi devam ettirir;

(l) 36(2) maddesinde atıfta bulunulan işleme faaliyetlerine ilişkin tavsiyede bulunur;

(m) 40(1) maddesi uyarınca davranış kurallarının hazırlanmasını teşvik eder ve 40(5) maddesi uyarınca bir görüş verir ve yeterli güvencelerin sağlandığı davranış kurallarını onaylar;

(n) 42(1) maddesi uyarınca veri koruma belgelendirme mekanizmalarının ve veri koruma mühürleri ile işaretlerinin oluşturulmasını teşvik eder ve 42(5) maddesi uyarınca belgelendirme kriterlerini onaylar;

(o) uygun olan hallerde, 42(7) maddesi uyarınca verilen sertifikaları düzenli aralıklarla gözden geçirir;

(p) 41. madde uyarınca davranış kurallarının izlenmesine yönelik bir organın ve 43. madde uyarınca bir belgelendirme organının akreditasyonuna yönelik kriterleri taslak olarak hazırlar ve yayımlar;

(q) 41. madde uyarınca davranış kurallarının izlenmesine yönelik bir organın ve 43. madde uyarınca bir belgelendirme organının akreditasyonunu gerçekleştirir;

(r) 46(3) maddesinde atıfta bulunulan sözleşme hükümlerini ve hükümleri onaylar;

(s) 47. madde uyarınca bağlayıcı şirket kurallarını onaylar;

(t) Kurulun faaliyetlerine katkıda bulunur;

(u) bu Tüzük'e ilişkin ihlallerin ve 58(2) maddesi uyarınca alınan tedbirlerin iç kayıtlarını tutar; ve

(v) Kişisel verilerin korunmasıyla ilgili diğer her türlü görevi yerine getirir.

2. Her denetim makamı, diğer iletişim araçları hariç tutulmaksızın elektronik olarak da doldurulabilecek bir şikâyet bildirim formu gibi tedbirlerle 1. paragrafın (f) bendinde atıfta bulunulan şikâyet bildirimini kolaylaştırır.

3. Her denetim makamının görevlerinin yerine getirilmesi veri öznesi ve uygun olan hallerde veri koruma görevlisi için ücretsizdir.

4. Taleplerin özellikle tekrar eden niteliği nedeniyle, asılsız veya ölçüsüz olduğunun açıkça görüldüğü hallerde, denetim makamı idari masraflara dayalı olarak makul bir ücret talep edebilir veya taleple ilgili işlem yapmayı reddedebilir. Denetim makamı talebin açık bir şekilde asılsız veya ölçüsüz nitelikte olduğunu ispat yükümlülüğünü taşır.

Madde 58

Yetkiler

1. Her denetim makamı aşağıdaki tüm soruşturma yetkilerine sahiptir:

(a) görevlerinin yerine getirilmesi için ihtiyaç duyduğu bilgilerin sağlanması hususunda veri sorumlusu ve veri işleyen ve uygun olduğu hallerde, veri sorumlusunun veya veri işleyenin temsilcisine talimat verilmesi;

(b) veri koruma denetimleri biçiminde soruşturmalar yürütülmesi;

(c) 42(7) maddesi uyarınca verilen sertifikalara ilişkin bir gözden geçirme yapılması;

(d) bu Tüzük ile ilgili bir ihlal iddiasının veri sorumlusu veya veri işleyene bildirilmesi;

(e) görevlerinin yerine getirilmesi için gereken tüm kişisel veriler ve tüm bilgilere erişimin veri sorumlusu ve veri işleyenden sağlanması;

(f) Birlik veya Üye Devlet usul hukuku uyarınca her türlü veri işleme ekipmanı ve aracı da dâhil olmak üzere veri sorumlusu ve veri işleyenin her türlü tesisine erişim sağlanması.

2. Her denetim makamı aşağıdaki tüm düzeltme yetkilerine sahiptir:

(a) bir veri sorumlusu veya veri işleyene amaçlanan işleme faaliyetlerinin bu Tüzük'ün hükümlerini ihlal etmesinin muhtemel olduğu hususunda ihtarlarda bulunulması;

(b) işleme faaliyetlerinin bu Tüzük'ün hükümlerini ihlal etmiş olduğu hallerde, bir veri sorumlusu veya veri işleyene kınama cezaları verilmesi;

(c) veri öznesinin bu Tüzük uyarınca sahip olduğu haklarının kullanımına ilişkin taleplerinin yerine getirilmesi hususunda veri sorumlusu veya veri işleyene talimat verilmesi;

(d) işleme faaliyetlerinin, uygun olduğu hallerde, belirtilen bir şekilde ve belirtilen bir süre içinde bu Tüzük'ün hükümlerine uyumlu hale getirilmesi hususunda veri sorumlusu veya veri işleyene talimat verilmesi;

(e) bir kişisel veri ihlali hakkında veri öznesinin bilgilendirilmesi hususunda veri sorumlusuna talimat verilmesi;

(f) bir işleme yasağı da dâhil olmak üzere geçici veya kati bir sınırlama getirilmesi;

(g) 16, 17 ve 18. maddeler uyarınca kişisel verilerin düzeltilmesi ya da kalıcı olarak silinmesi veya işlemenin kısıtlanması ve 17(2) maddesi ile 19. madde uyarınca söz konusu işlemlerin kişisel verilerin açıklandığı alıcılara bildirilmesi yönünde talimat verilmesi;

(h) 42 ve 43. maddeler uyarınca verilen bir sertifikanın geri çekilmesi veya belgelendirme organına söz konusu sertifikanın geri çekilmesi yönünde talimat verilmesi veya belgelendirme gerekliliklerinin yerine getirilmediği veya artık yerine getirilmediği hallerde, belgelendirme organına sertifika vermemesi yönünde talimat verilmesi;

(i) her münferit durumun koşullarına dayalı olarak, bu paragrafta atıfta bulunulan tedbirlere ek olarak veya bu tedbirler yerine 83. madde uyarınca bir idari para cezası kesilmesi;

(j) bir üçüncü ülkedeki bir alıcıya veya bir uluslararası kuruluşa yönelik veri akışlarının askıya alınması yönünde talimat verilmesi.

3. Her denetim makamı aşağıdaki tüm izin ve danışma yetkilerine sahiptir:

(a) 36. maddede atıfta bulunulan ön istişare usulü uyarınca veri sorumlusuna tavsiyede bulunulması;

(b) kendi inisiyatifiyle veya talep üzerine, ulusal parlamento, Üye Devlet hükümeti veya Üye Devlet hukuku uyarınca, diğer kuruluşlar ve organların yanı sıra kamuya kişisel verilerin korunmasıyla ilgili herhangi bir konuda görüş bildirilmesi;

(c) Üye Devlet hukukunun bir ön izin gerektirmesi hâlinde, işlemeye, 36(5) maddesinde atıfta bulunulan iznin verilmesi;

(d) 40(5) maddesi uyarınca davranış kuralları taslağına ilişkin bir görüş bildirilmesi ve taslağın onaylanması;

(e) 43. madde uyarınca belgelendirme organlarının akredite edilmesi;

(f) 42(5) maddesi uyarınca sertifikaların verilmesi ve belgelendirme kriterlerinin onaylanması;

(g) 28(8) maddesinde ve 46(2) maddesinin (d) bendinde atıfta bulunulan standart veri koruma şartlarının kabul edilmesi;

(h) 46(3) maddesinin (a) bendinde atıfta bulunulan sözleşme hükümlerine izin verilmesi;

(i) 46(3) maddesinin (b) bendinde atıfta bulunulan idari düzenlemelere izin verilmesi;

(j) 47. madde uyarınca bağlayıcı şirket kurallarının onaylanması.

4. Bu madde uyarınca denetim makamına verilen yetkilerin kullanımı etkili yargı yolu ve yargı süreci de dâhil olmak üzere Şart uyarınca Birlik ve Üye Devlet hukukunda belirlenen uygun güvencelere tabidir.

5. Her Üye Devlet, mevzuatında, denetim makamının bu Tüzük'e ilişkin ihlalleri adli makamların dikkatine sunması ve uygun olduğu hallerde, bu Tüzük'ün hükümlerinin uygulanmasına yönelik yasal süreçleri başlatması veya bu süreçlere başka bir şekilde müdâhil olmasını öngörür.

6. Her Üye Devlet, mevzuatında, denetim makamının 1, 2 ve 3. paragraflarda atıfta bulunulanlara ek yetkilere sahip olmasını öngörebilir. Bu yetkilerin kullanımı VII. Bölümün etkili şekilde uygulanmasını olumsuz etkilemez.

Madde 59

Faaliyet raporları

Her denetim makamı faaliyetleriyle ilgili olarak, bildirilen ihlal türleri ve 58(2) maddesi uyarınca alınan tedbir türlerine yönelik bir listeye yer verilebilecek bir yıllık rapor hazırlar. Bu raporlar ulusal parlamentoya, hükümete ve Üye Devlet hukuku çerçevesinde belirlenen diğer makamlara iletilir. Raporlar kamuya, Komisyona ve Kurula sunulur.

BÖLÜM VII

İş birliği ve tutarlılık

Kesim 1

İş birliği

Madde 60

Baş denetim makamı ve diğer ilgili denetim makamları arasında iş birliği

1. Baş denetim makamı uzlaşıya varmak adına bu madde uyarınca diğer ilgili denetim makamları ile iş birliği yapar. Baş denetim makamı ve ilgili denetim makamları ilgili tüm bilgileri birbirleriyle paylaşır.

2. Baş denetim makamı, özellikle soruşturmaların yürütülmesi açısından veya başka bir Üye Devlet'te kurulu bulunan bir veri sorumlusu veya veri işleyene ilişkin bir tedbirin uygulanmasının izlenmesi açısından, ilgili diğer denetim makamlarının 61. madde uyarınca karşılıklı yardım sağlamasını her zaman talep edebilir ve 62. madde uyarınca ortak operasyonlar gerçekleştirebilir.

3. Baş denetim makamı konuyla ilgili bilgileri gecikmeksizin, diğer ilgili denetim makamlarına iletir. Baş denetim makamı bir taslak kararı gecikmeksizin, diğer ilgili denetim makamlarının görüşüne sunar ve onların görüşlerini dikkate alır.

4. İlgili denetim makamlarından herhangi birinin bu maddenin 3. paragrafı uyarınca danışıldıktan sonra dört haftalık bir süre içinde, taslak karara yönelik yerinde ve gerekçeli bir itirazda bulunduğu hallerde, baş denetim makamı, yerinde ve gerekçeli itiraza uygun hareket

etmemesi veya itirazın yerinde veya gerekçeli olmadığını düşünmesi durumunda, konuyu 63. maddede atıfta bulunulan tutarlılık mekanizmasına sunar.

5. Baş denetim makamının yapılan yerinde ve gerekçeli itiraza uygun hareket etmeyi amaçladığı hallerde, baş denetim makamı revize edilmiş bir taslak kararı diğer ilgili denetim makamlarının görüşüne sunar. Revize edilmiş bu taslak karar iki haftalık bir süre içinde 4. paragrafta atıfta bulunulan usule tabi olur.

6. Diğer ilgili denetim makamlarının hiçbirinin 4 ve 5. paragraflarda atıfta bulunulan süre içinde baş denetim makamı tarafından sunulan taslak karara itiraz etmediği hallerde, baş denetim makamı ve ilgili denetim makamları bu taslak karar ile ilgili mutabakata varmış sayılır ve bu makamlar söz konusu kararla bağlı olur.

7. Baş denetim makamı kararı kabul eder ve uygun olduğu hallerde, veri sorumlusunun veya veri işleyenin ana kuruluşuna veya tek kuruluşuna bildirir ve diğer ilgili denetim makamları ve Kurulu ilgili olguların ve gerekçelerin bir özeti de dâhil olmak üzere söz konusu karar konusunda bilgilendirir. Bir şikâyetin yapıldığı denetim makamı şikâyet sahibini karardan haberdar eder.

8. 7. paragrafa istisna olarak, bir şikâyetin geri çevrildiği veya reddedildiği hallerde, şikâyetin yapıldığı denetim makamı kararı kabul edip şikâyet sahibine bildirir ve veri sorumlusunu karar konusunda bilgilendirir.

9. Baş denetim makamı ve diğer ilgili denetim makamlarının bir şikâyetin belirli kısımlarını geri çevirme veya reddetme ve söz konusu şikâyetin diğer kısımları ile ilgili işlem yapma konusunda mutabık kaldığı hallerde, konunun bu bölümlerinin her birine yönelik ayrı bir karar kabul edilir. Baş denetim makamı veri sorumlusu ile ilgili eylemlere yönelik kısma ilişkin kararı kabul eder, veri sorumlusu veya veri işleyenin kendi Üye Devleti topraklarındaki ana kuruluşu veya tek kuruluşuna bildirir ve şikâyet sahibini bu karardan haberdar ederken, şikâyet sahibinin denetim makamı bu şikâyetin geri çevrildiği veya reddedildiği kısma yönelik kararı kabul eder ve kararı söz konusu şikâyet sahibine bildirir ve veri sorumlusu veya veri işleyeni bu karardan haberdar eder.

10. Veri sorumlusu veya veri işleyen, 7 ve 9. paragraflar uyarınca, baş denetim makamının kararının kendisine bildirilmesinin ardından, Birlik içindeki tüm kuruluşları bağlamındaki işleme faaliyetleri ile ilgili olarak karara uyum sağlanması için gereken tedbirleri alır. Veri sorumlusu veya veri işleyen, karara uyum sağlanması amacıyla alınan tedbirleri, diğer ilgili denetim makamlarını bilgilendirecek olan baş denetim makamına bildirir.

11. İstisnai durumlarda ilgili bir denetim makamını veri öznelerinin menfaatlerinin korunması amacıyla acil bir şekilde harekete geçilmesi yönünde bir ihtiyacın bulunduğunu düşünmeye sevk edecek sebeplerin bulunduğu hallerde, 66. maddede atıfta bulunulan aciliyet usulü uygulanır.

12. Baş denetim makamı ve diğer ilgili denetim makamları bu madde kapsamında gereken bilgileri standart bir format kullanarak elektronik yollarla birbirlerine sağlar.

Madde 61

Karşılıklı yardım

1. Denetim makamları bu Tüzük'ün tutarlı bir şekilde yürütülmesi ve uygulanması amacıyla birbirlerine ilgili bilgileri ve karşılıklı yardımı sağlar ve birbirleriyle etkili iş birliğine yönelik tedbirleri uygulamaya koyar. Karşılıklı yardım, özellikle, ön izinlerin ve istişarelerin, denetimlerin ve soruşturmaların yürütülmesine ilişkin talepler gibi bilgi talepleri ve denetim tedbirlerini kapsar.

2. Her denetim makamı başka bir denetim makamının talebine fazla gecikmeksizin ve talebi aldıktan sonra en geç bir ay içinde yanıt verilmesi için gereken tüm uygun tedbirleri alır. Bu tür tedbirler özellikle, bir soruşturmanın yürütülmesi ile ilgili bilgilerin iletilmesini içerebilir.

3. Yardım talepleri, talebin amacı ve sebepleri de dâhil olmak üzere gerekli tüm bilgileri içerir. Paylaşılan bilgiler yalnızca talep edilme amacı doğrultusunda kullanılır.

4. Talebin iletildiği denetim makamı, aşağıdaki durumlar dışında, talebi yerine getirmeyi reddedemez:

(a) talebin konusu veya yerine getirmesi istenen tedbirler açısından yetkili olmaması veya;

(b) talebe uygun hareket etmenin bu Tüzük'ü veya Birlik hukukunu ya da talebi alan denetim makamının tabi olduğu Üye Devlet hukukunu ihlâl edecek olması.

5. Talebin iletildiği denetim makamı talepte bulunan denetim makamını talebe yanıt verilmesi amacıyla alınan tedbirlerin sonuçları veya duruma göre, seyri konusunda bilgilendirir. Talebin iletildiği denetim makamı, 4. paragraf uyarınca bir talebi yerine getirmeyi reddetmesi durumunda bunun gerekçelerini sunar.

6. Talebin iletildiği denetim makamları, kural olarak, diğer denetim makamları tarafından talep edilen bilgileri standart bir format kullanarak elektronik yollarla sağlar.

7. Talebin iletildiği denetim makamları, karşılıklı yardım talebi uyarınca kendileri tarafından gerçekleştirilen herhangi bir eylem için ücret talep etmez. Denetim makamları, istisnai durumlarda karşılıklı yardım sağlanmasından kaynaklanan özel harcamalar ile ilgili olarak birbirlerinin zararının ödenmesine ilişkin kurallar üzerinde anlaşabilir.

8. Bir denetim makamının bu maddenin 5. paragrafında atıfta bulunulan bilgileri başka bir denetim makamının talebini aldıktan sonra bir ay içinde sağlamadığı hallerde, talepte bulunan denetim makamı 55(1) maddesi uyarınca kendi Üye Devlet topraklarında geçici bir tedbir kabul edebilir. Bu durumda, 66(1) maddesi kapsamındaki acil bir şekilde harekete geçme ihtiyacının mevcut olduğu varsayılır ve 66(2) maddesi uyarınca Kuruldan acil bir bağlayıcı karar gerekir.

9. Komisyon, özellikle bu maddenin 6. paragrafında atıfta bulunulan standart format başta olmak üzere, bu maddede atıfta bulunulan karşılıklı yardıma ilişkin format ile usulleri ve denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin düzenlemeleri, uygulama tasarrufları vasıtasıyla belirtebilir. Bu uygulama tasarrufları 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

Madde 62

Denetim makamlarının ortak operasyonları

1. Denetim makamları, uygun olduğu hallerde, ortak soruşturmalar ve ortak uygulama tedbirleri de dâhil olmak üzere, diğer Üye Devletlerin denetim makamlarının üyeleri veya personelinin dâhil olduğu ortak operasyonlar gerçekleştirir.

2. Veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te kuruluşlarının bulunduğu veya birden fazla Üye Devlet'teki önemli sayıda veri öznesinin işleme faaliyetlerinden kayda değer biçimde etkilenmesinin muhtemel olduğu hallerde, her Üye Devlet'in bir denetim makamının ortak operasyonlara katılma hakkı bulunur. 56(1) veya (4) maddesi uyarınca yetkili olan denetim makamı söz konusu Üye Devletlerin her birinin denetim makamını ortak operasyonlara katılmaya davet eder ve bir denetim makamının katılma talebini gecikmeksizin yanıtlar.

3. Bir denetim makamı, Üye Devlet hukuku uyarınca ve destekleyen denetim makamının izniyle, soruşturma yetkileri de dâhil olmak üzere, destekleyen denetim makamının ortak

operasyonlara dahil olan üyeleri ya da personeline yetki verebilir veya ev sahibi denetim makamının Üye Devleti'nin hukuku izin verdiği ölçüde, destekleyen denetim makamının üyeleri veya personelinin soruşturma yetkilerini, destekleyen denetim makamının Üye Devleti'nin hukuku uyarınca kullanmasına izin verebilir. Söz konusu soruşturma yetkileri yalnızca ev sahibi denetim makamının üyeleri veya personelinin kılavuzluğunda ve bu üyeler veya personelin huzurunda kullanılabilir. Destekleyen denetim makamının üyeleri ya da personeli ev sahibi denetim makamının Üye Devleti'nin hukukuna tabidir.

4. 1. paragraf uyarınca, destekleyen denetim makamının personelinin başka bir Üye Devlet'te faaliyet gösterdiği hallerde, ev sahibi denetim makamının Üye Devleti, söz konusu personelin faaliyet gösterdiği Üye Devlet'in hukuku uyarınca, faaliyetleri esnasında sebep oldukları her türlü zarara ilişkin sorumluluk da dâhil olmak üzere onların eylemlerine ilişkin sorumluluğu üstlenir.

5. Topraklarında zarar meydana gelen Üye Devlet, söz konusu zararı, kendi personelinin sebep olduğu zarar için geçerli koşullar altında giderir. Personeli başka bir Üye Devlet'in topraklarında herhangi bir kişiye zarar veren destekleyen denetim makamının Üye Devleti, söz konusu personel adına hak sahibi kişilere yaptığı ödemeler ile ilgili olarak diğer Üye Devlet'in zararını eksiksiz olarak tazmin eder.

6. Haklarının üçüncü kişilerle karşılıklı olarak kullanımına halel gelmeksizin ve 5. paragraf haricinde, her Üye Devlet, 1. paragrafta öngörülen durumda, 4. paragrafta atıfta bulunulan zararla ilgili olarak başka bir Üye Devlet'ten tazminat talep etmekten kaçınır.

7. Bir ortak operasyonun amaçlandığı ve bir denetim makamının bu maddenin 2. paragrafının ikinci cümlesinde ortaya konan yükümlülüğü bir ay içinde yerine getirmediği hallerde, diğer denetim makamları 55. madde uyarınca kendi Üye Devlet topraklarında geçici bir tedbir kabul edebilir. Bu durumda, 66(1) maddesi kapsamındaki acil bir şekilde harekete geçme ihtiyacının mevcut olduğu varsayılır ve 66(2) maddesi uyarınca Kurulun bir görüşü veya acil bir bağlayıcı kararı gerekir.

Kesim 2

Tutarlılık

Madde 63

Tutarlılık mekanizması

Bu Tüzük'ün Birlik genelinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla, denetim makamları, bu Kesimde belirtilen tutarlılık mekanizması vasıtasıyla, birbirleriyle ve gerekli olduğu hallerde, Komisyon ile iş birliği yapar.

Madde 64

Kurulun görüşü

1. Kurul, yetkili denetim makamının aşağıdaki tedbirlerden herhangi birini kabul etmeyi amaçlaması hâlinde, bir görüş bildirir. Bu amaçla, yetkili denetim makamı, taslak kararı, şu özellikleri taşıdığında, Kurula iletir:

(a) karar ile 35(4) maddesi uyarınca bir veri koruma etki değerlendirmesi gerekliliğine tabi işleme faaliyetlerine ilişkin bir listenin kabul edilmesinin amaçlanması;

(b) kararın, 40(7) maddesi uyarınca, bir davranış kuralları taslağının veya davranış kurallarında bir değişikliğin veya genişletmenin bu Tüzük ile uyumlu olup olmadığına ilişkin bir husus ile ilgili olması;

(c) karar ile 41(3) maddesi uyarınca bir organın veya 43(3) maddesi uyarınca bir belgelendirme organının akreditasyonuna yönelik kriterlerin onaylanmasının amaçlanması;

(d) karar ile 46(2) maddesinin (d) bendinde ve 28(8) maddesinde atıfta bulunulan standart veri koruma hükümlerinin belirlenmesinin amaçlanması;

(e) karar ile 46(3) maddesinin (a) bendinde atıfta bulunulan sözleşme hükümlerine izin verilmesinin amaçlanması veya

(f) karar ile 47. madde kapsamındaki bağlayıcı şirket kurallarının onaylanmasının amaçlanması.

2. Herhangi bir denetim makamı, Kurul Başkanı veya Komisyon, özellikle bir yetkili denetim makamının 61. madde uyarınca karşılıklı yardım yükümlülüklerine veya 62. madde uyarınca ortak operasyonlara ilişkin yükümlülüklerine uymadığı hallerde, genel uygulamaya ilişkin veya birden fazla Üye Devlet'te etkilere neden olan herhangi bir hususun görüş alınması amacıyla Kurul tarafından incelenmesini talep edebilir.

3. 1 ve 2. paragraflarda atıfta bulunulan durumlarda, Kurul, aynı husus ile ilgili daha önce bir görüş bildirmemiş olması koşuluyla, kendisine sunulan hususla ilgili bir görüş bildirir. Bu görüş Kurul üyelerinin basit çoğunluğuyla sekiz hafta içinde kabul edilir. Bu süre, konunun karmaşıklığı dikkate alınarak, altı hafta daha uzatılabilir. 1. paragrafta atıfta bulunulan ve 5. paragraf uyarınca Kurul üyelerine dağıtılan taslak karar ile ilgili olarak, Başkan tarafından belirtilen makul bir süre içinde itiraz etmeyen bir üye, taslak kararla aynı görüşte sayılır.

4. Denetim makamları ve Komisyon, fazla gecikmeksizin, duruma göre, olgulara ilişkin bir özet, taslak karar, söz konusu tedbirin alınmasını gerekli kılan gerekçeler ve diğer ilgili denetim makamlarının görüşleri de dâhil olmak üzere ilgili her türlü bilgiyi standart bir format kullanarak ve elektronik yollarla Kurula iletir.

5. Kurul Başkanı, fazla gecikmeksizin elektronik yollarla:

(a) Kurul üyelerini ve Komisyonu, kendisine iletilen her türlü ilgili bilgi hakkında standart bir format kullanarak bilgilendirir. Kurul sekretaryası, gerekli hallerde, ilgili bilgilerin yazılı çevirilerini sağlar ve

(b) duruma göre, 1 ve 2. paragraflarda atıfta bulunulan denetim makamını ve Komisyonu, görüş hakkında bilgilendirir ve görüşü kamuya açıklar.

6. Yetkili denetim makamı, 1. paragrafta atıfta bulunulan taslak kararını 3. paragrafta atıfta bulunulan süre içinde kabul etmez.

7. 1. paragrafta atıfta bulunulan yetkili denetim makamı Kurulun görüşünü azami ölçüde dikkate alır ve taslak kararını aynı şekilde muhafaza edip etmeyeceğini veya değiştirip değiştirmeyeceğini ve değişiklik varsa, değiştirilmiş taslak kararını, görüşün alınmasından itibaren iki hafta içinde standart bir format kullanarak elektronik yollarla Kurul Başkanına iletir.

8. Bu maddenin 7. paragrafında atıfta bulunulan süre içinde, ilgili denetim makamının yerinde gerekçeler sağlayarak Kurulun görüşüne tamamen veya kısmen uygun hareket etme niyetinde olmadığını Kurul Başkanına bildirmesi halinde, 65(1) maddesi uygulanır.

Madde 65

Uyuşmazlıkların Kurul tarafından çözülmesi

1. Bu Tüzük'ün münferit durumlarda doğru ve tutarlı bir şekilde uygulanmasını sağlamak amacıyla, Kurul aşağıdaki durumlarda bağlayıcı bir karar alır:

(a) 60(4) maddesinde atıfta bulunulan bir durumda, ilgili denetim makamının baş makamın bir taslak kararına yerinde ve gerekçeli bir itirazda bulunduğu veya baş makamın böyle bir itirazı yerinde veya gerekçeli görmeyerek reddettiği hâllerde. Bağlayıcı karar, yerinde ve gerekçeli itiraza konu olan tüm hususlar ile özellikle bu Tüzük'ün ihlal edilip edilmediğiyle ilgilidir;

(b) ilgili denetim makamlarından hangisinin ana kuruluş açısından yetkili olduğuna ilişkin çelişkili görüşler bulunduğu hâllerde;

(c) yetkili denetim makamının 64(1) maddesinde atıfta bulunulan durumlarda Kurulun görüşünü talep etmediği veya 64. madde kapsamında sunulan Kurul görüşüne uygun hareket etmediği hâllerde. Bu durumda, ilgili herhangi bir denetim makamı veya Komisyon bu hususu Kurula iletebilir.

2. 1. paragrafta atıfta bulunulan karar, konunun iletilmesinden itibaren bir ay içinde Kurul üyelerinin üçte iki çoğunluğu ile alınır. Bu süre, konunun karmaşıklığı dikkate alınarak, bir ay daha uzatılabilir. 1. paragrafta atıfta bulunulan karar gerekçeli olur ve baş denetim makamı ile ilgili tüm denetim makamlarına iletilir ve onlar açısından bağlayıcıdır.

3. Kurulun 2. paragrafta atıfta bulunulan süreler içinde bir karar alamaması halinde, Kurul 2. paragrafta atıfta bulunulan ikinci ayın dolmasının ardından iki hafta içinde kararını Kurul üyelerinin basit çoğunluğu ile alır. Kurul üyeleri arasında eşitlik olması hâlinde, karar Kurul Başkanının oyu ile alınır.

4. İlgili denetim makamları, 2 ve 3. paragraflarda atıfta bulunulan süreler esnasında, 1. paragraf kapsamında Kurula sunulan konu ile ilgili bir karar kabul etmez.

5. Kurul Başkanı, 1. paragrafta atıfta bulunulan kararı fazla gecikmeksizin ilgili denetim makamlarına bildirir. Başkan karar hususunda Komisyonu da bilgilendirir. Denetim makamının 6. paragrafta atıfta bulunulan nihai kararı bildirmesinin ardından, karar gecikmeksizin Kurulun internet sitesinde yayımlanır.

6. Baş denetim makamı veya duruma göre, şikâyetin yapıldığı denetim makamı, fazla gecikmeksizin ve Kurulun kararını bildirmesinden sonra en geç bir ay içinde, bu maddenin 1. paragrafında atıfta bulunulan karara dayalı olarak nihai kararını verir. Baş denetim makamı veya duruma göre, şikâyetin yapıldığı denetim makamı, nihai kararının ayrı ayrı veri sorumlusu veya veri işleyene ve veri öznesine bildirildiği tarih hususunda Kurulu bilgilendirir. İlgili denetim makamlarının nihai kararı 60(7), (8) ve (9) maddesinin koşulları çerçevesinde alınır. Nihai kararda bu maddenin 1. paragrafında atıfta bulunulan karara atıfta bulunulur ve söz konusu paragrafta atıfta bulunulan kararın bu maddenin 5. paragrafı uyarınca Kurulun internet sitesinde yayımlanacağı belirtilir. Bu maddenin 1. paragrafında atıfta bulunulan karar nihai karara eklenir.

Madde 66

Aciliyet usulü

1. İstisnai durumlarda, ilgili denetim makamının veri öznelerinin hak ve özgürlüklerinin korunmasına yönelik olarak acil bir şekilde harekete geçilmesine ihtiyaç olduğunu değerlendirdiği hallerde, söz konusu denetim makamı, 63, 64 ve 65. maddelerde atıfta bulunulan tutarlılık mekanizmasından veya 60. maddede atıfta bulunulan usule istisna olarak, kendi topraklarında üç ayı geçmeyen belirli bir geçerlilik süresi boyunca hukuki sonuçlar

doğurması amaçlanan geçici tedbirleri ivedilikle alabilir. Denetim makamı, bu tedbirleri ve bu tedbirlerin alınma sebeplerini, gecikmeksizin diğer ilgili denetim makamlarına, Kurula ve Komisyona iletir.

2. Bir denetim makamının 1. paragraf uyarınca bir tedbir aldığı ve nihai tedbirlerin ivedilikle alınmasının gerektiğini değerlendirdiği hâllerde, söz konusu denetim makamı, acil bir görüş veya acil bir bağlayıcı kararın talep edilmesine ilişkin sebepleri sunarak, söz konusu görüşü veya kararı Kuruldan talep edebilir.

3. Herhangi bir denetim makamı, veri öznelerinin hak ve özgürlüklerinin korunmasına yönelik acil bir şekilde harekete geçilmesine ihtiyaç olup yetkili denetim makamının uygun tedbir almadığı hâllerde, acil bir şekilde harekete geçme ihtiyacının sebepleri de dâhil olmak üzere, duruma göre, acil bir görüş veya acil bir bağlayıcı kararın talep edilmesine ilişkin sebepleri sunarak, söz konusu görüşü veya kararı Kuruldan talep edebilir.

4. 64(3) ve 65(2) maddelerine istisna olarak, bu maddenin 2 ve 3. paragraflarında atıfta bulunulan acil bir görüş veya acil bir bağlayıcı karar Kurul üyelerinin basit çoğunluğuyla iki hafta içinde alınır.

Madde 67

Bilgi alışverişi

Komisyon, özellikle 64. maddede atıfta bulunulan standart format başta olmak üzere, denetim makamları arasında ve denetim makamları ile Kurul arasında elektronik yollarla bilgi alışverişine ilişkin düzenlemeleri belirten genel kapsamlı uygulama tasarrufları kabul edebilir.

Bu uygulama tasarrufları 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca kabul edilir.

Kesim 3

Avrupa veri koruma kurulu

Madde 68

Avrupa Veri Koruma Kurulu

Avrupa Veri Koruma Kurulu ("Kurul") bu Tüzük ile Birlik organı olarak kurulmuştur ve tüzel kişiliğe sahiptir.

2. Kurul, Başkanı tarafından temsil edilir.

3. Kurul her Üye Devlet'in bir denetim makamı başkanı ile Avrupa Veri Koruma Denetçisi veya bunların kendi temsilcilerinden oluşur.

4. Bir Üye Devlet'te birden fazla denetim makamının bu Tüzük uyarınca hükümlerin uygulanmasını denetlemekten sorumlu olduğu hâllerde, söz konusu Üye Devlet'in hukuku uyarınca ortak bir temsilci atanır.

5. Komisyonun Kurulun faaliyetleri ve toplantılarına oy hakkı olmaksızın katılma hakkı bulunur. Komisyon bir temsilci belirler. Kurul Başkanı Kurulun faaliyetlerini Komisyona bildirir.

6. 65. maddede atıfta bulunulan hâllerde, Avrupa Veri Koruma Denetçisinin yalnızca Birlik kurumları, organları, ofisleri ve ajanslarına uygulanan ilke ve kurallar ile ilgili olan ve esasen bu Tüzük'ün ilke ve kurallarına tekabül eden kararlarda oy hakkı bulunur.

Madde 69

Bağımsızlık

1. Kurul, 70 ve 71. maddeler uyarınca görevlerini yerine getirirken veya yetkilerini kullanırken bağımsız bir şekilde hareket eder.

2. 70(1) maddesinin (b) bendinde ve 70(2) maddesinde atıfta bulunulan Komisyon tarafından yapılan taleplere halel gelmeksizin, Kurul, görevlerini yerine getirirken veya yetkilerini kullanırken, hiç kimseden talimat talebinde bulunmaz ve talimat almaz.

Madde 70

Kurulun görevleri

1. Kurul bu Tüzük'ün tutarlı bir şekilde uygulanmasını sağlar. Bu amaçla, Kurul kendi inisiyatifiyle veya ilgili olduğu hâllerde, Komisyonun talebi üzerine, özellikle:

(a) ulusal denetim makamlarının görevlerine halel gelmeksizin, 64 ve 65. maddelerde öngörülen durumlarda bu Tüzük'ün doğru bir şekilde uygulanmasını izler ve sağlar;

(b) bu Tüzük'te yapılması önerilen herhangi bir değişiklik de dâhil olmak üzere, Birlik içinde kişisel verilerin korunmasıyla ilgili her türlü hususta Komisyona tavsiyede bulunur;

(c) Veri sorumluları, veri işleyenleri ve denetim makamları arasında bağlayıcı şirket kurallarına yönelik bilgi alışverişine ilişkin format ve usuller hususunda Komisyona tavsiyede bulunur;

(d) 17(2) maddesinde atıfta bulunulduğu üzere, kişisel verilerin linkleri, nüshaları veya kopyalarının kamuya açık iletişim hizmetlerinden kalıcı olarak silinmesiyle ilgili usullere yönelik kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(e) kendi inisiyatifiyle veya üyelerinden birinin talebi üzerine ya da Komisyonun talebi üzerine, bu Tüzük'ün uygulanmasına ilişkin her türlü meseleyi inceler ve bu Tüzük'ün tutarlı bir şekilde uygulanmasını teşvik etmek üzere kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(f) 22(2) maddesi uyarınca profillemeye dayalı kararlara yönelik kriterler ve koşulların daha ayrıntılı olarak belirtilmesi için bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(g) kişisel veri ihlallerinin tespit edilmesi ve 33(1) ve (2) maddesinde atıfta bulunulan fazla gecikmenin belirlenmesine yönelik olarak ve bir veri sorumlusu veya veri işleyenin kişisel veri ihlalini bildirmesinin gerekli olduğu özel durumlar açısından, bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(h) kişisel veri ihlalinin 34(1) maddesinde atıfta bulunulan gerçek kişilerin hak ve özgürlükleri açısından yüksek bir risk teşkil etmesinin muhtemel olduğu haller ile ilgili olarak, bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(i) veri sorumluları tarafından uyulan bağlayıcı şirket kuralları ve veri işleyenler tarafından uyulan bağlayıcı şirket kurallarına ve 47. maddede atıfta bulunulan ilgili veri öznelerinin kişisel verilerinin korunmasını sağlamak için ek gerekliliklere dayalı olarak gerçekleştirilen kişisel veri aktarımlarına yönelik kriterler ve gerekliliklerin daha ayrıntılı olarak belirtilmesi amacıyla, bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(j) 49(1) maddesine dayalı olarak gerçekleştirilen kişisel veri aktarımlarına yönelik kriterler ve gerekliliklerin daha ayrıntılı olarak belirtilmesi amacıyla, bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(k) 58(1), (2) ve (3) maddesinde atıfta bulunulan tedbirlerin uygulanması ve 83. madde uyarınca idari para cezalarının belirlenmesi ile ilgili olarak denetim makamlarına yönelik kılavuzlar hazırlar;

(l) (e) ve (f) bentlerinde atıfta bulunulan kılavuzlar, tavsiyeler ve en iyi uygulamaların pratikte uygulanmasını gözden geçirir;

(m) 54(2) maddesi uyarınca bu Tüzük'e ilişkin ihlallerin gerçek kişiler tarafından bildirilmesine yönelik ortak usullerin oluşturulması hususunda, bu paragrafın (e) bendi uyarınca kılavuzlar, tavsiyeler ve en iyi uygulamaları yayımlar;

(n) 40 ve 42. maddeler uyarınca davranış kurallarının hazırlanmasını ve veri koruma belgelendirme mekanizmaları ve veri koruma mühürleri ile işaretlerinin oluşturulmasını teşvik eder;

(o) 43. madde uyarınca belgelendirme organlarının akreditasyonunu ve düzenli aralıklarla gözden geçirilmesini gerçekleştirir ve 43(6) maddesi uyarınca akredite organların ve 42(7) maddesi uyarınca üçüncü ülkelerde kurulu bulunan akredite veri sorumluları veya veri işleyenlerinin halka açık bir sicilini tutar;

(p) 42. madde kapsamında belgelendirme organlarının akreditasyonuna yönelik olarak 43(3) maddesinde atıfta bulunulan gereklilikleri belirtir;

(q) 43(8) maddesinde atıfta bulunulan belgelendirme gerekliliklerine ilişkin Komisyona görüş sunar;

(r) 12(7) maddesinde atıfta bulunulan simgelere ilişkin Komisyona görüş sunar;

(s) bir üçüncü ülke, bir bölge veya söz konusu üçüncü ülke içinde belirtilen bir veya daha fazla sayıda sektörün veya bir uluslararası kuruluşun artık yeterli bir koruma düzeyi sağlayıp sağlamadığına ilişkin değerlendirme de dâhil olmak üzere, bir üçüncü ülke veya bir uluslararası kuruluştaki koruma düzeyinin yeterliliğinin değerlendirilmesine ilişkin bir görüşü Komisyona sunar. Bu amaçla, Komisyon üçüncü ülkenin hükümeti ile yapılan yazışmalar da dâhil olmak üzere, söz konusu üçüncü ülke, bölge veya belirtilen sektör ya da uluslararası kuruluşla ilgili gerekli tüm belgeleri Kurula sunar.

(t) 64(1) maddesinde atıfta bulunulan tutarlılık mekanizması uyarınca denetim makamlarının taslak kararlarına, 64(2) maddesi uyarınca arz edilen meselelere ilişkin görüşler bildirir ve 66. maddede atıfta bulunulan haller de dâhil olmak üzere 65. madde uyarınca bağlayıcı kararlar alır;

(u) denetim makamları arasında işbirliğini ve etkili iki taraflı ve çok taraflı bilgi ve en iyi uygulamaların paylaşımını teşvik eder;

(v) uygun olduğu hâllerde, üçüncü ülkelerin denetim makamları veya uluslararası kuruluşlarla birlikte, ortak eğitim programlarını teşvik eder ve denetim makamları arasında personel değişimlerini kolaylaştırır;

(w) dünya çapında veri koruma denetim makamlarıyla veri koruma mevzuatı ve uygulamasına ilişkin bilgi ve belge paylaşımını teşvik eder;

(x) 40(9) maddesi uyarınca Birlik düzeyinde hazırlanan davranış kurallarına ilişkin görüşler bildirir ve

(y) tutarlılık mekanizmasında ele alınan konular ile ilgili olarak denetim makamları ve mahkemeler tarafından alınan kararlara ilişkin halkın erişebileceği bir elektronik sicil tutar.

2. Komisyonun Kuruldan tavsiye talebinde bulunduğu hâllerde, Komisyon konunun aciliyetini dikkate alarak bir süre sınırı belirtebilir.

3. Kurul görüşlerini, kılavuzlarını, tavsiyelerini ve en iyi uygulamalarını Komisyona ve 93. maddede atıfta bulunulan komiteye iletir ve bunları kamuya açıklar.

4. Kurul, uygun olduğu hâllerde, ilgili taraflara danışır ve onlara makul bir süre içinde görüşlerini bildirme olanağı tanır. Kurul, 76. maddeye halel gelmeksizin, istişare usulünün sonuçlarını halka açık hale getirir.

Madde 71

Raporlar

1. Kurul, Birlik içinde ve gerekli olduğu hâllerde, üçüncü ülkelerde ve uluslararası kuruluşlarda, işleme bakımından gerçek kişilerin korunması ile ilgili bir yıllık rapor hazırlar. Rapor kamuya açıklanır ve Avrupa Parlamentosuna, Konseye ve Komisyona iletilir.

2. Yıllık raporda 70(1) maddesinin (l) bendinde atıfta bulunulan kılavuzlar, tavsiyeler ve en iyi uygulamaların ve 65. maddede atıfta bulunulan bağlayıcı kararların pratikte uygulamasına ilişkin bir gözden geçirmeye yer verilir.

Madde 72

Usul

1. Bu Tüzük'te aksi belirtilmedikçe, Kurul kararlarını üyelerinin basit çoğunluğu ile alır.

2. Kurul kendi usul kurallarını üyelerinin üçte iki çoğunluğuyla kabul eder ve kendi çalışma düzenlemelerini yapar.

Madde 73

Başkan

1. Kurul, kendi üyeleri arasından bir başkan ve iki başkan yardımcısını basit çoğunluk ile seçer.

2. Başkan ve başkan yardımcılarının görev süresi beş yıldır ve bir kez yenilenebilir.

Madde 74

Başkanın görevleri

1. Başkan aşağıdaki görevleri yerine getirir:

(a) Kurul toplantılarının düzenlenmesi ve gündemin hazırlanması;

(b) Kurul tarafından 65. madde uyarınca alınan kararların baş denetim makamına ve ilgili denetim makamlarına bildirilmesi;

(c) 63. maddede atıfta bulunulan tutarlılık mekanizması ile ilgili görevi başta olmak üzere, Kurul görevlerinin zamanında yerine getirilmesinin sağlanması.

2. Kurul, Başkan ile başkan yardımcıları arasındaki görev dağılımını usul kurallarında ortaya koyar.

Madde 75

Sekretarya

1. Kurulun Avrupa Veri Koruma Denetçisi tarafından sağlanan bir sekretaryası bulunur.

2. Sekretarya, görevlerini münhasıran Kurul Başkanının talimatları doğrultusunda gerçekleştirir.

3. Avrupa Veri Koruma Denetçisinin bu Tüzük ile Kurula verilen görevlerin yerine getirilmesine müdahil olan personeli, Avrupa Veri Koruma Denetçisine verilen görevlerin yerine getirilmesine müdahil olan personelden farklı raporlama yükümlülüklerine tabidir.

4. Uygun olduğu hâllerde, Kurul ve Avrupa Veri Koruma Denetçisi bu maddeyi uygulayan, aralarındaki işbirliği koşullarını belirleyen ve Avrupa Veri Koruma Denetçisinin bu Tüzük ile Kurula verilen görevlerinin yerine getirilmesine müdahil olan personeline uygulanan bir Mutabakat Zaptı hazırlar ve yayımlar.

5. Sekretarya, Kurula analitik, idari ve lojistik destek sağlar.

6. Sekretarya özellikle aşağıdaki hususlardan sorumludur:

(a) Kurulun günlük işleri;

(b) Kurul üyeleri, Kurul Başkanı ve Komisyon arasındaki iletişim;

(c) diğer kurumlar ve halk ile iletişim;

(d) iç ve dış iletişim için elektronik araçların kullanımı;

(e) ilgili bilgilerin yazılı çevirisinin yapılması;

(f) Kurul toplantılarının hazırlanması ve takip edilmesi;

(g) görüşlerin, denetim makamları arasındaki uyuşmazlıkların çözümüne ilişkin kararların ve Kurul tarafından kabul edilen diğer metinlerin hazırlanması, taslak haline getirilmesi ve yayımlanması.

Madde 76

Gizlilik

1. Usul kurallarında belirtildiği üzere, Kurulun gerekli gördüğü hâllerde, Kurul görüşmeleri gizlidir.

2. Kurul üyelerine, uzmanlara ve üçüncü kişilerin temsilcilerine sunulan belgelere erişim (AT) 1049/2001 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü[21] ile düzenlenir.

[21] Avrupa Parlamentosu, Konsey ve Komisyon belgelerine kamu erişimine ilişkin 30 Mayıs 2001 tarihli ve (AT) 1049/2001 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (ATRG L 145, 31.5.2001, s.43).

BÖLÜM VIII

Başvuru yolları, sorumluluk ve cezalar

Madde 77

Bir denetim makamına şikâyette bulunma hakkı

1. Tüm veri özneleri, kendisi ile alakalı kişisel verilerin işlenmesinin bu Tüzük'ü ihlal ettiğini değerlendirmesi durumunda, başka bir idari başvuru yoluna veya yargı yoluna halel gelmeksizin, özellikle, mutat meskeninin veya iş yerinin bulunduğu ya da iddia edilen ihlalin gerçekleştiği Üye Devlet'te, bir denetim makamına şikâyette bulunma hakkına sahiptir.

2. Şikâyetin yapıldığı denetim makamı, 78. madde uyarınca bir yargı yoluna başvurma imkânı da dâhil, şikâyetin seyri ve sonucu ile ilgili olarak şikâyet sahibini bilgilendirir.

Madde 78

Bir denetim makamına karşı etkili bir yargı yoluna başvurma hakkı

1. Başka herhangi bir yargısal olmayan veya idari başvuru yoluna halel gelmeksizin, her gerçek veya tüzel kişinin bir denetim makamının kendileriyle ilgili yasal bağlayıcılığı olan bir kararına karşı etkili bir yargı yoluna başvurma hakkı vardır.

2. 55 ve 56. maddeler uyarınca yetkili olan denetim makamının üç ay içinde bir şikâyeti ele almadığı veya 77. madde uyarınca yapılan şikâyetin seyri veya sonucu hakkında veri öznesini bilgilendirmediği hâllerde, her veri öznesinin, başka bir yargısal olmayan veya idari başvuru yoluna halel gelmeksizin, etkili bir yargı yoluna başvurma hakkı bulunur.

3. Bir denetim makamına karşı açılacak davalar, denetim makamının kurulu bulunduğu Üye Devlet'in mahkemelerinde açılır.

4. Kurulun tutarlılık mekanizmasındaki bir görüşü veya kararından sonra bir denetim makamının bir kararına karşı davaların açıldığı hâllerde, denetim makamı söz konusu görüş veya kararı mahkemeye iletir.

Madde 79

Veri sorumlusu veya veri işleyene karşı etkili bir yargı yoluna başvurma hakkı

1. Veri özneleri, kişisel verilerinin bu Tüzük'e aykırı bir şekilde işlenmesi sonucu bu Tüzük kapsamındaki haklarının ihlâl edildiğini değerlendirdikleri hâllerde, 77. madde uyarınca bir denetim makamına şikâyette bulunma hakkı da dâhil olmak üzere, mevcut yargısal olmayan veya idari başvuru yollarına halel gelmeksizin, etkili bir yargı yoluna başvurma hakkına sahiptir.

2. Veri sorumlusu veya veri işleyene karşı açılacak davalar, veri sorumlusu veya veri işleyenin, kuruluşunun bulunduğu Üye Devlet'in mahkemelerinde açılır. Alternatif olarak, veri sorumlusu veya veri işleyenin, bir Üye Devlet'in kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu makamı olması haricinde, söz konusu davalar veri öznesinin mutat meskeninin bulunduğu Üye Devlet'in mahkemelerinde açılabilir.

Madde 80

Veri öznelerinin temsili

1. Veri öznesi; bir Üye Devlet hukuku uyarınca uygun bir şekilde kurulmuş olan, kamu yararına yasal hedefleri bulunan ve veri öznelerinin kişisel verilerinin korunmasına ilişkin hakları ve özgürlüklerinin korunması alanında aktif olan kâr amacı gütmeyen bir organ, organizasyon veya birliğe, kendi adına şikâyette bulunma, 77, 78 ve 79. maddelerde atıfta bulunulan hakları kendisi adına kullanma ve Üye Devlet hukukunda öngörülmesi hâlinde, 82. maddede atıfta bulunulan tazminat alma hakkını kullanma yetkilerini verme hakkına sahiptir.

2. Üye Devletler, veri öznesinin verdiği yetkiden bağımsız olarak, bu maddenin 1. paragrafında atıfta bulunulan herhangi bir organ, organizasyon veya birliğin, bir veri öznesinin bu Tüzük kapsamındaki haklarının işleme sonucu ihlâl edilmiş olduğunu değerlendirmesi hâlinde, söz konusu Üye Devlet'te, 77. madde uyarınca yetkili olan denetim makamına şikâyette bulunma ve 78 ve 79. maddelerde atıfta bulunulan hakları kullanma hakkına sahip olmasını öngörebilirler.

Madde 81

Davanın askıya alınması

1. Bir Üye Devlet'in yetkili mahkemesinin aynı veri sorumlusu veya veri işleyen tarafından gerçekleştirilen bir işleme ile ilgili olarak aynı konu hakkında başka bir Üye Devlet'te bulunan bir mahkemede devam eden bir davanın bulunduğu yönünde bilgisinin olması hâlinde, söz konusu yetkili mahkeme böyle bir davanın varlığını teyit etmek üzere diğer Üye Devlet'te bulunan mahkemeyle irtibat kurar.

2. Aynı veri sorumlusu veya veri işleyenin işleme faaliyeti ile ilgili olarak aynı konu hakkındaki davaların, başka bir Üye Devlet'teki bir mahkemede devam ettiği hâllerde, davayı ilk ele alan mahkeme haricindeki yetkili mahkemeler söz konusu davaları askıya alabilir.

3. Söz konusu davaların ilk derece mahkemesinde devam ettiği hâllerde, davayı ilk ele alan mahkemenin bu davalara ilişkin yargı yetkisinin bulunması ve hukukunun davaların birleştirilmesine olanak tanıması hâlinde, taraflardan birinin başvurusu üzerine, davayı ilk ele alan mahkeme haricindeki herhangi bir mahkeme, yetkisizlik kararı da verebilir.

Madde 82

Tazminat hakkı ve sorumluluk

1. Bu Tüzük'ün ihlali nedeniyle maddi veya manevi zarar gören herkes, uğradığı zarara ilişkin olarak veri sorumlusu veya veri işleyenden tazminat alma hakkına sahiptir.

2. İşleme faaliyetine müdahil herhangi bir veri sorumlusu bu Tüzük'ü ihlâl eden işlemenin sebep olduğu zarardan sorumludur. Veri işleyen, ancak bu Tüzük'ün özellikle veri işleyenlere yönelik yükümlülüklerine uyum göstermediği veya veri sorumlusunun hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hâllerde, işlemenin sebep olduğu zarardan sorumludur.

3. Zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığını kanıtlaması hâlinde, veri sorumlusu veya veri işleyen 2. paragraf kapsamındaki sorumluluktan muaftır.

4. Birden fazla veri sorumlusu veya veri işleyenin ya da hem bir veri sorumlusu hem de bir veri işleyenin aynı işlemeye müdahil olduğu ve 2 ve 3. paragraflar çerçevesinde, işlemenin sebep olduğu herhangi bir zarardan sorumlu olduğu hâllerde, veri öznesinin zararının etkili bir şekilde

tazmininin sağlanması amacıyla, her bir veri sorumlusu veya veri işleyen tüm zarardan sorumludur.

5. Veri sorumlusu veya veri işleyenin, uğranan zararı 4. paragraf uyarınca eksiksiz bir şekilde tazmin ettiği hâllerde, söz konusu veri sorumlusu veya veri işleyenin, aynı işlemeye müdahil diğer veri sorumlusu veya veri işleyenlerden zarardan sorumlu oldukları kısma tekabül eden tazminat kısmını, 2. paragrafta ortaya konan koşullar uyarınca, talep etme hakkı bulunur.

6. Tazminat alma hakkının kullanımına ilişkin davalar Üye Devlet hukuku çerçevesinde yetkili olan 79(2) maddesinde atıfta bulunulan mahkemelerde açılır.

Madde 83

İdari para cezaları kesilmesine ilişkin genel koşullar

1. Denetim makamları, bu Tüzük'ün 4, 5 ve 6. paragraflarda atıfta bulunulan ihlalleri ile ilgili olarak bu madde uyarınca idari para cezaları kesilmesinin her münferit durumda etkili, orantılı ve caydırıcı olmasını sağlar.

2. İdari para cezaları, her münferit durumun koşullarına bağlı olarak, 58(2) maddesinin (a) ilâ (h) ve (j) bentlerinde atıfta bulunulan tedbirlere ek olarak veya bu tedbirler yerine kesilir. Her münferit durumda, idari para cezası kesilip kesilmeyeceğine ve idari para cezasının meblağına karar verilirken, aşağıdaki hususlar dikkate alınır:

(a) ilgili işlemenin mahiyeti, kapsamı veya amacı dikkate alındığında ihlalin mahiyeti, ağırlığı ve süresinin yanı sıra etkilenen veri öznesi sayısı ve veri öznelerinin uğradığı zararın düzeyi;

(b) ihlalin kasıtlı olması veya ihmalden kaynaklanması;

(c) veri öznelerinin uğradığı zararın azaltılması için veri sorumlusu veya veri işleyen tarafından gerçekleştirilen herhangi bir eylem;

(d) 25 ve 32. maddeler uyarınca kendileri tarafından uygulanan teknik ve kurumsal tedbirler dikkate alındığında, veri sorumlusu veya veri işleyenin sorumluluk derecesi;

(e) veri sorumlusu veya veri işleyenin konuyla ilgili önceki ihlalleri;

(f) ihlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacıyla denetim makamı ile gerçekleştirilen işbirliği derecesi;

(g) ihlalden etkilenen kişisel veri kategorileri;

(h) veri sorumlusu veya veri işleyenin ihlali bildirip bildirmediği ve bildirdiyse ne ölçüde bildirdiği başta olmak üzere, denetim makamının ihlalden haberdar olma şekli;

(i) 58(2) maddesinde atıfta bulunulan tedbirlerin, ilgili veri sorumlusu veya veri işleyene karşı aynı konu ile ilgili olarak daha önceden alınmış olduğu hâllerde, bu tedbirlere uyum;

(j) 40. madde uyarınca onaylı davranış kurallarına veya 42. madde uyarınca onaylı belgelendirme mekanizmalarına riayet edilmesi;

(k) ihlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi durumun özellikleri açısından geçerli diğer tüm ağırlaştırıcı veya hafifletici unsurlar.

3. Veri sorumlusu veya veri işleyenin aynı veya bağlantılı işleme faaliyetlerine ilişkin olarak bu Tüzük'ün çeşitli hükümlerini kasıtlı olarak veya ihmal suretiyle ihlal etmesi durumunda, idari para cezasının toplam meblağı en ağır ihlal için belirtilen meblağı aşamaz.

4. Aşağıdaki hükümlerin ihlâlleri, 2. paragraf uyarınca, yüksek olan meblağ geçerli olmak üzere, 10.000.000 EUR'a kadar veya bir teşebbüs olması hâlinde, bir önceki mali yılın yıllık dünya çapındaki toplam cirosunun %2'sine kadar idari para cezalarına tabidir:

(a) veri sorumlusu ve veri işleyenin 8, 11, 25 ilâ 39 ile 42 ve 43. maddeler uyarınca yükümlülükleri;

(b) belgelendirme organının 42 ve 43. maddeler uyarınca yükümlülükleri;

(c) izleme organının 41(4) maddesi uyarınca yükümlülükleri .

5. Aşağıdaki hükümlerin ihlâlleri, 2. paragraf uyarınca, yüksek olan meblağ geçerli olmak üzere, 20.000.000 EUR'a kadar veya bir teşebbüs olması hâlinde, bir önceki mali yılın yıllık dünya çapındaki toplam cirosunun %4'üne kadar idari para cezalarına tabidir:

(a) 5, 6, 7 ve 9. maddeler uyarınca rıza koşulları da dâhil olmak üzere işlemeye ilişkin temel ilkeler;

(b) veri öznelerinin 12 ilâ 22. maddeler uyarınca hakları;

(c) 44 ilâ 49. maddeler uyarınca bir üçüncü ülkedeki veya bir uluslararası kuruluştaki bir alıcıya kişisel veri aktarımları;

(d) IX. Bölüm çerçevesinde Üye Devlet hukuku uyarınca kabul edilen her türlü yükümlülük;

(e) 58(2) maddesi uyarınca denetim makamı tarafından verilen bir talimata veya getirilen geçici ya da kesin işleme sınırlamasına veya veri akışlarını askıya almasına uygun hareket edilmemesi veya 58(1) maddesinin ihlal edilmesi suretiyle erişim sağlanmaması.

6. Denetim makamının, 58(2) maddesinde atıfta bulunulan bir talimatına uygun hareket edilmemesi, 2. paragraf uyarınca, yüksek olan meblağ geçerli olmak üzere, 20.000.000 EUR'a kadar veya bir teşebbüs olması hâlinde, bir önceki mali yılın yıllık dünya çapındaki toplam cirosunun %4'üne kadar idari para cezalarına tabidir.

7. Denetim makamlarının 58(2) maddesi uyarınca düzeltme yetkilerine halel gelmeksizin her Üye Devlet, söz konusu Üye Devlet'te kurulu olan kamu makamlarına ve organlara idari para cezalarının kesilip kesilemeyeceğine ve ne ölçüde kesilebileceğine ilişkin kurallar belirleyebilir.

8. Bu madde kapsamındaki yetkilerin denetim makamı tarafından kullanılması, etkili yargı yolu ve yargı süreci de dâhil olmak üzere, Birlik ve Üye Devlet hukuku uyarınca uygun usuli güvencelere tabidir.

9. Üye Devlet'in hukuk sisteminde idari para cezalarının öngörülmediği hâllerde bu madde, söz konusu yargı yollarının etkili olması ve denetim makamları tarafından kesilen idari para cezaları ile eşdeğer bir etkiye sahip olması sağlanarak, para cezası yetkili denetim makamı tarafından girişimde bulunulacak ve yetkili ulusal mahkemeler tarafından kesilecek şekilde uygulanabilir. Her hâlükârda, kesilen para cezaları etkili, orantılı ve caydırıcı olur. Söz konusu Üye Devletler, bu paragraf uyarınca kabul ettikleri mevzuat hükümlerini 25 Mayıs 2018 tarihine kadar ve bunları etkileyen müteakip değişiklik mevzuatını veya değişiklikleri, gecikmeksizin, Komisyona bildirirler.

Madde 84

Cezalar

1. Üye Devletler, 83. madde uyarınca idari para cezalarına tabi olmayan ihlaller başta olmak üzere bu Tüzük'ün ihlalleri açısından geçerli olan diğer cezalara ilişkin kuralları belirlerler ve

bunların uygulanmasının sağlanması amacıyla gereken tüm tedbirleri alırlar. Söz konusu cezalar etkili, orantılı ve caydırıcı olur.

2. Her Üye Devlet, 1. paragraf uyarınca kabul ettiği mevzuat hükümlerini 25 Mayıs 2018 tarihine kadar ve bunları etkileyen sonraki değişiklikleri, gecikmeksizin Komisyona bildirir.

BÖLÜM IX

Özel işleme durumlarına ilişkin hükümler

Madde 85

İşleme ve ifade özgürlüğü ve bilgi edinme hakkı

1. Üye Devletler, mevzuat yoluyla, bu Tüzük uyarınca kişisel verilerin korunması hakkı ile gazetecilik amaçları ve akademik, sanatsal veya edebi anlatım amaçları doğrultusunda işleme dâhil olmak üzere, ifade özgürlüğü ve bilgi edinme hakkını bağdaştırırlar.

2. Gazetecilik amaçları veya akademik, sanatsal veya edebi anlatım amacıyla gerçekleştirilen işleme için, Üye Devletler, kişisel verilerin korunması hakkı ile ifade özgürlüğü ve bilgi edinme hakkını bağdaştırma amacıyla gerekli olmaları durumunda, II. Bölüm (ilkeler), III. Bölüm (veri öznesinin hakları), IV. Bölüm (veri sorumlusu ve veri işleyen), V. Bölüm (kişisel verilerin üçüncü ülkeler veya uluslararası kuruluşlara aktarılması), VI. Bölüm (bağımsız denetim makamları), VII. Bölüm (işbirliği ve tutarlılık) ve IX. Bölüm (belirli veri işleme durumları) ile ilgili olarak muafiyetler veya derogasyonlar sağlarlar.

3. Her Üye Devlet, 2. paragraf uyarınca kabul ettiği mevzuat hükümlerini ve bunları etkileyen müteakip değişiklik mevzuatını veya değişiklikleri, gecikmeksizin Komisyona bildirir.

Madde 86

Resmi belgelerin işlenmesi ve resmi belgelere kamunun erişimi

Bir kamu makamı veya bir kamu organı ya da bir özel organ tarafından kamu yararına yürütülen bir görevin ifası için tutulan resmi belgelerde yer alan kişisel veriler, resmi belgelere kamunun erişiminin bu Tüzük uyarınca kişisel verilerin korunması hakkıyla bağdaştırılması amacıyla, Birlik hukuku veya kamu makamı ya da organının tabi olduğu Üye Devlet hukuku uyarınca söz konusu makam veya organ tarafından açıklanabilir.

Madde 87

Ulusal kimlik numarasının işlenmesi

Üye Devletler, bir ulusal kimlik numarasının veya genel uygulama kapsamındaki başka bir kimlik belirleyicinin işlenmesine özgü koşulları da belirleyebilirler. Bu durumda, ulusal kimlik numarası veya genel uygulama kapsamındaki başka bir kimlik belirleyici, ancak veri öznesinin bu Tüzük uyarınca hakları ve özgürlüklerine ilişkin uygun güvenceler çerçevesinde kullanılır.

Madde 88

İstihdam kapsamında işleme

1. Üye Devletler, özellikle işe alım, mevzuatla ya da toplu sözleşmeler yoluyla belirtilen yükümlülüklerin sona ermesi de dâhil olmak üzere iş sözleşmesinin ifası, işin yönetimi, planlanması ve düzenlenmesi, iş yerinde eşitlik ve çeşitlilik, iş sağlığı ve güvenliğinin yönetimi,

planlanması ve düzenlenmesi, işverenin veya müşterinin mallarının korunması ile ilgili amaçlar ve istihdam ile ilgili haklar ve menfaatlerin münferit ya da toplu olarak kullanımı ve bunlardan yararlanılmasına ilişkin amaçlar ve iş ilişkisinin sona erdirilmesi amacı doğrultusunda çalışanların kişisel verilerinin istihdam bağlamında işlenmesi bakımından hakların ve özgürlüklerin korunmasının sağlanması amacıyla mevzuatla veya toplu sözleşmeler yoluyla daha özel kurallar belirleyebilirler.

2. Bu kurallar özellikle işlemenin şeffaflığı, teşebbüsler grubu veya ortak bir ekonomik faaliyette bulunan işletmeler grubu içinde kişisel verilerin aktarılması ve iş yerindeki izleme sistemleri ile ilgili olarak, veri öznesinin insanlık onuru, meşru menfaatleri ve temel haklarının güvence altına alınmasına ilişkin uygun ve özel tedbirleri içerir.

3. Her Üye Devlet, 1. paragraf uyarınca kabul ettiği mevzuat hükümlerini 25 Mayıs 2018 tarihine kadar ve bunları etkileyen sonraki değişiklikleri, gecikmeksizin Komisyona bildirir.

Madde 89

Kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlemeye ilişkin güvenceler ve derogasyonlar

1. Kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme veri öznesinin hakları ve özgürlükleri açısından bu Tüzük uyarınca uygun güvencelere tabidir. Söz konusu güvenceler ile özellikle veri minimizasyonu ilkesine uygun hareket edilmesinin sağlanması amacıyla teknik ve kurumsal tedbirlerin uygulamaya konulması sağlanır. Bu tedbirler, söz konusu amaçlara bu şekilde ulaşmanın mümkün olduğu durumlarda, takma ad kullanımını içerebilir. Bu amaçlara veri öznelerinin kimliklerinin belirlenmesine imkân vermeyen veya artık imkân vermeyen sonraki işleme ile ulaşılabildiği hâllerde, söz konusu amaçlara bu şekilde ulaşılır.

2. Kişisel verilerin bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlendiği hâllerde, Birlik veya Üye Devlet hukuku, 15, 16, 18 ve 21. maddelerde atıfta bulunulan hakların belirli amaçlara ulaşılmasını imkânsız hale getirmesinin veya ulaşılmasına ciddi şekilde zarar vermesinin muhtemel olduğu ve bu tür derogasyonların bu amaçlara ulaşılması için gerekli olduğu ölçüde, bu maddenin 1. paragrafında atıfta bulunulan koşullar ve güvencelere tabi olarak söz konusu haklardan derogasyonlar öngörebilir.

3. Kişisel verilerin kamu yararına arşivleme amaçları doğrultusunda işlendiği hâllerde, Birlik veya Üye Devlet hukuku, 15, 16, 18, 19, 20 ve 21. maddelerde atıfta bulunulan hakların belirli amaçlara ulaşılmasını imkânsız hale getirmesinin veya ulaşılmasına ciddi şekilde zarar vermesinin muhtemel olduğu ve bu tür derogasyonların bu amaçlara ulaşılması için gerekli olduğu ölçüde, bu maddenin 1. paragrafında atıfta bulunulan koşullar ve güvencelere tabi olarak söz konusu haklardan derogasyonlar öngörebilir.

4. 2 ve 3. paragrafta atıfta bulunulan işlemenin aynı zamanda başka bir amaca hizmet ettiği hâllerde, derogasyonlar yalnızca bu paragraflarda atıfta bulunulan amaçlara yönelik işlemeye uygulanır.

Madde 90

Sır saklama yükümlülükleri

1. Üye Devletler, kişisel verilerin korunması hakkı ile sır saklama yükümlülüğünün bağdaştırılması amacıyla gerekli ve orantılı olduğu hâllerde, Birlik veya Üye Devlet hukuku ya da ulusal yetkili makamlar tarafından konulan kurallar çerçevesinde bir mesleki sır saklama yükümlülüğüne ya da diğer eşdeğer sır saklama yükümlülüklerine tabi veri sorumluları veya

veri işleyenler ile ilgili olarak, denetim makamlarının 58(1) maddesinin (e) ve (f) bentlerinde belirtilen yetkilerini ortaya koymak üzere özel kurallar kabul edebilirler. Bu kurallar yalnızca veri sorumlusu veya veri işleyenin söz konusu sır saklama yükümlülüğü kapsamına giren bir faaliyet sonucu aldığı veya bu faaliyet esnasında elde ettiği kişisel veriler açısından uygulanır.

2. Her Üye Devlet, 1. paragraf uyarınca kabul edilen kuralları 25 Mayıs 2018 tarihine kadar ve bunları etkileyen sonraki değişiklikleri, gecikmeksizin Komisyona bildirir.

Madde 91

Kiliseler ve dini cemiyetlerin mevcut veri koruma kuralları

1. Bir Üye Devlet'te bulunan kiliseler ve dini cemiyetler ya da toplulukların, bu Tüzük'ün yürürlüğe giriş tarihinde, gerçek kişilerin işleme ile ilgili olarak korunmasına ilişkin kapsamlı kurallar uyguladığı hâllerde, bu Tüzük'e uygun hale getirilmesi koşuluyla, söz konusu kurallar uygulanmaya devam edebilir.

2. Bu maddenin 1. paragrafı uyarınca kapsamlı kurallar uygulayan kiliseler ve dini cemiyetler, bu Tüzük'ün VI. Bölümünde ortaya konan şartları yerine getirmesi koşuluyla, özel nitelikte olabilecek bağımsız bir denetim makamının denetimine tabidir.

BÖLÜM X

Yetki devrine dayanan tasarruflar ve uygulama tasarrufları

Madde 92

Yetki devrinin uygulaması

1. Yetki devrine dayanan tasarrufları kabul etme yetkisi bu maddede belirtilen koşullara tabi olarak Komisyona verilir.

2. 12(8) maddesi ve 43(8) maddesinde atıfta bulunulan yetki devri, 24 Mayıs 2016 tarihinden itibaren belirsiz bir süre için Komisyona verilir.

3. 12(8) maddesi ve 43(8) maddesinde atıfta bulunulan yetki devri, Avrupa Parlamentosu veya Konsey tarafından her zaman kaldırılabilir. Bir kaldırma kararı, söz konusu kararda belirtilen yetki devrini sona erdirir. Bu karar, *Avrupa Birliği Resmi Gazetesi*'nde yayımlanmasından sonraki gün veya kararda belirtilen sonraki bir tarihte hüküm doğurur. Karar hâlihazırda yürürlükte bulunan yetki devrine dayanan tasarrufların geçerliliğine halel getirmez.

4. Komisyon, yetki devrine dayanan bir tasarrufu kabul eder etmez, bunu eş zamanlı olarak Avrupa Parlamentosu ve Konseye iletir.

5. 12(8) maddesi ve 43(8) maddesi uyarınca kabul edilen yetki devrine dayanan bir tasarruf, ancak söz konusu tasarrufun Avrupa Parlamentosu ve Konseye iletilmesinden itibaren üç aylık bir süre içinde Avrupa Parlamentosu ya da Konsey tarafından herhangi bir itirazda bulunulmaması durumunda ya da, söz konusu sürenin dolmasından önce, hem Avrupa Parlamentosu hem de Konseyin itirazda bulunmayacağını Komisyona bildirmesi hâlinde, yürürlüğe girer. Bu süre Avrupa Parlamentosu veya Konseyin inisiyatifiyle üç ay uzatılır.

Madde 93

Komite usulü

1. Komisyona bir komite tarafından yardımcı olunur. Söz konusu komite, (AB) 182/2011 sayılı Tüzük kapsamında bir komitedir.

2. Bu paragrafa atıfta bulunulan hâllerde, (AB) 182/2011 sayılı Tüzük'ün 5. maddesi uygulanır.

3. Bu paragrafa atıfta bulunulan hâllerde, (AB) 182/2011 sayılı Tüzük'ün 8. maddesi, ilgili Tüzük'ün 5. maddesi ile bağlantılı olarak, uygulanır.

BÖLÜM XI

Nihai hükümler

Madde 94

95/46/AT sayılı Direktif'in yürürlükten kaldırılması

1. 95/46/AT sayılı Direktif 25 Mayıs 2018 tarihinden itibaren yürürlükten kaldırılmıştır.

2. Yürürlükten kaldırılan Direktif'e yapılan atıflar bu Tüzük'e yapılmış gibi yorumlanır. 95/46/AT sayılı Direktif'in 29. maddesi ile kurulan Kişisel Verilerin İşlenmesiyle ilgili olarak Bireylerin Korunması hakkında Çalışma Grubuna yapılan atıflar bu Tüzük ile kurulan Avrupa Veri Koruma Kurulu'na yapılmış gibi yorumlanır.

Madde 95

2002/58/AT sayılı Direktif ile ilişki

Bu Tüzük, Birlik içinde kamu iletişim ağlarında kamuya açık elektronik iletişim hizmetlerinin sağlanması ile bağlantılı işleme hususunda, gerçek veya tüzel kişilere, 2002/58/AT sayılı Direktif'te belirtilen aynı hedefe yönelik belirli yükümlülüklere tabi bulundukları konular ile ilgili olarak, ek yükümlülükler getirmez.

Madde 96

Önceden imzalanan anlaşmalarla ilişki

Kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasını içeren, Üye Devletler tarafından 24 Mayıs 2016 tarihinden önce imzalanan ve bu tarihten önce geçerli Birlik hukuku ile uyumlu olan uluslararası anlaşmalar, değiştirilene, yenilenene veya yürürlükten kaldırılana kadar yürürlükte kalır.

Madde 97

Komisyon raporları

1. Komisyon, bu Tüzük'ün değerlendirilmesi ve gözden geçirilmesine ilişkin bir raporu, 25 Mayıs 2020 tarihine kadar ve bu tarihten sonra dört yılda bir, Avrupa Parlamentosu ve Konseye sunar. Raporlar kamuya açıklanır.

2. 1. paragrafta atıfta bulunulan değerlendirmeler ve gözden geçirmeler bağlamında, Komisyon özellikle aşağıdaki hususların uygulanmasını ve işleyişini inceler:

(a) bu Tüzük'ün 45(3) maddesi uyarınca alınan kararlar ve 95/46/AT sayılı Direktif'in 25(6) maddesine dayanılarak alınan kararlar başta olmak üzere, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına ilişkin V. Bölüm;

(b) işbirliği ve tutarlılığa ilişkin VII. Bölüm.

3. 1. paragrafın amacı doğrultusunda Komisyon, Üye Devletlerden ve denetim makamlarından bilgi talep edebilir.

4. Komisyon, 1 ve 2. paragraflarda atıfta bulunulan değerlendirmeler ve gözden geçirmeleri gerçekleştirirken, Avrupa Parlamentosu, Konsey ve diğer ilgili organlar veya kaynakların tutumlarını ve bulgularını dikkate alır.

5. Komisyon, gerekmesi hâlinde, özellikle bilgi teknolojisindeki gelişmeleri dikkate alarak ve bilgi toplumundaki ilerleme durumu doğrultusunda, bu Tüzük'te değişiklik yapılmasına ilişkin uygun önerilerde bulunur.

Madde 98

Birlik'in veri korumaya ilişkin diğer hukuki tasarruflarının gözden geçirilmesi

Komisyon, uygun olduğu hâllerde, gerçek kişilerin işleme ile ilgili olarak standart ve tutarlı bir şekilde korunmasının sağlanması amacıyla, Birlik'in kişisel verilerin korunmasına ilişkin diğer hukuki tasarruflarında değişiklik yapılmasına yönelik yasama önerilerinde bulunur. Bu husus, özellikle gerçek kişilerin Birlik kurumları, organları, ofisleri ve ajansları tarafından gerçekleştirilen işleme ile ilgili olarak korunması ve söz konusu verilerin serbest dolaşımına ilişkin kurallarla ilgilidir.

Madde 99

Yürürlük ve uygulama

1. Bu Tüzük, *Avrupa Birliği Resmi Gazetesi*'nde yayımlandığı günden sonraki yirminci gün yürürlüğe girer.

2. Bu Tüzük, 25 Mayıs 2018 tarihinden itibaren uygulanır.

Bu Tüzük, bütün unsurlarıyla bağlayıcıdır ve tüm Üye Devletlerde doğrudan uygulanır.

Brüksel'de, 27 Nisan 2016 tarihinde düzenlenmiştir.

Avrupa Parlamentosu adına
M. SCHULZ
Başkan

Konsey adına
J.A. HENNIS-PLASSCHAERT
Başkan