# General Data Protection Regulation (GDPR) ve Uygulanması

9 Mayıs, 2018

Leyla Keser

BİLGİ Bilişim ve Teknoloji Hukuku Enstitüsü

# GDPR Nedir ?

BİLGİ Bilişim ve Teknoloji Hukuku Enstitüsü

**Mayıs 2016'da kabul edilen ve 25 Mayıs 2018'de yürürlüğe girecek olan Avrupa Birliği'nin veri koruma düzenlemesidir.**

***«Gerçek kişilerin kişisel verilerinin korunması ve bu verilerin serbest dolaşımına ilişkin bir düzenleme»***

**GDPR bir regülasyon olduğu için yürürlüğe girmesiyle birlikte uygulanabilir olacaktır.**

GDPR'ın yürürlüğe girmesiyle birlikte AB'nin mevcut veri koruma direktifi (Directive 95/46/EC) yürürlükten kalkacaktır.

**GDPR'ın Bazı Temel Farklılıkları**

- ***Uygulanabilirlik kapsamı genişletildi.***
- ***Veri işlenmesi için alınacak rızanın şartları ağırlaştırıldı.***
- ***Veri işlenmesi sırasında göz önünde tutulacak «hesap verilebilirlik» ve «privacy by design» gibi yeni ilkeler getirildi.***
- ***Veri taşınabilirliği imkanı getirildi.***
- ***Veri sahiplerine yeni haklar tanındı.***
- ***Veri korumasına ilişkin cezalar ağırlaştırıldı.***

# GDPR’ın Getirdiği Yenilikler



## Genişletilmiş Etki Alanı

AB’de yerleşik olmayıp AB’de yaşayan kişilere mal ve hizmet sunan kuruluşlar da GDPR kapsamındadır.

## Şeffaflık Prensibi

Kişisel verilerin işlenmesine ilişkin her türlü bilgi ve ileti kolayca ulaşılabilir olmalı ve içeriğinde sade, açık ve anlaşılabilir bir dil kullanılmalı.

## Onay / Açık Rıza

Onay, açık ve onaylayıcı eylem ile verilmiş beyandır. Onay talebinin veri işleme sebebini içermesi, verilecek onayın ise işleme faaliyetleri özelinde olması gerekmektedir. Ayrıca, veri sorumluları onay alınmadan evvel, veri sahibi kişilere onayın geri alınması hakkını bildirmek zorundadır.

## Unutulma Hakkı

Veri sahipleri, veri sahibinin rızasının olmadığı, verilerin toplanma amacı ile ilgili olarak tutulmasının gerekliliğinin ortadan kalktığı veya verilerin GDPR’a aykırı olarak işlendiği hallerde verilerin silinmesini veya artık işlenmemesini talep etme hakkına sahiptir.

## Kişisel Verilerin Yurt Dışına Aktarılması

Kişisel verilerin yurtdışına aktarılması için verinin aktarılacağı ülkede, bölgede ya da ilgili ülkenin belirli bir sektöründe yeterli derecede koruma sağlanması şarttır.

# GDPR’ın Getirdiği Yenilikler



## Privacy by Design

Her türlü yeni ürün ve servisin tasarlanması aşamasında veri koruması hukuku hükümleri ile uyumluluğun gözetilmesi ve veri koruması açısından riskli sayılabilecek hallerde Veri Koruması Etki Analizi (*data protection impact assessment*) yapma zorunluluğu getirilmiştir.

## Hesap Verilebilirlik Prensibi

Veri sorumluları, hesap verilebilirlik prensibi uyarınca gerektiğinde veri işleme ilkelerine uygun hareket ettiğini gösterebilmelidir.

## Veri Koruma Sorumlusu Atanması

Veri sahiplerinin kapsamlı olarak izlenmesini gerektiren veri işleme faaliyetlerinin varlığı veya veri sorumlusu veya veri işleyenin esas faaliyetlerinin kapsamlı olarak özel nitelikli kişisel verilerin işlenmesinden oluşması durumunda, veri koruma sorumlusu atanmalıdır.

## One-Stop Shop Mekanizması

AB içerisinde farklı üye devletlerde kurulu ve faaliyet gösteren şirketlerin tüm düzenleme ve yükümlülüklere istinaden tek bir veri koruma otoritesine tabi olması düzenlemesi getirilmektedir.

## Ağırlaştırılmış Yaptırımlar

Maddi ve manevi tazminatla beraber, 20.000.000 Euro’ya kadar para cezası veya teşebbüsün bir önceki mali yılına ait dünya genelindeki cirosunun %4’üne kadar para cezası öngörülmüştür.

## Risk Temelli Yaklaşım

GDPR’ın getirmiş olduğu sorumluluk rejimi risk temelli bir yaklaşım benimsemektedir. Veri sorumlularının yükümlülükleri, veri işleme faaliyetinin doğurduğu risk ile doğru orantılıdır.

# GDPR’ın Getirdiği Yenilikler



## Veri Sorumlularının Yükümlülükleri

- Veri Koruması Etki Analizi düzenlemek
- Veri koruma politikaları oluşturmak ve uygulamak
- Mevcut ve yeni veri işleme faaliyetlerinin privacy by design ilkesine uyumlu olarak gerçekleştirilmesini sağlamak
- Veri işleme faaliyetlerine ilişkin talep, şikayet ve ihtilafları yürütmek
- Veri işleme ihlallerine karşın gerekli önlemleri almak
- Veri işleme sürecine dahil olan kişileri yönetmek
- Veri Koruması regülasyonlarını takip ederek uygun organizasyonel değişiklikleri gerçekleştirmek

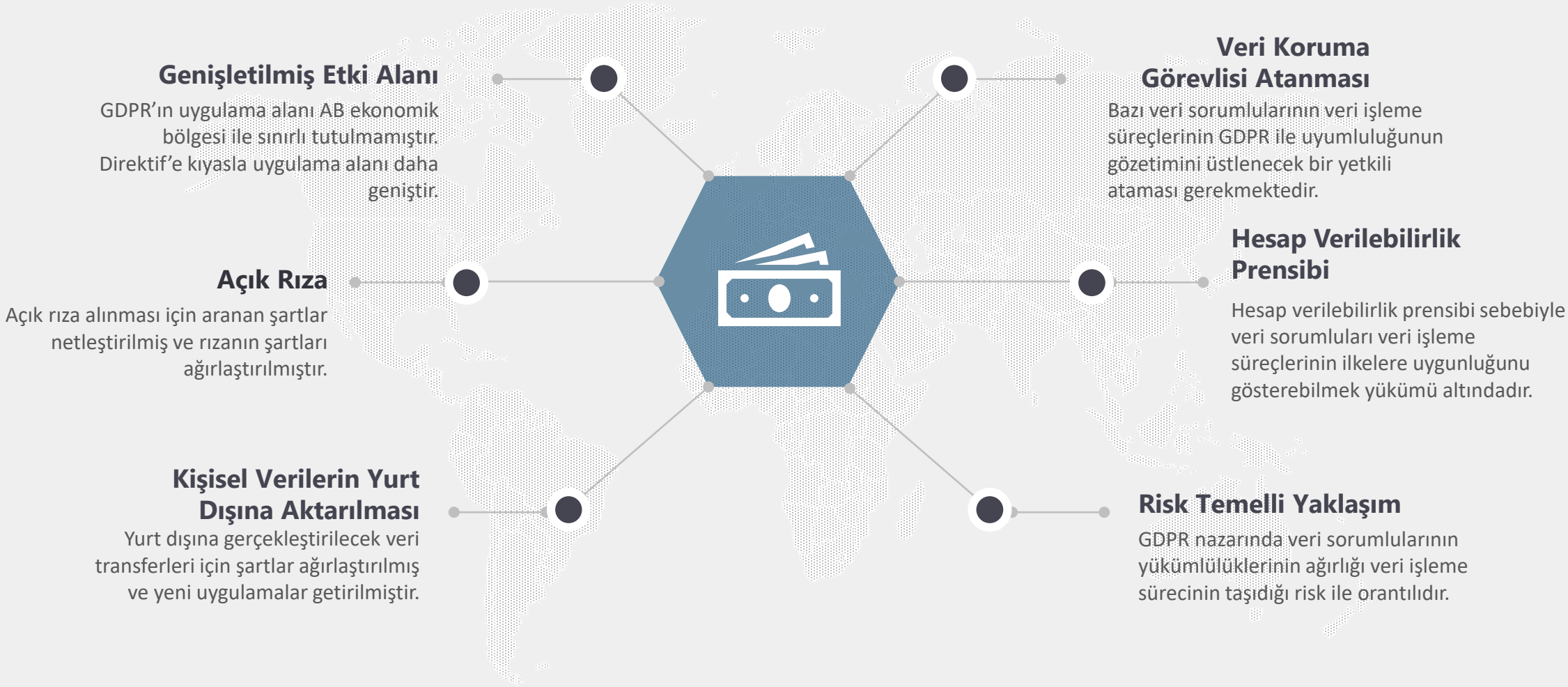
## Veri İşleyenlerin Yükümlülükleri

- AB’de yerleşik olmayan veri sorumluları için, kendilerini temsil edecek AB’de yerleşik bir temsilci atamak
- Kişisel verilerin işlenmesinde bir ihlal tespit etmeleri halinde, gecikmeksizin söz konusu ihlali veri sorumlusuna bildirmek
- Gerektiği takdirde veri koruma sorumlusu atamak
- Veri sorumluları adına ve talimatları doğrultusunda gerçekleştirilen veri işleme faaliyetlerine dair yazılı kayıt tutmak

# GDPR - Önemli Hususlar



Uyum – Regülasyon – Güvenlik - Talepler



### Genişletilmiş Etki Alanı

GDPR'ın uygulama alanı AB ekonomik bölgesi ile sınırlı tutulmamıştır. Direktif'e kıyasla uygulama alanı daha geniştir.

### Açık Rıza

Açık rıza alınması için aranan şartlar netleştirilmiş ve rızanın şartları ağırlaştırılmıştır.

### Kişisel Verilerin Yurt Dışına Aktarılması

Yurt dışına gerçekleştirilecek veri transferleri için şartlar ağırlaştırılmış ve yeni uygulamalar getirilmiştir.

### Veri Koruma Görevlisi Atanması

Bazı veri sorumlularının veri işleme süreçlerinin GDPR ile uyumluluğunun gözetimini üstlenecek bir yetkili ataması gerekmektedir.

### Hesap Verilebilirlik Prensibi

Hesap verilebilirlik prensibi sebebiyle veri sorumluları veri işleme süreçlerinin ilkelere uygunluğunu gösterebilmek yükümü altındadır.

### Risk Temelli Yaklaşım

GDPR nazarında veri sorumlularının yükümlülüklerinin ağırlığı veri işleme sürecinin taşıdığı risk ile orantılıdır.

# GDPR'ın Getirdiği Yenilikler



## Genişletilmiş Etki Alanı

AB'de yerleşik olmayıp AB'de yaşayan kişilere mal ve hizmet sunan kuruluşlar da GDPR kapsamındadır.

GDPR, AB içerisinde faaliyet gösteren veri işleyen kuruluşların faaliyetleri kapsamında gerçekleştirdikleri veri işleme faaliyetlerini, bu kuruluşların AB'de yerleşik olup olmadıklarına veya veri işlemenin AB içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, kapsamaktadır.

AB'de yaşayan kişilere mal ve hizmet sunmak, yalnızca bir internet sitesi veya e-posta adresine erişimi ifade etmez, aynı zamanda birden çok AB ülkesinde faaliyette olunduğunu gösteren, dil, para birimi, ödeme cinsi seçiminin bulunmasını veya kişilerin tüketim tercih ve alışkanlıklarının tespiti amacıyla internetteki faaliyetlerinin gözlemlenmesi anlamında gelen müşterilerin izlenmesini de ifade eder. Dolayısıyla AB dışında faaliyet göstermesine karşın AB tüketicisini hedefleyen şirketler de GDPR'a tabidir.

AB vatandaşlarına yönelik Bankacılık faaliyetleri gerçekleştiren Türkiye merkezli bankaların da GDPR'a uyum sağlamaları gerekecektir.

# GDPR'ın Getirdiği Yenilikler



## Şeffaflık Prensibi

Kişisel verilerin işlenmesine ilişkin her türlü bilgi ve ileti kolayca ulaşılabilir olmalı ve içeriğinde sade, açık ve anlaşılabilir bir dil kullanılmalı.

Veri sorumluları, veri işleme faaliyetlerine ilişkin verdiği bilgilerde olabildiğince anlaşılabilir olmalıdır. Özellikle veri sorumlusunun kimliği, hangi verilerin işleneceği, nasıl bir işleme faaliyeti yürütüleceği ve veri işlemenin sonucunda doğacak etkiler açıkça ortaya koyulmalıdır.

Şeffaflık prensibi, işleme hakkında bilgi verilirken olabildiğince hukuki ve teknik terimlerden kaçınmayı gerektirir. Özellikle aydınlatma metinleri okunması ve anlaşılması zor olmamalıdır.

Bankalar özellikle müşterilerini veri işleme faaliyetleri hakkında bilgilendirirken olabildiğince anlaşılabilir olmaya çalışmalıdır.

*Örneğin uzun aydınlatma metinleri yerine karikatürler, videolar veya interaktif internet sayfaları kullanarak hem müşteriler özelinde itibarınızı artırabilir hem de GDPR'a tam uyum sağlayabilirsiniz.*

## Açık Rıza

Açık rıza, açık ve onaylayıcı eylem ile verilmiş beyandır. Bu beyanın veri işleme faaliyetleri özelinde olması gerekmektedir.

Veri sahiplerinin açık rızalarını diledikleri zaman geri alabilecekleri, rızanın alınmasından önce kendilerine bildirilmelidir. Açık rızaya konu olan veri işleme faaliyetleri şeffaf bir şekilde ve anlaşılabilir bir dil ile veri sahiplerine açıklanmalıdır.

Rızanın alındığına ilişkin kanıt yükümlülüğü veri sorumlusunda olacağından rızaya ilişkin bilgi ve belgelerin saklanması gerekmektedir.

GDPR, çocukların verilerinin işlenmesinde ebeveynlerinin onayının alınmasını zorunlu kılmıştır. Operasyonların bu mekanizmayı devreye sokacak şekilde değiştirilmesi gerekmektedir.

# GDPR’ın Getirdiği Yenilikler



## Kişisel Verilerin Yurt Dışına Aktarılması

Kişisel verilerin yurtdışına aktarılması için verinin aktarılacağı ülkede yeterli derecede koruma sağlandığına ilişkin teminat verilmesi şarttır.
Bu değerlendirme, veri koruması otoritesi tarafından yapılmaktadır.

GDPR’a uygun veri transferi gerçekleştirilebilmesi için verinin aktarılacağı ülkede, bölgede veya ilgili ülkedeki belirli sektörde «yeterli seviyede koruma» bulunması gerekir. «Yeterli seviyede koruma» bulunduğuna dair değerlendirme Komisyon tarafından gerçekleştirilecektir.

İlgili ülkenin bağımsız otoritelerinin çalışmaları, ülkedeki temel hak ve özgürlüklere ait koruma, veri koruma mevzuatı gibi kriterler «yeterli seviyede koruma» değerlendirmesinde göz önüne alınmaktadır.

Yapılan değerlendirme en az her dört senede bir tekrardan gözden geçirilecektir.

Eğer ilgili üçüncü ülkede «yeterli seviyede koruma» sağlandığı Komisyon tarafından onaylanmadıysa bu sefer veri sorumluları transferi «uygun güvenlik önlemlerine» dayandırabilecektir. Bunlarla sınırlı olmamakla beraber, «uygun güvenlik önlemlerinin» sağlandığına ilişkin bazı göstergeler şunlardır: (→) kamu kurumları ile veri sorumlusu arasında bağlayıcı bir belge (→) Bağlayıcı Şirket Kuralları (→) bağlayıcı hükümleri olan davranış kurallarının onaylanmış olması ya da (→) iki veri sorumlusu arasında verilerin korunmasına ilişkin sözleşmesel bir ilişki bulunması. Ancak bu son durumda yetkili veri koruma otoritesinden onay alınması gerekmektedir.

# GDPR’ın Getirdiği Yenilikler



## Privacy by Design ve Privacy by Default

Her türlü yeni ürün ve servisin tasarlanması aşamasında veri koruması hukuku hükümleri ile uyumluluğun gözetilmesi ve veri koruması açısından riskli sayılabilecek hallerde Veri Etki Analizi (privacy impact assessment) yapma zorunluluğu getirilmiştir.

«Privacy by Design» ilkesine göre, yeni uygulamaya geçirilecek sistemlerin dizayn sürecinden başlayarak veri koruma ilkelerine (şeffaflık, veri minimizasyonu, ölçülülük vb.) uygun şekilde tasarlanması gerekmektedir. İlgili ilkelere uygunluk sistemlere sonradan entegre edilmemelidir. Bankalar, yeni kurdukları sistemlerde bu ilkenin gözetilmesine dikkat etmelidir.

Örneğin, Bankalar yeni işleme koydukları telefon uygulamalarının (*Application*) tasarımı sırasında uygulama vasıtasıyla işlenecek kişisel verilerin korunması için her türlü önlemi almak durumundadır. Örneğin, tasarım sürecinde uygulamanın işlevselliği için telefon üzerinde hangi datalara ulaşılmasının zorunlu, hangilerinin zorunlu olmadığı belirlenmeli ve veri minimizasyonu ilkesiyle hareket edilmelidir.

Ayrıca, gizliliğe yönelik riskler gerçekleştikten sonra bunlara çare bulmak değil önceden önlem almak gerekir. (p*roactive, not reactive*)

Uygulamadaki kullanıcılarının gizliliğinin korunması için her türlü seçenek varsayılan olarak aktif olarak gelmelidir *(«Privacy by Default»).*

# GDPR’ın Getirdiği Yenilikler



## Hesap Verilebilirlik Prensibi

Veri sorumluları, hesap verilebilirlik prensibi uyarınca gerektiğinde veri işleme ilkelerine uygun hareket ettiğini gösterebilmelidir.

«Hesap verilebilirlik» prensibine göre veri sorumluları, veri işleme ilkelerine uygun veri işlediğini gösterebilmelidir. Hesap verilebilirliğe ilişkin ispat yükümlülüğünün veri sorumlusunda olduğu GDPR’da açıkça belirtilmiştir. Bankalar, *gerçekleştirdikleri her türlü veri işleme faaliyetinde ilkelere uyanın yanında, ilkelere uygun hareket ettiğini kanıtlayabilmek adına* gerekli önlemleri almak durumundadır.

Uygulamada bankalar, veri işleme ilkelerine uyum sağladığını kanıtlayacak içsel mekanizmalar ve kontrol sistemleri kurmalıdır. Örneğin, bağımsız denetçilerden dış kaynak denetim hizmeti alınması ve bunlara ait raporların saklanması ve istendiğinde veri koruma otoritelerine bunların sunulması hesap verilebilirlik prensibine uyum sağlandığını gösterecektir.

# GDPR'ın Getirdiği Yenilikler



«Hesap Verilebilirlik» Prensibi

- Neden gereklidir?
- Nedir?
- Örnekler
- Nasıl yerine getirilir?
- Tasarımla ve Varsayılan Olarak Veri Koruması Prensibi

# GDPR'ın Getirdiği Yenilikler



## «Hesap Verilebilirlik» Prensibi Neden Gereklidir?

- Kişisel verilerin korunması prensipleri ve kuralları sıklıkla gerektiği gibi günlük uygulamaya yansıtılamamaktadır.
- «Kişisel verilerin korunması» kurumların organizasyon yapısının ve kurumsal kültürünün bir parçası olmadıkça kanunlara ve kurallara gereken uyum sağlanamayacaktır.
- **Kısacası; «kişisel verilerin korunması» teoriden uygulamaya geçirilmelidir.**
- ***GDPR Art. 5(2)*** *«The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')»*.

# GDPR'ın Getirdiği Yenilikler



## «Hesap Verilebilirlik» Prensibi Neden Gereklidir?

**6698 Sayılı Kişisel Verilerin Korunması Kanunu**

**Genel İlkeler**

**MADDE 4-** (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

**General Data Protection Regulation («GDPR»)**

**Article – 5 : Principles relating to processing of personal data**

1) Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation')**;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation**');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation');**

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability').**

# GDPR'ın Getirdiği Yenilikler



## «Hesap Verilebilirlik» Prensibi Nedir?

- Kanuni bir hesap verilebilirlik prensibi iki unsura sahip olmalıdır:

I. **İlkelere uyum yükümlülüğü →** Veri sorumluları, kişisel verilerin korunması prensiplerinin ve yükümlülüklerinin yerine getirilmesi için gerekli tüm önlemleri almalıdır.

II. **Gerektiğinde hesap verebilme →** Veri sorumlusu bu yükümlülüğü yerine getirdiğini, talep edilmesi durumunda düzenleyici otoriteye ispatlayabilmeli/gösterebilmelidir.

- ***GDPR Art. 5(2)*** *«The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')»*.

**«Hesap Verilebilirlik» Prensibi Ne Değildir?**

Yeni bir kişisel veri koruma prensibi getirmemekte veya mevcut ilkeleri değiştirmemektedir. Yalnızca mevcut ilkelerin daha efektif şekilde uygulamaya yansımasını amaçlar.

# GDPR'ın Getirdiği Yenilikler



## «Hesap Verilebilirlik» Prensibi Örnekler

**6698 Sayılı Kişisel Verilerin Korunması Kanunu**

**Veri güvenliğine ilişkin yükümlülükler**
**MADDE 12-** (1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak,

amacıyla **uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.**
(…)
(3) Veri sorumlusu, kendi kurum veya kuruluşunda, **bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.**

**General Data Protection Regulation («GDPR»)**

**Section 1**
**General obligations**
*Article 24*
**Responsibility of the controller**
1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the **controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.** Those measures shall be reviewed and updated where necessary.

# GDPR'ın Getirdiği Yenilikler



## «Hesap Verilebilirlik» Prensibi Nasıl Yerine Getirilir?

**«... kişisel verilerin korunması prensiplerinin ve yükümlülüklerinin yerine getirilmesi için gerekli tüm önlemleri...»**

**«tüm önlemler» → ?**

**Açıklık yok, dolayısıyla iki soru sorulabilir:**
**Sektörel ve veri işleme faaliyetlerin durumuna göre hangi önlemler alınabilir?**

**Veri sorumlusunun alabileceği özel önlemler nasıl belirlenmelidir?**

**Sektörel ve veri işleme faaliyetlerin durumuna göre hangi önlemler alınabilir?**

- WP29, Sektör birlikleri, Kişisel Verileri Koruma Kurumu gibi otoritelerin yol göstericiliğinde belirlenecektir.
- Aşağıdaki örnek önlemlerin alınması hesap verilebilirlik prensibinin yerine getirildiğinin göstergesi olarak kabul edilebilir:
  - Kişisel veri işleme envanteri hazırlanması.
  - Kurumsal veri gizliliği politikaları hazırlanması.
  - Bazı veri işleme süreçleri için «veri koruması etki değerlendirmesi» yapılması. (GDPR Art. 35)
  - Veri güvenliği için organizasyon içi prosedürlerin hazırlanması.
  - Şirket içinde «veri koruması görevlisi» atanması. (GDPR Art.37)
  - Kişisel veri işleme süreçlerinin düzayn edilme aşamasında (Privacy by Design) ve her türlü işleme sürecinde (privacy by default) hesap verilebilirlik ı prensibinin en sıkı haliyle işletilmesi (GDPR Art.25)

Veri sorumlusunun alabileceği özel önlemler nasıl belirlenmelidir? Alınacak önlemlerin veri işleme sürecinin niteliklerine göre ölçeklendirilmesi önemlidir. Ssağlık verisi işleyen bir hastane ile müşterilerin alışveriş geçmişlerini işleyen bir perakende mağazanın alacağı veri koruma önlemleri aynı olmayacaktır.

Önlem ölçeklendirmesinde kullanılabilecek kriterler [«Risk Temelli Yaklaşım»];
Veri işleme faaliyetinin doğurduğu riskler,
İşlenen verinin niteliği,
Veri işleme faaliyetinin ölçeği,
Veri işleme faaliyetinin amacı,
Veri sorumlusunun kimliği,
...

# GDPR'ın Getirdiği Yenilikler



## «Hesap Verilebilirlik» Prensibi Data Protection by Design – By Default Yaklaşımı Bakımından İncelenmesi

Data protection by design and by default: veri işleme süreçlerinin tasarımından ve en başından itibaren veri koruması prensiplerinin göz önünde tutulması anlamına gelir.

Bu prensibin yerine getirilmesi için alınabilecek önlemler arasında:

- Veri minimizasyonu
- Pseudonymisation
- Şeffaflık
- Veri sahiplerinin veri işleme süreçlerini denetlemesine imkan tanımak,
- Düzenli olarak veri güvenliğine ilişkin önlemleri geliştirmek, uygulamak ve var olanları iyileştirmek.

## Veri Koruma Görevlisinin Atanması

Veri sahiplerinin kapsamlı olarak izlenmesini gerektiren veri işleme faaliyetlerinin varlığı veya veri sorumlusu veya veri işleyenin esas faaliyetlerinin kapsamlı olarak özel nitelikli kişisel verilerin işlenmesinden oluşması durumunda, veri koruma görevlisi atanmalıdır.

**Veri koruma görevlisi atanmasını zorunlu kılan haller**

- Veri işleme faaliyetinin bir kamu kurumu tarafından gerçekleştirilmesi
- Veri sorumlusunun veri sahiplerinin kapsamlı olarak izlenmesini gerektiren veri işleme faaliyetlerini gerçekleştirmesi
- Veri sorumlusunun veya veri işleyenin esas faaliyetlerinin kapsamlı olarak özel nitelikli kişisel veri işlenmesinden oluşması

- GDPR hükümleri uyarınca veri koruma görevlisi atanmasının gerekli olup olmadığı araştırılarak, GDPR'ın bu konudaki uygulamasının yakından takip edilmesi gerekmektedir.

# GDPR'ın Getirdiği Yenilikler



## Psödoanonimizasyon (*pseudonymisation*)

| | |
|---|---|
| John Doe ←→ no. 34562018 | Anonim olmayan data |
| **John Doe ←→ *ID18236* ←→ no. 34562018** | **Psödoanonim data** |
| XYZXYXYZ ← [X] → no. 34562018 | Anonim data |

GDPR ile getirilen veri güvenliği önlemlerinden biridir.

Anonimleştirilmiş veriden farklı olarak, verinin gerçek kişi ile bağlantısı tamamen koparılmamakta ancak bağın kurulması zorlaştırılmaktadır. Veri doğrudan kişiyi belirleyici değildir ancak başka verilerle birleştirilerek belirleyicilik kazanabilir.

Başka bir deyişle, psödoanonim verinin sahibinin kimliği doğrudan belirlenemez ama dolaylı olarak kimliğin belirlenmesi hala mümkündür.

- Psödoanonimizasyon uygulamasına örnek olarak, banka hesap verilerin tutulduğu sistemde gerçek kişinin ismi kullanılmaz ancak bir müşteri ID'si atanır ve bu ID üzerinden hesap bilgileri tutulur. Görüldüğü üzere veri tamamen kişiden ayrı değildir ancak hesap bilgilerinden gerçek kişiye ulaşılması için ekstra bir adım eklenmektedir.

Eklenen bu adım sayesinde verilerin gerçek kişiler ile bağlantısının kurulması zorlaştırılmakta ve ek veri güvenliği sağlanmış olmaktadır.

# GDPR’ın Getirdiği Yenilikler



## Risk Temelli Yaklaşım (Risk Based Approach)

GDPR’ın getirmiş olduğu sorumluluk rejimi risk temelli bir yaklaşım benimsemektedir. Veri sorumlularının yükümlülükleri, veri işleme faaliyetinin doğurduğu risk ile doğru orantılıdır.

GDPR’ın getirmiş olduğu sorumluluk rejimi risk temelli bir yaklaşım benimsemektedir.

Bu yaklaşıma göre, veri sorumlusunun veri işleme faaliyetindeki risk seviyesi arttıkça, hesap verilebilirliğe ilişkin yükümlülükleri de ağırlaşmaktadır. Benzer şekilde, düşük riskli veri işleme faaliyetlerinde bulunan veri sorumluları ise bazı özel yükümlülükleri yerine getirmek zorunda tutulmamıştır.

GDPR’da kategorik olarak sayılan yüksek riskli faaliyetler:

- Kişileri kayda değer şekilde etkileyen sistematik ve geniş çaplı otomatik profilleme faaliyetleri,
- Geniş kapsamlı özel nitelikli kişisel veri işleme faaliyetleri,
- Kamuya açık alanların sistematik olarak gözetlendiği durumlar.

→Veri ihlallerinin yüksek risk arz ettiği durumlarda veri sahiplerine bildirim yapılması, → «veri koruması etki değerlendirmesi» yapılması, → veri işleme öncesi veri koruma otoritesine başvuru gibi yükümlülükler yalnızca yüksek riskli veri işleme faaliyetleri yürüten veri sorumluları üzerinde doğmaktadır.

# GDPR'ın Getirdiği Yenilikler



## Risk Temelli Yaklaşım (Risk Based Approach)

### Risk Temelli Yaklaşım Nedir?

- GDPR'ın getirmiş olduğu sorumluluk rejimi risk temelli bir yaklaşım benimsemektedir.
- Bu yaklaşıma göre, veri sorumlusunun veri işleme faaliyetindeki risk seviyesi arttıkça, hesap verilebilirliğe ilişkin yükümlülükleri de ağırlaşmaktadır. Benzer şekilde, düşük riskli veri işleme faaliyetlerinde bulunan veri sorumluları ise bazı özel yükümlülükleri yerine getirmek zorunda tutulmamıştır.

### Risk Temelli Yaklaşım Ne Değildir?

- Risk Temelli Yaklaşım kişisel verilerin korunması hakkına ve ilkelerine alternatif değildir. Her ne kadar düşük riskli olursa olsun, her türlü veri işleme faaliyeti sırasında kişilerin kişisel verileri üzerindeki hakları eksiksiz bir şekilde korunmak durumundadır.
- Risk temelli yaklaşım daha çok mevcut mevzuata uyumluluk sırasında kullanılacak bir ölçeklendirme ve orantılılık metodu olarak düşünülebilir.

# GDPR'ın Getirdiği Yenilikler

## Risk Temelli Yaklaşım Risk Ölçümü?

- GDPR Madde 24 kapsamında «risk», iki unsur ekseninde ölçümlenmektedir:
  I. Riskin gerçekleşme ihtimali (*Likelihood of occurence*).
  II. Riskin gerçekleşmesi durumunda kişilerin hak ve özgürlükleri üzerinde doğuracağı etkinin ağırlığı (*Severity of the impact*).
- Risk ölçümü sorumluluğu veri sorumlularının üzerindedir. Risk ölçümü, veri işleme faaliyeti öncesinde gerçekleştirilmelidir.
- GDPR Madde 35 uyarınca kategorik olarak «yüksek riskli» faaliyetler:
  - Kişileri kayda değer şekilde etkileyen sistematik ve geniş çaplı otomatik profilleme faaliyetleri,
  - Özel nitelikli verileri geniş kapsamlı işleme faaliyetleri,
  - Kamuya açık alanların sistematik olarak gözetlendiği durumlar.
- Verilen örneklerden yola çıkarak şu çıkarımlar yapılabilir:
  - Verisi işlenen kişi sayısı arttıkça risk artmaktadır.
  - Ayrımcılığa sebep olabilecek veri işleme faaliyetleri ile kişileri sosyal veya ekonomik açıdan negatif etkileyecek işleme faaliyetleri riskli görülmektedir.
- Yüksek riskli veri işleme faaliyetleri bunlarla sınırlı değildir. Madde 35'e göre ulusal veri koruma otoritelerinin hangi veri işleme faaliyetlerinin doğrudan «yüksek riskli» kabul edeceğine ilişkin liste yayınlama yetkisi vardır.

# Veri Güvenliği



- GDPR'ın 32. maddesi veri işlemede güvenliğe ayrılmıştır. Maddede veri sorumlularına veri işleme eyleminin doğuracağı risklerle doğru orantılı olarak gerekli teknik ve idari tedbirleri alma yükümlülüğü getirilmektedir («*risk temelli yaklaşım*»). Hangi önlemlerin alınması gerektiği tahdidi olarak sayılmamış ancak alınabilecek önlemlere örnekler verilmiştir:
  - Kişisel verilerin psödoanonimizasyon ve kriptolama yöntemleriyle korunması,
  - Veri işleme sistemlerinin ve hizmetlerinin gizliliğinin, güvenliğinin, ulaşılabilirliğinin ve dirençliliğinin sağlanması
  - Teknik veya fiziksel bir kazanın meydana gelmesi durumunda sistemlerin eski haline döndürülmesi için gerekli önlemlerin alınması
  - Sistemlerin güvenilirliğinin sağlanması için alınan önlemlerin düzenli olarak kontrol edilmesi.
- Mesleki kurallara uyulduğunun veya çeşitli veri güvenliği sertifikalarının (ISO 27001 gibi) alındığının belgelenmesi halinde bu belgelerin veri güvenliği yükümlüğünün yerine getirildiğine ilişkin kanıt teşkil edeceği de maddede açıkça belirtilmiştir (*«hesap verilebilirlik prensibi»*).
- Ayrıca, ilgili hükme göre veri sorumlularına, talimatlarına uygun olarak çalışan kendisine veya veri işleyene bağlı olarak çalışan kişilerin veri sorumlusunun talimatlarına uygun olarak veri işlediğini güvence altına alacak adımları atma yükümlülüğü getirmiştir.
  - Bu durumda, örneğin bankalar kendi çalışanlarının veri işleme faaliyetlerini denetlemeli ve banka tarafından verilen talimatlar haricinde veri işleme faaliyetleri gerçekleştirmelerini önleyici önlemler almalıdır.

# Teşekkürler

BİLGİ Bilişim ve
Teknoloji Hukuku
Enstitüsü