

GENEL VERİ KORUMA TÜZÜĞÜ (GDPR) VE GETİRDİĞİ YENİLİKLER

Doç. Dr. Murat Volkan Dülger

Kişisel Verilerin Korunması Hakkı

- Uzun bir süre “*özel hayatın gizliliği*” veya “*özel ve aile hayatına saygı*” başlıkları altında değerlendirilmiştir.
- Zamanla bu hakların kapsamlarının birbirinden farklılığı kabul edilmiş ve “*kişisel verilerin korunması hakkı*” temel haklar içerisinde, ayrı ve bağımsız bir hak olarak değerlendirilmeye başlanmıştır.

Avrupa Genel Veri Koruma Tüzüğü'nün Ortaya Çıkışı

- ▢ 95/46/EC Sayılı Direktif, farklı ülkelerde farklı şekillerde yorumlanması sebebiyle iç hukuklara yeknesak olarak aktarılamamıştır.
- ▢ Değişen ve gelişen teknoloji ile AB ülkelerinde kişisel verilerin korunması hukukunun yeknesaklaştırılması gerekliliği yeni bir düzenleme yapılması gerekliliği doğurmuştur.
- ▢ GDPR, 95/46/EC sayılı AB Veri Koruma Direktifinin yerine geçmektedir.

Avrupa Genel Veri Koruma Tüzüğü (GDPR)

- ▢ Kişisel verilerin korunması alanında halihazırda var olan ilkelerin modernize edilmesi ve kişisel verilerin korunması hukukunun yeknesaklaştırılması amacıyla 24 Mayıs 2016 tarihinde Avrupa Genel Veri Koruma Tüzüğü kabul edilmiştir.
- ▢ Regülasyon için iki yıllık bir geçiş süresi belirlenmiş ve uygulama tarihi 25 Mayıs 2018 olarak öngörülmüştür.

GDPR

- GDPR 99 maddeden oluşturmaktadır ve 173 Gerekçesi (Recital) bulunmaktadır.
- GDPR 11 ana bölümden oluşmaktadır:
 - Bölüm 1: Genel Hükümler
 - Bölüm 2: İlkeler
 - Bölüm 3: Veri Sahibinin Hakları
 - Bölüm 4: Veri Sorumlusu ve Veri İşleyen
 - Bölüm 5: Üçüncü Ülkeler veya Uluslararası Kuruluşlara Veri Aktarımları
 - Bölüm 6: Bağımsız Denetim Makamları
 - Bölüm 7: İş Birliği ve Tutarlılık
 - Bölüm 8: Kanun Yolları, Sorumluluk ve Yaptırımlar
 - Bölüm 9: Özel İşleme Durumlarına İlişkin Hükümler
 - Bölüm 10: Yetki Devrine Dayanan Tasarruflar ve Uygulama Tasarrufları
 - Bölüm 11: Nihai Hükümler

Temel Kavramlar (m. 4) - I

- **“Kişisel veri”:** belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi.
 - Bir kişinin belirlenebilir olup olmadığı değerlendirilirken; o bireyin belirlenmesi için direkt veya dolaylı olarak kullanılabilecek ve o bireye diğerlerinden farklı bir muamelede bulunulmasını mümkün kılabilecek makul her türlü araç dikkate alınmalıdır.
- **“Veri sahibi”:** kişisel verileri işlenen gerçek kişi.
- **“Veri sorumlusu”:** yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ.
- **“Veri işleyen”:** veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ.
 - Veri sorumlusu ve veri işleyen arasındaki ayrım: veri sorumlusu, veri işlemenin amaçlarını ve yöntemlerini belirleyen tüzel veya gerçek kişi olup, veri işleyen ise veri sorumlusu adına ve onun talimatları uyarınca veri işlemeyi gerçekleştirmektedir.

Temel Kavramlar (m. 4) - II

- **“Özel nitelikli kişisel veriler”:** Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin veriler.
- **“Kişisel veri ihlali”:** iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlali.

Tüzüğün Uygulama Alanı (m. 3)-I

- Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır.
- Tüzük, veri sorumlusu ve veri işleyen kişilere uygulanacaktır. Dolayısıyla, veri korunmasına ilişkin sorumluluklar bu kişiler üzerinde doğacaktır.
- Tüzük, Birlik içerisindeki bir veri sorumlusu veya işleyicinin işletmesinin veri işleme faaliyetlerine uygulanacağı gibi, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin işlenmesine de uygulanır.

Tüzüğün Uygulama Alanı (m. 3)-II

1. Bu Tüzük, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir veri sorumlusu veya işleyenin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır.
2. Bu Tüzük, işleme faaliyetlerinin aşağıdaki hususlarla alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir veri sorumlusu veya işleyen tarafından işlenmesine uygulanır:
 - a. Veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması veya
 - b. Davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi.
3. Bu Tüzük, yalnızca Birlik içerisinde değil, ancak bir üye devletin hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde kurulu bulunan bir veri sorumlusu tarafından kişisel verilerin işlenmesine de uygulanır.

Tüzüğün Uygulama Alanı (m. 3)-III

- ❖ ABAD, yerel veri koruma yasalarının coğrafi kapsamını incelediği *Weltimmo* kararında (C-230/14, 1 Ekim 2015), «kuruluş» (establishment) kavramının geniş yorumlanması gerektiğini belirtmiştir. Bu doğrultuda, bir şirketin farklı bir ülke hukukuna göre kurulmuş olmasına rağmen başka bir ülkede istikrarlı ve etkin bir biçimde faaliyet göstermesi halinde, şirketin bu ülke sınırları içerisinde de kurulmuş olduğu kabul edilerek değerlendirme yapılacaktır.

Temel İlkeler (m. 5)

- ▢ Hukuka Uygunluk, Adillik ve Şeffaflık
- ▢ Belirli, Açık ve Meşru Amaçlara Yönelik İşleme (Amaçın Sınırlandırılması İlkesi)
- ▢ Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması (Veri Minimizasyonu)
- ▢ Doğru ve Gerektiğinde Güncel Tutulma
- ▢ Verilerin Amaç İçin Gereken Süre Kadar Muhafaza Edilmesi (Sınırlı Süre Saklama İlkesi)
- ▢ Veri Güvenliği İlkesi
- ▢ Hesap Verebilme Zorunluluğu

Hukuka Uygunluk, Adillik ve Şeffaflık (m. 5/1/a)

❑ Hukuka Uygunluk (m. 6)

- ❑ Veri işlemenin, veri sahibinin rızası veya Tüzükte düzenlenmiş diğer bir hukuka uygunluk sebebine dayanılarak gerçekleştirilmesi gereklidir.

❑ Adillik

- İşleme faaliyetine dayanak yapılan hukuk normları adalete uygun olarak düzenlenmiş olmalıdır.
- Veri sorumluları; veri sahiplerini ve kamuyu, verileri hukuka uygun ve şeffaf bir şekilde işleyecekleri konusunda haberdar etmelidir.
- Veri sorumluları veri işleme faaliyetlerinin Tüzüğe uygun olarak gerçekleştirildiğini gösterebilecek durumda olmalıdır.

❖ *AIHM, K.H. ve Diğerleri v. Slovakya*

❑ Şeffaflık (m. 12)

- Veri sorumluları, veri sahiplerini, verilerinin nasıl kullanıldığı ile ilgili bilgilendirmelidir.
- Bu kapsamdaki her türlü bildirim “öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak” veri sahibine sağlanmalıdır.
- İşleme faaliyeti başlamadan önce yapılan bilgilendirmeler, işleme sırasında veri sahiplerinin erişimine hazır bulunan bilgiler ve veri sahiplerinin erişim talebi üzerine verilen bilgiler bu kapsamdadır.
- Kişisel verilerinin işlenmesinin riskleri, kuralları, koruyucuları, amaçları ve işlemeye ilişkin veri sahiplerinin hakları, ilgili kişiler için açık ve net olmalıdır.

❖ *AIHM, Haralambie v. Romanya.*

Belirli, Açık ve Meşru Amaçlara Yönelik İşleme (Amaçın Sınırlandırılması İlkesi) (m. 5/1/b)

- ❑ Kişisel veriler belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve yalnızca bu amaçlara uygun bir şekilde işlenebilir.
- ❑ İlk amaç ile bağdaşmayan başka bir amaçla veri işleme faaliyetinin gerçekleştirilebilmesi için, sonraki işlemlere yönelik veri sahibinin tekrar rızası alınmalı veya işleme faaliyeti başka bir hukuki dayanağa sahip olmalıdır. Ancak amaçlar bağdaşıyorsa tekrar rıza almaya gerek yoktur!
- ❑ Bu kapsamda; iki amaç arasındaki ilişki, kişisel verilerin toplandığı bağlam, veri sahiplerinin makul beklentileri, kişisel verilerin niteliği, planlanan ilave işlemin veri sahipleri açısından sonuçları, uygun korumaların varlığı gibi faktörler dikkate alınmalıdır.
- ❑ Kamu yararına arşivleme, bilimsel veya tarihi araştırma veya istatistiki amaçlarla işleme faaliyetleri baştaki amaçlara *a priori* olarak uygundur.

Verilerin İşlendikleri Amaçla Bağılantılı, Sınırlı ve Ölçülü Olması (Veri Minimizasyonu) (m. 5/h/c)

- Kişisel veriler, işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlı olmalıdır.
 - 95/46/EC sayılı Direktif ve 108 No'lu Sözleşme'de ise verilerin toplanmasının “*gerekli olanla sınırlı olması*” yerine “*aşırı olmaması*” gerektiği düzenlenmiştir.
- ❖ ABAD, *Digital Rights Ireland*.

Doğru ve Gerektiğinde Güncel Tutulma (m. 5/1/d)

- Kişisel veriler doğru ve gerektiğinde güncel tutulmalıdır.
 - Tüzüğün lafzından da anlaşıldığı üzere, kişisel verilerin güncel tutulması “*gerektiğinde*” sağlanmalıyken, kişisel verilerin doğruluğu için böyle bir parantez açılmamıştır. Bu doğrultuda, bazı verilerin mutlaka düzenli olarak kontrol edilerek güncellenmesi gerekirken, bazı kaydedilmiş verilerin güncellenmesi ise hukuken yasaklanmıştır. Örneğin; bir medikal kayıttaki bulgular daha sonra yanlış oldukları anlaşılabilirse bile güncellenerek değiştirilmemelidir.
- İşlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır.

Verilerin Amaç İçin Gereken Süre Kadar Muhafaza Edilmesi (Sınırlı Süre Saklama İlkesi) (m. 5/t/e)

- ▮ Kişisel veriler, veri sahiplerinin, yalnızca kişisel verilerin işleme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan bir şekilde tutulmalıdır.
 - ▮ Kişisel verilerin kamu yararı için, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla arşivlenmesi durumunda bu veriler daha uzun süre saklanabilecektir.
 - ▮ Bu amaçla, veri sorumlusu tarafından verilerin silinmesi veya periyodik kontrolü için bazı zaman aralıkları belirlenmesi gerekir.
- ❖ *AIHM, S. and Marper.*

Veri Güvenliği İlkesi (m. 5/1/f)

▢ Veri sorumlusu;

- işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli riskleri dikkate alarak,
- hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında,
- veri koruma ilkelerinin etkili bir şekilde uygulanması ve Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak,
- yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere, gerekli güvencelerin entegre edilmesi amacı ile tasarlanan,

uygun teknik ve düzenlemeye ilişkin tedbirler uygulamalı ve veri sahiplerinin haklarını korumalıdır.

Hesap Verebilme Zorunluluğu (m. 5/2)

- ▢ Veri sorumlusu, Tüzükte düzenlenmiş ilkelere uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmek yükümlülüğü altındadır.
- ▢ Bu kapsamda izlenecek prosedürler ve kurulacaklar sistemler, veri işlemenin yarattığı risk ve verinin niteliğine bağlı olarak değişiklik gösterecektir.
- *Madde 29 Çalışma Grubu hesap verme zorunluluğunu; veri sorumlusunun, işleme faaliyetleri bağlamında ve olağan şartlarda veri koruma kurallarına bağlılığı sağlayacak tedbirler alması ve veri koruma kurallarına uygun hareket edildiğini veri sahipleri ve denetim makamlarına gösterecek gerekli belgeleri hazır bulundurması yükümlülüğü olarak özetlemiştir.*

Veri İşlemenin Kuralları-I

- ▢ Veri Sorumlusunun Genel Yükümlülükleri
 - ▢ Temsilci Atama Yükümlülüğü
 - ▢ Ortak Veri Sorumlularının İş Bölümü Anlaşması Yapma Yükümlülüğü
 - ▢ Veri İşleyenlerin Seçimi İle İlgili Yükümlülükler
- ▢ Veri İşlemede Hukuka Uygunluk Nedenleri
 - ▢ Rıza
 - ▢ İşlemenin Bir Sözleşmenin Kurulması veya İfası İçin Gerekli Olması
 - ▢ İşlemenin Veri Sorumlusunun Hukuki Yükümlüğünü Yerine Getirebilmesi İçin Zorunlu Olması
 - ▢ İşlemenin İlgili Kişinin veya Diğer Bir Gerçek Kişinin Hayati Menfaatlerini Korumak İçin Gerekli Olması
 - ▢ İşlemenin Kamu Yararı İçin Gerçekleştirilen Bir Görevin İfası İçin veya Veri Sorumlusunun Resmi Yetkisinin Kullanılması İçin Gerekli Olması
 - ▢ Veri İşlemenin Meşru Menfaatlere Ulaşmak Amacıyla Gerekli Olması
- ▢ Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

Veri İşlemenin Kuralları-II

- ▢ Veri İşlemenin Güvenliğine İlişkin Kurallar
 - ▢ Gizlilik
 - ▢ Kişisel Veri İhlali Bildirimi
- ▢ Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar
 - ▢ Veri Koruma Görevlileri
 - ▢ Faaliyetlerin Kaydı
 - ▢ Veri Koruma Etki Değerlendirmesi ve Ön İstişare
 - ▢ Davranış Kuralları (Codes of Conduct)
 - ▢ Belgelendirme
- ▢ Özel ve Olağan Veri Koruması
- ▢ Sınıraşan Veri Transferleri

Veri Sorumlusunun Genel Yükümlülükleri

❑ Temsilci Atama Yükümlülüğü (m. 27)

- Tüzüğün uygulama alanının AB üyesi ülkelerden daha geniş öngörülmüş olmasına paralel olarak, veri sorumlusu veya işleyen yazılı olarak Birlik içerisinde bir temsilci atamalıdır.
 - İşlemenin nadir olarak gerçekleştiği ve özel nitelikli kişisel verilerin büyük ölçekli olarak işlenmesinin söz konusu olmadığı hallerde -söz konusu işlemenin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebep olmasının muhtemel olmadığı sonucuna ulaşıyorsa- ve işlemenin bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi halinde bu yükümlülük doğmaz.

❑ Ortak Veri Sorumlularının İş Bölümü Anlaşması Yapma Yükümlülüğü (m. 26/ı)

- ❑ Birlik veya Üye Devlet hukuku tarafından belirlenmiş olmadıkça, ortak veri sorumlularının Tüzükte yer alan yükümlülüklerinin gerçekleştirilecek bir anlaşma ile şeffaf bir şekilde belirlemesi gerekmektedir.

❑ Veri İşleyenlerin Seçimi İle İlgili Yükümlülükler (m. 28/ı)

- Veri sorumlusu yalnızca işleme faaliyetinin Tüzüğün gerekliliklerinin yerine getirilmesini ve veri sahibinin haklarının korunmasını sağlayacak biçimde uygun teknik ve düzenlemeye ilişkin tedbirler uygulama hususunda yeterli güvenceler sağlayan veri işleyenleri kullanmalıdır.

Veri İşlemede Hukuka Uygunluk Nedeni: Rıza (m. 7)-I

- Veri sahibinin rızası, veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir.
 - KVKK'da tek başına rıza kavramı düzenlenmemiş olup, açık rıza tanımlanmıştır: *belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.*
 - Tüzükte sözcük olarak “açık rıza” kavramına yer verilmediyse de KVKK ile karşılaştırma yapıldığında “bilgilendirmeye dayalı bir rıza” alındığı için bunun da açık rızaya benzer olduğu görülür. Ancak bu husus etkisini aydınlatma yapılmadan hukuka uygun şekilde yapılan işlemlerde göstermektedir!
- Rıza bilinçli olmalıdır.
 - Madde 29 Çalışma Grubu yapılacak rıza alınmadan önce yapılacak bilgilendirmenin açık ve anlaşılabilir şekilde gerçekleştirilmesi ve işlenen veriler, işlemenin amaçları, verilerin muhtemel alıcıları ve veri sahibinin hakları gibi konularda tam ve eksizsiz bilgiler içermesi gerektiğini belirtmiştir.
- Rıza spesifik olmalıdır.
 - Rızanın hangi işleme faaliyetlerine yönelik olarak verildiği açıkça anlaşılabilmelidir.
- Veri sahibinin her zaman rızasını geri alma hakkı bulunmaktadır.
 - Veri sahibi, rıza vermeden önce bu hususta bilgilendirilmelidir.
 - Rızanın geri alınması, rızanın verilmesi kadar kolay olmalıdır.

Veri İşlemede Hukuka Uygunluk Nedeni: Rıza (m. 7)-II

- ▢ Rıza özgür bir şekilde verilmelidir.
 - ▢ Rızanın özgürce verilip verilmediği değerlendirilirken bir hizmetin sağlanması da dahil olmak üzere, bir sözleşmenin ifasının, söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlı olup olmadığına azami özen gösterilmelidir.
 - ▢ Bu husus rızanın bir şarta bağlanamaması anlamına da gelir. Veri sahibine seçim hakkı tanınmalıdır!
 - *Örneğin; Madde 29 Çalışma Grubu, işçilerin, işçi/işveren ilişkisinden kaynaklanan tabi olunuş nedeniyle neredeyse hiçbir zaman özgürce rıza verebilecek, rıza vermeyi reddedebilecek veya rızasını geri alabilecek bir pozisyonda olmadığını belirtmiştir.*

Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri (m. 9)-I

- Özel nitelikli kişisel verilerin işlenmesi kural olarak yasaktır.
- Özel nitelikli kişisel veriler ancak aşağıdaki hukuka uygunluk hallerinde işlenebilir:
 - (a) Veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;
 - (b) Birlik veya Üye Devlet hukuku çerçevesinde ya da Üye Devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, veri sorumlusunun veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;
 - (c) Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;
 - (d) İşleme faaliyetinin bir vakıf, birlik veya kâr amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;
 - (e) İşleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;

Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri (m. 9)-II

(f) Yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;

(g) Gözetilen amaçla orantılı olan, verinin korunması hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya Üye Devlet hukukuna dayalı olarak kayda değer ölçüde ağır basan kamu yararı olması halinde işleme faaliyetinin gerekmesi;

(h) Koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;

(i) Özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;

(j) Kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

Veri İşlemenin Güvenliğine İlişkin Kurallar (m. 32)-I

- Veri sorumlusu ve işleyen, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, uygun teknik ve düzenlemeye ilişkin tedbirler uygulamalıdır.

Veri İşlemenin Güvenliğine İlişkin Kurallar (m. 32)-II

□ Gizlilik (m. 5/ı/f)

- **Bütünlük ve gizlilik ilkesi:** Yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirlerin kullanılması suretiyle kişisel verilerin güvenliğini sağlayan bir şekilde işlenmesi gereklidir.
- Veri sorumlusu ile veri işleyen arasında veri işlemeye ilişkin sözleşmede, işleyenin, kışisel verileri işleme yetkisi bulunan kişilerin gizlilik taahhüdünde bulunmasını veya uygun bir yasal gizlilik yükümlülüğü altında bulunmasını sağlaması gerektiği belirtilmiştir.

Veri İşlemenin Güvenliğine İlişkin Kurallar (m. 32)-III

❑ Kişisel Veri İhlali Bildirimi (m. 33)

- Kişisel verilerin güvenliğinin ihlali halinde, ihlal, ilgili kişi için teşkil ettiği risk göz önünde bulundurularak, denetim makamına ve ilgili kişiye bildirilmelidir.
- Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, veri sorumlusu, gereksiz gecikmeye mahal vermeden ve uygun olması halinde, ihlalden haberdar olduktan itibaren “en geç 72 saat içerisinde”, kişisel veri ihlalini yetkili denetim makamına bildirmelidir.
- Gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesi muhtemel olan veri ihlallerini, veri sorumlusu, veri sahibine “gereksiz bir gecikmeye mahal vermeden” iletmelidir.
- Veri işleyen, bir kişisel veri ihlalden haberdar olduktan sonra, “herhangi bir gecikmeye mahal vermeden” veri sorumlusuna bildirimde bulunmalıdır.

Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar - I

□ Veri Koruma Görevlileri (m 37-39)

- Belirli durumlarda, veri sorumluları veri koruma kurallarına uygun faaliyet göstermesi hususunda onlara bilgi ve tavsiye verecek “veri koruma görevlileri” atayabilir. Bazı durumlarda ise veri koruma görevlisi atamak zorunludur.
- Veri koruma görevlisi atamanın zorunlu olduğu haller:
 - (i) işleme faaliyetinin bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi,
 - (ii) veri sorumlusu veya işleyenin temel faaliyetlerinin yapıları, kapsamı ve/veya amaçları gereği veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya
 - (iii) veri sorumlusu veya işleyenin temel faaliyetlerinin özel nitelikli kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi

Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar - II

- Bir veri koruma görevlisi atandığında, veri sorumlusu ve işleyen, bu kişinin kişisel verilerin korunmasına ilişkin tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlar.
- Veri koruma görevlisinin görevlerini efektif bir şekilde yerine getirebilmesi için, veri sorumluları ve veri işleyenler, ona gereken kaynakları sağlamalıdır.
- Veri koruma görevlileri bağımsız hareket etmelidir.
 - Veri sorumlusu ve işleyen, veri koruma görevlisinin görevlerini yerine getirmesi ile ilgili olarak hiçbir şekilde talimat almaması için gerekli önlemleri alır.
 - Veri koruma görevlisi, görevlerinin yerine getirilmesi nedeniyle veri sorumlusu ya da işleyen tarafından işten çıkarılamaz veya cezalandırılmaz

Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar - III

❑ Faaliyetlerin Kaydı (m. 30)

- Her veri sorumlusu ve uygun olduğu hallerde, veri sorumlusunun temsilcisi kendi sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutmalıdır.
- Faaliyetlerin kaydının tutulması;
 - Veri sorumlusunun işleme kurallarına uyumlu hareket ettiğini gösterilebilmesi ve dolayısıyla veri işleme faaliyetlerinden sorumlu tutulabilmesi için önemlidir.
 - Denetim makamlarının veri işlemenin hukuka uygunluğunu denetlemesine imkan tanır.
- Ayrıca veri işleyenler ve uygun olduğu hallerde, işleyen temsilcileri de bir veri sorumlusu adına gerçekleştirilen tüm kategorilerdeki işleme faaliyetlerine ilişkin olarak kayıt tutma yükümlülüğü altındadır.
- 250'den az kişi istihdam eden bir işletme veya kuruluş için veri sorumlusu veya veri işleyen için böyle bir yükümlülük doğmayacaktır.
 - Bu muafiyet için ayrıca veri sorumlusu veya işleyen gerçekleştirdiği işleme faaliyetlerinin veri sahiplerinin hakları ve özgürlükleri açısından bir riske sebebiyet vermesi muhtemel olmamalı, işleme faaliyetinin nadiren gerçekleştirilmeli veya işleme faaliyetinin özel nitelikli verileri kapsamamalıdır.

Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar - IV

❑ Veri Koruma Etki Değerlendirmesi ve Ön İstişare (m. 35-36)

- Veri işlemenin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusu, işleme faaliyetinden önce, bu işleme faaliyetinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapma yükümlülüğü altındadır.
 - Bu kapsamda veri işlemenin
 - (i) gerçek kişilerle ilgili kişisel özellikler hususunda, profil çıkarma da dahil olmak üzere, otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirmeyi;
 - (ii) özel nitelikli kişisel verilerin veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi veya
 - (iii) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi yüksek riskli kabul edilmektedir.
- ❑ Veri koruma etki değerlendirmesi sonucunda, veri sorumlusunun riski hafifletmek için tedbir almaması durumunda veri işlemenin bireylerin hakları için yüksek risk oluşturacağı anlaşılırsa, veri sorumlusunun işleme faaliyetinden önce denetim makamına danışması gerekir.

Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar - V

□ Davranış Kuralları (Codes of Conduct) (m. 40-41)

- Davranış kurallarının amacı, soyut ve teknik hukuk kurallarına, uygulamaya yönelik ve pratik bir yorum kazandırmaktır.
- Davranış kuralları birlikler ve veri sorumlusu veya veri işleyen kategorilerini temsil eden diğer organlar tarafından hazırlanabilir, değiştirilebilir veya kapsamı genişletilebilir.
- Davranış kuralları, Tüzüğün maddi olarak yorumlanmasının dışında; bu kurallara uyumluluğun izlenmesi için, kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan ve bu amaca yönelik olarak yetkin denetim makamı tarafından akredite edilen bir organın, söz konusu görevi gerçekleştirmesine olanak sağlayacak usul kurallarına da yer vermelidir.
- Davranış kuralları hazırlandıktan sonra, ilgili kuruluş/organ, kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağı yetkin denetim makamına ibraz eder. Denetim makamı bu taslağın Tüzük ile uyumlu olup olmadığı konusunda bir görüş sunar. Denetim makamı, yeterli güvenceleri sağladığını tespit etmesi durumunda söz konusu taslağı onaylar.

Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar - VI

□ Belgelendirme (m. 42-43)

- Veri koruma belgelendirme mekanizmaları, veri koruma mühürleri ve işaretleri (“belgelendirme”), veri sorumlusu ve işleyenlerin Tüzük ile uyumluluğunu göstermelerini sağlayabilecek yöntemlerdendir.
- Belgelendirme gönüllülük esasına dayanır ve şeffaf bir süreç vasıtasıyla sağlanır.
- Belgelendirme, yetkili denetim makamı veya belgelendirme organları tarafından sağlanabilir.
 - Belgelendirme organlarının yetkili denetim makamı veya ulusal akreditasyon organı tarafından akredite edilmesi gereklidir.

Özel ve Olağan Veri Koruması (m. 25)

❑ Özel Veri Koruması

- Veri sorumlusu, veri koruma ilkelerinin etkili bir şekilde uygulanması ve Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile uygun teknik ve düzenlemeye ilişkin tedbirler alarak veri sahiplerinin haklarını korunmasını sağlamalıdır.
- Bu tedbirleri belirler ve uygularken, veri sorumlusu, son teknolojiler, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri de dikkate almalıdır.

❑ Olağan Veri Koruması

- Veri sorumlusu, olağan durumlarda, yalnızca işleme amacı için gerekli olan kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve düzenlemeye ilişkin tedbirler almalıdır.

Sınırışan Veri Transferleri-I

▢ Sınırışan Veri Transferleri

- ▢ Avrupa Birlięi Komisyonunun Uygunluk Kararı erevesinde Aktarım
- ▢ Avrupa Birlięi Komisyonunun Uygunluk Kararı Bulunmayan Hallerde Aktarım
- ▢ Spesifik Durumlara Ynelik Hukuka Uygunluk Nedenleri
- ▢ Uluslararası Anlařmalara Dayalı Aktarımlar

Sınıraşan Veri Transferleri-II

- **Avrupa Birliği Komisyonunun Uygunluk Kararı Çerçevesinde Aktarım (m. 45)**
- Komisyon, bir 3. ülke veya söz konusu 3. ülke dahilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verebilir.
 - Böyle bir durumda spesifik bir onaya gerek olmaksızın bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleştirilebilir.
 - Yeterli düzeyde bir koruma sağlamak → 3. ülkenin temel hak ve özgürlüklere ilişkin olarak sağladığı korumanın temel olarak AB hukukunca sağlanan garantiler ile eş düzeyde olması gerekir (ABAD).

Sınırötesi Veri Transferleri-III

- Komisyon, yabancı ülkelerin yeterli düzeyde bir koruma sağlayıp sağlamadığına bu ülkelerin yerel hukuklarını, tabi olduğu uluslararası yükümlülüklerini ve sahip olduğu bağımsız denetim mekanizmalarını inceleyerek karar verir.
 - Komisyon, ilgili 3. ülke veya uluslararası kuruluşun yeterli düzeyde bir koruma sağladığına kanaat getirirse, bağlayıcı olan “uygunluk kararı” verebilir.
 - Komisyon, haklarında uygunluk kararı verilmiş 3. ülkeler ve uluslararası kuruluşlarda meydana gelen gelişmeleri *sürekli* olarak izler.
 - Verilen uygunluk kararları *en az dört yılda bir* tüm gelişmeler dikkate alınarak gözden geçirilmelidir.
 - Elde edilen bilgiler ışığında, uygunluk kararının geri alınması, değiştirilmesi veya askıya alınması her zaman mümkündür.

Sınıraşan Veri Transferleri-IV

- ❑ Avrupa Birliği Komisyonunun Uygunluk Kararı Bulunmayan Hallerde Aktarım (m. 46)
 - Avrupa Birliği Komisyonu tarafından alınan bir karar olmaması halinde, ancak bir veri sahibi veya işleyenin uygun güvenceler sağlamış olması halinde ve uygulanabilir veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olması koşuluyla, söz konusu veri sahibi veya işleyen bir 3. ülke veya uluslararası bir kuruluşa kişisel veri aktarabilir.

Sınırışan Veri Transferleri-V

- Uygun güvenceler aşğıdaki yöntemlerle sağlanabilir:
 - (a) Kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge,
 - (b) Bağlayıcı kurumsal kurallar,
 - (c) Komisyon tarafından kabul edilen standart veri koruma şartları,
 - (d) Bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma şartları,
 - (e) Onaylı davranış kuralları,
 - (f) Onaylı bir belgelendirme mekanizması,
 - (g) Yetkili denetim makamı tarafından onaylanmış, veri sahibi veya işleyen ile 3. ülke ya da uluslararası kuruluştaki kişisel veri sorumlusu, işleyeni ya da alıcısı arasındaki özelleştirilmiş sözleşme maddeleri ,
 - (h) Yetkili denetim makamı tarafından onaylanmış, kamu kuruluşları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri sahibi haklarını kapsayan hükümler.

Sınıraşan Veri Transferleri-VI

□ Spesifik Durumlara Yönelik Hukuka Uygunluk Nedenleri (m. 49)

- Bir uygunluk kararı veya uygun güvenceler olmaması durumunda dahi aşağıdaki durumlarda 3. bir ülkeye veya uluslararası bir kuruluşa kişisel veri aktarımı gerçekleştirilebilir :
- (a) Veri sahibinin, bir yeterlilik kararı ve uygun güvencelerin bulunmaması nedeniyle söz konusu aktarımların kendisine yönelik risklerin haberdar edilmesinin ardından, önerilen aktarıma açık bir şekilde rıza göstermesi,
- (b) Aktarımın veri sahibi ile veri sorumlusu arasındaki bir sözleşmenin yürütülmesi veya veri sahibinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması açısından gerekli olması,
- (c) Aktarımın veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında veri sahibi yararına yapılan bir sözleşmenin imzalanması veya yürütülmesi açısından gerekli olması,
- (d) Aktarımın kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması,
- (e) Aktarımın yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından gerekli olması,
- (f) Aktarımın veri sahibi veya diğer kişilerin hayati menfaatlerinin korunması açısından gerekli olması,
- (g) Aktarımın istişareye açık olan bir sicilden yapılması.
- Böyle veri aktarımları; istisnai nitelikte olmalı ve her bireye ilişkin durum için ayrı olarak değerlendirilmelidir, ayrıca bu yöntem yinelemeli olmamalı ve geniş kapsamlı aktarımlar için kullanılmamalıdır. (Madde 29 Çalışma Grubu)

Sınıraşan Veri Transferleri-VII

- ❑ Bir uygunluk kararına veya uygun güvencelerin varlığına ya da hukuka uygunluk nedenlerine dayanmayan sınıraşan veri aktarımları;
 - aktarımın yinelenmeli olmaması,
 - yalnızca sınırlı sayıda veri sahibini ilgilendirmesi,
 - veri sahibinin menfaatleri veya hakları ile özgürlüklerinin ağır basmadığı zorlayıcı meşru menfaatler doğrultusunda gerekli olması ve
 - veri sahibinin veri aktarımı ile ilgili tüm durumları değerlendirmiş, olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olmasıdurumunda gerçekleştirilebilir.

Sınırışan Veri Transferleri-VIII

□ Uluslararası Anlaşmalara Dayalı Aktarımlar (m. 48)

- Avrupa Birliği ve Üye Devletler, üçüncü ülkelerle, belirli amaçlarla kişisel verilerin üçüncü ülkelere aktarımını düzenleyen uluslararası anlaşmalar imzalayabilir.
- Bu anlaşmalar, ilgili bireyin kişisel verilerinin korunmasını sağlayacak uygun güvenceler içermelidir.
- Tüzük, bu uluslararası anlaşmalara hâlel getirmez.

Bağımsız Denetim-I

- Her Üye Devletin, gerçek kişilerin işleme faaliyeti ile ilgili temel hakları ve özgürlüklerini korumak ve Birlik içerisinde kişisel verilerin serbest akışını kolaylaştırmak üzere, bir ya da daha fazla sayıda bağımsız kamu kuruluşunun (denetim makamı) Tüzüğün uygulamasının izlenmesinden sorumlu olmasını sağlaması gerektiği öngörülmüştür. (m. 51)

Bağımsız Denetim-II

□ Denetim Makamı (m. 51-59)

- Denetim makamı, ulusal hukukta Tüzük ile uyumluluğu sağlayan esas organdır.
- Denetim makamlarının izlemenin ötesine geçen, *proaktif ve önleyici* denetleme faaliyetlerini de içeren geniş görev ve yetkileri vardır.
- Görevlerini ifa edebilmeleri için denetim makamlarının *soruşturmaya ve tavsiye vermeye ilişkin ve düzeltici yetkileri* olması gerekmektedir.
- Denetim makamının yetkileri;
 - Veri sorumluları ve veri sahiplerine verilerin korunmasına ilişkin her konuda tavsiye vermek,
 - Standart sözleşme maddeleri, bağlayıcı kurumsal kurallar veya idare düzenlemeleri onaylamak,
 - İşleme faaliyetlerini araştırmak ve buna bağlı olarak müdahale etmek,
 - Veri sorumlularının faaliyetlerinin denetimi için ilgili bazı bilgilerin arzını talep etmek,
 - Veri sorumlularını uyarmak veya kınamak ve kişisel veri ihlali bildirimlerinin veri sahiplerine gönderilmesine karar vermek,
 - Verinin düzeltilmesine, engellemesine, silinmesine veya yok edilmesine karar vermek,
 - İşleme faaliyetlerine geçici veya kati bir sınırlama getirmek,
 - Bir konuyu mahkemeye havale etmek.

Bağımsız Denetim-III

- Her denetim makamı, kendi bölgesinde yetkilerini kullanmayı yetkilidir.
- Bunun yanında Tüzük “tek durak noktası” mekanizması kurmakta ve farklı denetim makamları arasında iş birliği yapılmasını gerekli kılmaktadır.
 - Buna göre, sınır ötesi veri işleme faaliyetleri olan hallerde etkili iş birliğinin sağlanabilmesi için, Tüzük, bir baş denetim makamının, veri sorumlusunun ana veya tek işletmesinin denetim makamını olarak kurulmasını öngörmektedir.
- “Tek durak noktası” mekanizması uyarınca, bir Üye Devlette birden fazla denetim makamının kurulmuş ise, söz konusu Üye Devlet bu makamları Kurul’da temsil edecek denetim makamını tayin etmelidir.
- “Tek durak noktası” mekanizması uyarınca, bir veri sorumlusu veya işleyenin birden çok Üye Devlette işletmesi varsa veya tek işletmesi olmasına rağmen işleme faaliyetleri birden çok Üye Devletteki veri sahiplerini önemli ölçüde etkiliyorsa, ana (veya tek) işletmenin denetim makamı, veri sorumlusu veya işleyenin sınır ötesi faaliyetlerine ilişkin olarak baş makamdır.

Bağımsız Denetim-IV

□ İş Birliği (m. 60-61)

- Denetim makamları, Tüzüğün tutarlı bir şekilde yürütülmesi ve uygulanması amacıyla birbirlerine ilgili bilgileri ve karşılıklı desteği sağlamalıdır, ayrıca birbirleriyle etkili iş birliğine yönelik tedbirleri uygulamaya koymalıdır.
- Yüksek seviyede bir veri korumasının sağlanabilmesi için, baş denetim makamı yalnız hareket etmemeli, veri sorumluları veya işleyenler tarafından gerçekleştirilen kişisel veri işlemeye yönelik kararlar alınması için ilgili diğer denetim makamları ile iş birliği yapmalıdır.
- Her denetim makamı başka bir denetim makamının karşılıklı yardım talebine herhangi bir *gecikmeye mahal verilmeksizin* ve talebi aldıktan sonra *en geç, bir ay içersiinde* yanıt vermelidir.

Bağımsız Denetim-V

□ Avrupa Veri Koruma Kurulu (m. 68-70)

- Komisyon’a bireylerin kişisel verilerin işlenmesi ve gizliliğe ilişkin haklarını etkileyen AB faaliyetleri hakkında tavsiye vermesi, direktifin yeknesak uygulanmasını teşvik etmesi ve Komisyon’a veri koruması ile ilgili konularda uzman görüşü sağlaması amacıyla kurulmuştur.

Bağımsız Denetim-VI

□ Tutarlılık Mekanizması (m. 63)

- Tüzük, hükümlerinin bütün Üye Devletler’de yeknesak bir şekilde uygulanmasını sağlamak için bir tutarlılık mekanizması öngörmüştür.
- Buna göre, Tüzüğün AB içerisinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla, denetim makamları, Tüzükte belirtilmiş tutarlılık mekanizması vasıtasıyla, birbirleriyle ve uygun olduğu hallerde, Komisyon ile işbirliği yapmalıdır.

Bağımsız Denetim-VII

❑ İvedilik Prosedürü (m. 66)

- İstisnai durumlarda, ilgili bir denetim makamının veri sahiplerinin hakları ve özgürlüklerinin korunmasına yönelik olarak acil bir şekilde harekete geçmesine ihtiyaç varsa, söz konusu denetim makamı, tutarlılık mekanizmasından veya iş birliği prosedüründen ayrılarak, üç, ayı geçmeyecek belirli bir süre için geçerli olacak şekilde ve ilgili Devlet sınırları içinde hukuki sonuç doğurmak üzere ivedilikle geçici tedbirler alabilir.
- Geçici tedbiri alan denetim makamı, gecikmeksizin, söz konusu tedbirleri alma sebeplerini, ilgili diğer denetim makamlarına, Kurul'a ve Komisyon'a bildirmelidir.
- Geçici tedbiri alan denetim makamı gerekçelerini belirterek Kurul'dan acil bir görüş veya nihai bir karar vermesini talep edebilir.

Veri Sahiplerinin Hakları

- ▢ Bilgilendirilme Hakkı
- ▢ Erişim Hakkı
- ▢ Düzeltme Talep Hakkı
- ▢ Silinmeyi Talep Hakkı/Unutulma Hakkı
- ▢ İşlemenin Sınırlandırılması Hakkı
- ▢ Veri Taşınabilirliği Hakkı
- ▢ İşlemeye İtiraz Hakkı
- ▢ Yalnızca Otomatik İşleme Faaliyetine Dayalı Bir Karara Tabi Olmama Hakkı

Veri Sahiplerinin Haklarının Kısıtlanması (m. 23)-I

- Bir hakkın meşru olarak sınırlanmasından bahsedilebilmek için üç aşamalı bir test uygulanır. Buna göre, söz konusu müdahale;
 - (1) Hukuki düzenlemeler tarafından öngörülmüş olmalı ve müdahaleyi düzenleyen mevzuat keyfilikten korumayı sağlayacak nitelikte olup, sonuçları açısından öngörülebilir olmalıdır.
 - (2) Meşru bir amaç gütmelidir.
 - (3) Demokratik bir toplumda gerekli olmalıdır. Bunun sağlanması için bu müdahale;
 - (a) gerekli ve zararı önlemek açısından ölçülü olmalı ve
 - (b) hakkın özüne zarar vermemelidir.

Veri Sahiplerinin Haklarının Kısıtlanması (m. 23)-II

- Bu kapsamda meşru amaç aşağıdakilerden biri olabilir:
- (a) milli güvenlik,
 - (b) savunma,
 - (c) kamu güvenliği,
 - (d) suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi,
 - (e) Birlik ya da bir üye devletin genel kamu yararına yönelik diğer önemli hedefler,
 - (f) yargı bağımsızlığının ve adli süreçlerin korunması,
 - (g) düzenlenmiş, mesleklere ilişkin etik kurallarının ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması,
 - (h) nadiren olsa dahi, (a) ila (e) ve (g) bentlerinde belirtilen durumlarda resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi,
 - (i) veri sahibinin veya başkalarının haklarının ve özgürlüklerinin korunması,
 - (j) medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası.

Bilgilendirilme Hakkı-I (m. 12-14)

- Veri sahiplerinin, hangi verilerinin nasıl toplandığını, kullanıldığını veya işlendiğini, veri işleme faaliyetlerinin barındırdığı riskleri, bu risklere karşı düzenlenen güvenceleri, işlemeye ilişkin haklarını bilme hakları mevcuttur.
- Veri sorumlularının, planlanan bir veri işlemesi için kişisel veri topladıkları zaman, veri sahiplerini bilgilendirme yükümlülüğü bulunmaktadır.
- Bu yükümlülüğün doğması için veri sahibinin veri sorumlusundan bilgilendirilme talep etmesi gerekli olmayıp, veri sorumlusunun işlemek üzere kişisel veri toplanması yeterlidir.
- Veri sorumlusu, işleme faaliyeti ile alakalı aşağıda detaylıca anlatılacak her türlü bilgiyi öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak veri sahibine sağlamalıdır.

Bilgilendirilme Hakkı-II (m. 12-14)

- Bu bilgiler, veri sahibine; *yazılı* olarak veya uygun olduğu hallerde, *elektronik yollar da dahil olmak üzere diğer yollarla*, ayrıca veri sahibi tarafından talep edilmesi durumunda, veri sahibinin kimliğinin diğer yollarla doğrulanması koşuluyla, *sözlü* olarak sağlanabilir. Bu bilgiler *standart simgelerle bir arada* sağlanabilir.
- Amacın sınırlandırılması ve şeffaflık ilkeleri uyarınca, veri sorumlusunun başta veri sahibine belirttiğinden farklı bir amaçla işleme yapmayı planlaması halinde, veri sorumlusu, veri sahibini, bu yeni amaç hakkında bilgilendirmelidir.
- Kişisel verilerin direkt sahibinden sağlandığı hallerde, veri sorumlusu bilgilendirmeyi verilerin toplanması sırasında gerçekleştirmelidir.
- Kişisel verilerin sahibinden alınmadığı durumlarda ise veri sorumlusu bilgilendirmeyi *makul bir süre içerisinde, ancak en geç bir ay içerisinde* yapmalıdır.

Bilgilendirilme Hakkı-III (m. 12-14)

- Bilgilendirme ücretsiz olarak sağlanmalıdır.
 - Bir veri sahibinin taleplerinin asılsız veya ölçüsüz olduğunun, özellikle taleplerin tekrarlanması nedeniyle, açıkça anlaşıldığı hallerde, veri sorumlusu makul bir ücret talep edebilir veya taleple ilgili işlem yapmayı reddedebilir.
- Bilgilendirme yükümlülüğü;
 - (i) Veri sahibinin halihazırda bu bilgilere sahip olduğu hallerde ve ölçüde,
 - (ii) Kişisel verilerin veri sahibinden alınmadığı hallerde; özellikle kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar için gerçekleştirilen işlemlerde,
 - (iii) İlgili bilgilerin sağlanmasının imkânsız olması veya ölçüsüz bir çaba gerektirmesi söz konusuysa, doğmayacaktır.

Erişim Hakkı (m. 15)

- ▢ Veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme ve eğer işleme faaliyeti varsa, ilgili kişisel verilere ve belirli bilgilere erişim hakkı vardır.
- ▢ Veri sahipleri kişisel verilere ilişkin olarak:
 - (i) işleme amaçları,
 - (ii) ilgili kişisel veri kategorileri,
 - (iii) kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri,
 - (iv) varsa, kişisel verilerin saklanması açısından öngörülen süre veya süre belirlenmemişse, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
 - (v) kişisel verilerin düzeltilmesini ve silinmesini talep etme ve veri işlemenin sınırlandırılması haklarının varlığı,
 - (vi) bir denetim makamına şikâyetle bulunma hakkı,
 - (vii) kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;
 - (viii) otomatik karar vermenin varlığı ve en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları hakkında bilgi talep etme ve bilgi alma hakkına sahiptir.
- ▢ Veri sorumlusu, işleme faaliyetinden geçen kişisel verilerin bir nüshasını veri sahibine sağlamalıdır.
- ▢ Veri sahibine sağlanan her bilgi, *anlaşılabilir* olmalıdır.

Düzeltilme Talep Hakkı (m. 16)

- ▢ Veri sahiplerinin kendileri ile ilgili doğru olmayan kişisel verilerin *gereksiz gecikmeye mahal verilmeksizin* düzeltilmesini veri sorumlusundan talep etme hakkı bulunmaktadır.
- ▢ Düzeltilmeyi talep etme hakkı verilerin hukuka uygun işlenmesine imkân sağladığından, veri sahipleri bu talepleri için herhangi bir neden belirtmek yükümlülüğü altında değildir.
 - ▢ Fakat, verilerin yanlışlığını veya eksikliğini gösterme noktasında ispat yükü veri sahibindedir.
- ▢ Düzeltilme hakkı yalnızca “veri sahiplerine”, “kendi kişisel verileri” ile ilgili tanınmıştır.
 - ▢ Bir kişi, 3. bir kişinin kişisel verilerinin düzeltilmesi talebinde bulunamaz

Silinmeyi Talep Hakkı ve Unutulma Hakkı-I (m. 17)

- ▢ Tüzükten önceki düzenlemelerde açık ve münhasır bir hak olarak yer almamaktaydı.
- **ABAD, Google Spain.**
- ▢ Bu hak uyarınca, aşağıdaki hallerden birinin geçerli olması durumunda, veri sahibinin kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü bulunur:
 - (a) kişisel verilerin toplanma veya işleme amaçlarıyla ilişkili olarak artık gerekli olmaması,
 - (b) veri sahibinin işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması,
 - (c) veri sahibinin işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması,
 - (d) kişisel verilerin yasa dışı biçimde işlenmiş olması,
 - (e) veri sorumlusunun tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması,
 - (f) kişisel verilerin toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması.
- ▢ Veri işlemenin hukuka uygun olduğunu ispat yükü, işleme faaliyetlerinin hukuka uygun olmasından sorumlu veri sorumlusundadır.

Silinmeyi Talep Hakkı ve Unutulma Hakkı-II (m. 17)

- ▢ Veri işleme faaliyetinin;
 - (i) ifade ve bilgi edinme hakkının kullanılması,
 - (ii) veri sorumlusunun tabi olduğu Birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk açısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması açısından,
 - (iii) halk sağlığı alanındaki kamu yararı sebeplerinden dolayı,
 - (iv) silinme hakkının ilgili işleme hedeflerinin yakalanmasını imkansız hale getirmesi veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistikî amaçlar doğrultusunda veya
 - (v) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından gerekli olması halinde silinme talep edilemeyecektir.

Silinmeyi Talep Hakkı ve Unutulma Hakkı-III

Tartışma:

Unutulma Hakkı = Silinme Hakkı?

İşlemenin Sınırlandırılması Hakkı (m. 18)

- ▢ Belirli hallerde, veri sahiplerinin, veri sorumlularının işletme faaliyetlerini geçici olarak kısıtlama hakları mevcuttur.
- ▢ Sınırlamanın talep edilebileceği durumlar aşağıdaki gibidir:
 - (a) kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi halinde, veri sahibinin kişisel verilerin doğruluğunu teyit etmesini sağlayan bir süre boyunca,
 - (b) işleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi,
 - (c) veri sahibinin işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması amacıyla söz konusu verilere ihtiyaç duyması,
 - (d) veri sorumlularının meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar, veri sahibinin işleme faaliyetine itiraz etmesi.

Veri Taşınabilirliği Hakkı (m. 20)

- Veri taşınabilirliği hakkı, Tüzük ile birlikte veri sahiplerine tanınan, daha önce hiçbir belgede düzenlenmemiş bir haktır.
- İşleme faaliyetinin *rızaya veya bir sözleşmeye dayanması* veya işleme faaliyetinin *otomatik yollarla gerçekleştirilmesi* halinde, veri sahibinin kendisi ile ilgili olarak bir veri sorumlusuna sağlamış, olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı vardır.
- Veri sahibinin, teknik açıdan uygulanabilir olması şartıyla, kişisel verilerini doğrudan bir veri sorumlusundan diğerine ilettirme hakkı vardır.
- Veri sahibinin veri taşıma talebi üzerine, veri sorumlusu, veri sahibinin talimatları ile hareket etmelidir.
- Veri taşınabilirliği hakkının kullanılması diğer herhangi bir hakkı olumsuz yönde etkilememelidir.

İşlemeye İtiraz Hakkı (m. 21)

- ▢ Veri sahibinin, *kendi özel durumu ile ilgili gerekçelere dayalı olarak veya kişisel verilerinin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda*, söz konusu kişisel verinin işlenmesine itiraz hakkı bulunmaktadır.
- ▢ Bu bağlamda ABAD, veri sahibinin haklarının, kural olarak, veri sorumlusunun ekonomik menfaatlerine üstün geldiğini belirtmiştir.
- ▢ Veri işlemeye devam edilmesini gerektiren hususların varlığına ilişkin ispat yükünün veri sorumlusundadır.
- ▢ Kişi kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz edebilir.

Yalnızca Otomatik İşleme Faaliyetine Dayalı Bir Karara Tabi Olmama Hakkı

(m. 22)

- Veri sahibinin *kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen*, profil çıkarma da dahil olmak üzere, yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı mevcuttur.
- Ancak;
 - (i) işleme veri sahibi ve bir veri sorumlusu arasında bir sözleşme yapılması veya uygulanması için gerekli ise veya,
 - (ii) veri sorumlusunun tabi olduğu ve veri sahibinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği Birlik veya üye devlet hukuku çerçevesinde işlemeye izin verilmiş ise veya,
 - (iii) işlemeye veri sahibinin açık rızası mevcut ise,yalnızca otomatik işlemeye dayalı karar hukuka aykırılık oluşturmaz.
- Veri sorumlusu, veri sahibinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacı ile uygun tedbirler uygulamalıdır.

Kanun Yolları, Sorumluluk, Cezalar ve Tazminat-I

□ Denetim Makamına Şikâyetle Bulunma Hakkı (m. 77)

- Her veri sahibi, kendisi ile alakalı kişisel verilerin işlenmesinin hukuka aykırı olarak gerçekleştiğini düşünmesi durumunda, başka bir idari veya adli çözüm yoluna hâlel gelmeksizin, yetkili denetim makamına şikâyetle bulunma hakkına sahiptir.
- Şikâyet sahibi soruşturmanın ilerlemesi ve sonucu konusunda makul bir süre içerisinde bilgilendirilmelidir.
- Denetim makamı şikâyetle ilişkin bir karar verdiğinde, her gerçek veya tüzel kişinin bu denetim makamının kendileriyle ilgili yasal *bağlayıcılığı* olan kararlarına karşı etkili bir kanun yoluna başvurma hakkı vardır.

Kanun Yolları, Sorumluluk, Cezalar ve Tazminat-II

□ Etkili Bir Kanun Yoluna Başvurma Hakkı (m. 78-79)

- Kişisel verilerinin Tüzüğe aykırı bir şekilde işlenmesi sonucu bu Tüzük kapsamındaki haklarının ihlal edildiğini değerlendirdiği hallerde, her veri sahibi etkili bir kanun yoluna başvurma hakkına sahiptir.
- Denetim makamlarının bağlayıcı kararlarına karşı ilgili kişilerin kanun yoluna başvurma hakkı mevcuttur.
- Ayrıca, (i) bir veri sahibi, veri sorumlusu, veri işleyen veya denetim makamının direkt ve bireysel olarak kendilerini ilgilendiren Avrupa Veri Koruma Kurulunun bir kararını iptal etmek amacıyla veya (ii) bir veri sahibinin herhangi bir AB kuruluş ve organın veri koruma hukukunu ihlal ettiği iddiasına dayanarak ABAD'a başvurma hakkı vardır.

Kanun Yolları, Sorumluluk, Cezalar ve Tazminat-III

❑ Kar Amacı Gütmeyen Bir Organ, Kuruluş veya Birlik Tarafından Temsil Edilme Hakkı (m. 80)

- Veri sahiplerinin,
 - bir Üye Devlet hukuku uyarınca düzgün şekilde kurulmuş,
 - kamu yararına yasal hedefleri bulunan ve veri sahiplerinin kişisel verilerinin korunmasına ilişkin hakları ve özgürlüklerinin korunması alanında aktif olan
 - kar amacı gütmeyen bir organ, kuruluş veya birliğe,
 - şikâyeti onun adına yapması,
 - ilgili hakları onun adına kullanması ve
 - Üye Devlet hukukunda sağlanması koşuluyla, onun adına tazminat alma hakkını kullanma yetkisi verme

hakkı mevcuttur.

Kanun Yolları, Sorumluluk, Cezalar ve Tazminat-IV

❑ Sorumluluk ve Tazminat (m. 82)

- ❑ Etkili bir kanun yoluna başvurma hakkı, kişisel verileri hukuka aykırı olarak işlenen bireylerin böyle bir işleme sonucunda uğradıkları zararlar için tazminat talep edebilme hakkını içinde barındırır.
- ❑ Tüzüğe ilişkin bir ihlal sonucu *maddi veya manevi* zarar gören herhangi bir kişinin, yaşanan zarara ilişkin olarak veri sorumlusu veya işleyenden tazminat alma hakkı bulunmaktadır.
- ❑ Bu kapsamda;
 - ❑ işleme faaliyetine müdahil herhangi bir veri sorumlusu Tüzüğü ihlal eden işleme faaliyetinin sebep olduğu zarardan sorumludur.
 - ❑ bir veri işleyen ise ancak Tüzüğün özellikle veri işleyenlerine yönelik yükümlülüklerine uyum göstermediği veya veri sorumlusunun hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde, işleme faaliyetinin sebep olduğu zarardan sorumludur.
- ❑ Birden fazla veri sorumlusu veya işleyenin ya da hem bir veri sorumlusu hem de bir veri işleyenin aynı işleme faaliyetinde bulunduğu ve işleme faaliyetinin sebep olduğu herhangi bir zarardan sorumlu olduğu hallerde, her veri sorumlusu veya işleyenin tüm zarardan sorumlu tutulacaktır.
- ❑ Zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığını kanıtlaması halinde, bir veri sorumlusu veya işleyenin bu sorumluluktan muaf tutulabilecektir.

Kanun Yolları, Sorumluluk, Cezalar ve Tazminat-V

❑ Cezalar (m. 83)

- Veri işlemenin temel ilkeleri ve rızanın koşullarına aykırılık, veri sahiplerinin haklarının ihlali ve Tüzüğün yurt dışına veri aktarımına ilişkin kurallarına uyulmaması durumunda, denetim makamlarının 20.000.000 Euro'ya kadar veya veri sorumlusu veya işleyenin bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezası (hangi meblağ yüksek ise o geçerli olmak üzere) kesme yetkisi vardır.
- Diğer ihlaller ile ilgili olarak ise denetim makamının 10.000.000 Euro'ya kadar veya veri sorumlusu veya işleyenin bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezası (hangi meblağ yüksek ise o geçerlidir) kesme yetkisi vardır.
- Üye Devletler, Tüzüğün ve Tüzük gereğince kabul edilen yerel düzenlemelerin ihlal edildiği durumlar için ceza verilmesine ilişkin kurallar düzenleyebilir.
 - Örneğin; Almanya'nın Federal Veri Koruma Yasasında (Bundesdatenschutzgesetz), çok sayıda veri sahibinin kamuya açık olmayan kişisel verilerinin hukuka aykırı olarak aktarılması durumunda para veya üç yıla kadar hapis cezası öngörülmüştür.
- Denetim makamlarının idari para cezası kesme yetkileri dışında, çeşitli “*düzeltici*” yetkileri mevcuttur.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Uygulanması

- Tüzüğün getirdiği düzenlemelerin uygulamaya konması için dört aşamalı bir yaklaşım izlenmelidir:
 - (1) boşluk analizi,
 - (2) risk analizi,
 - (3) proje idaresi ve kaynak/bütçe planlaması, ve
 - (4) uygulamaya koyma.

Teşekkürler...

Ayrıntılı bilgi ve konu ile ilgili makaleler için:
<http://independent.academia.edu/DoçDrMuratVolkanDülger>