

GDPR EĞİTİMİ

KVKK Karşılaştırmalı

&

AB Karar Örnekleriyle

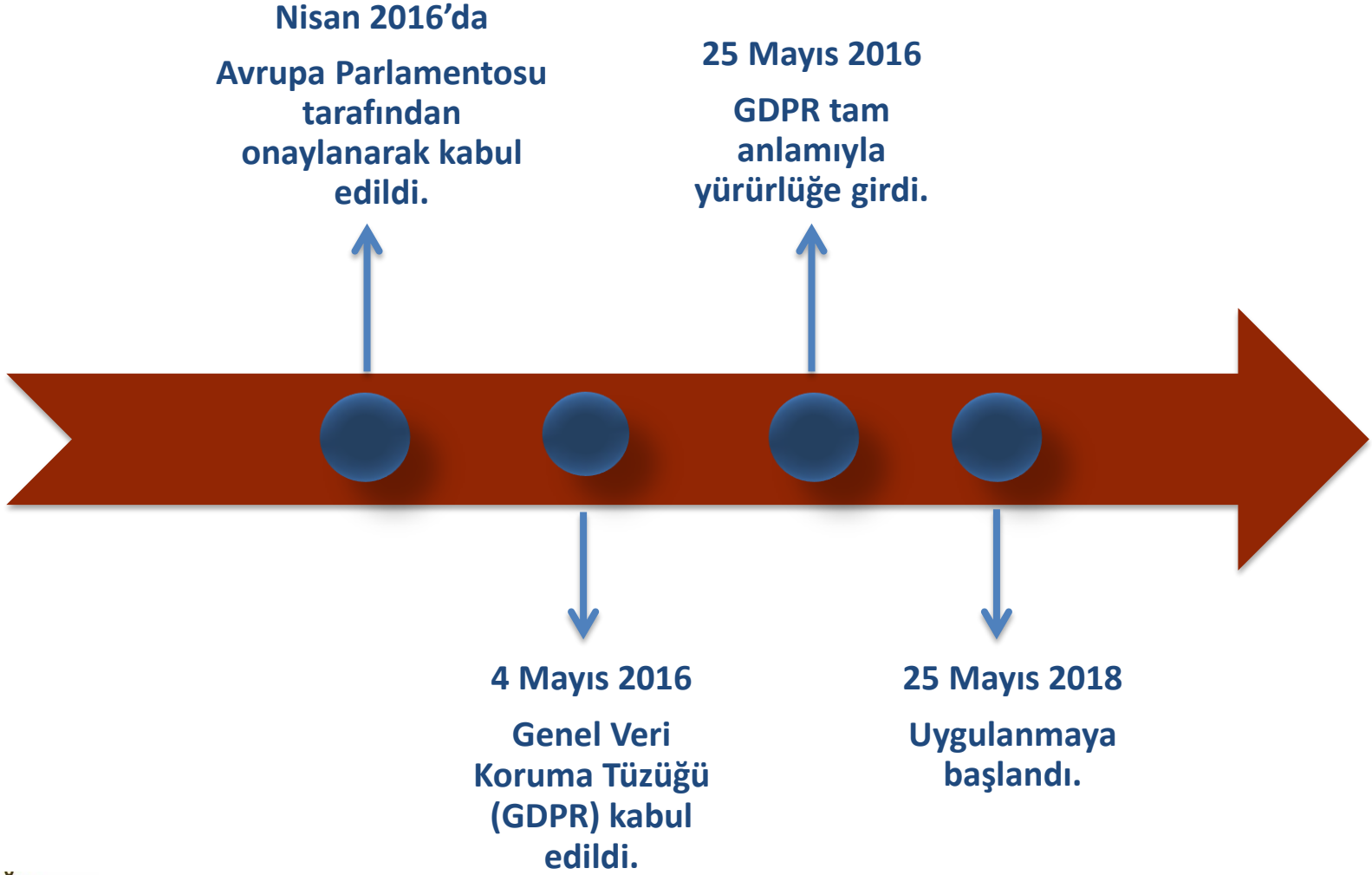
Av. Dr. Çiğdem Ayözger Öngün
Av. Begüm Ertürk

İçerik

- 1. GDPR'ın Amacı, Kapsamı ve Uyum Süreci**
- 2. GDPR'ın Getirdiği Başlıca Yenilikler**
- 3. GDPR'daki Aktörler ve Sorumlulukları**
- 4. GDPR Kapsamında Kişisel Veri İşleme ve Şartları**
- 5. GDPR Kapsamında Aydınlatma ve Açık Rıza**
- 6. GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci**
- 7. GDPR Kapsamında Veri Güvenliği**
- 8. GDPR Kapsamında Otoriteye ve Komisyona Başvuru**
- 9. GDPR'da Düzenlenen Yaptırımlar ve Tazminat Hakkı**
- 10. Şirketinizin GDPR'a Uyum Kapsamında Alması Gereken Aksiyonlar**

GDPR'ın Amacı, Kapsamı ve Uyum Süreci

GDPR Yürürlük ve Uyum Süreci



GDPR'ın Amacı

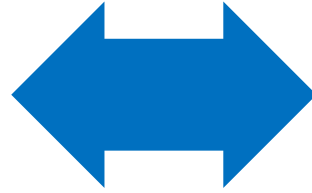
GDPR'ın Amacı Nedir?



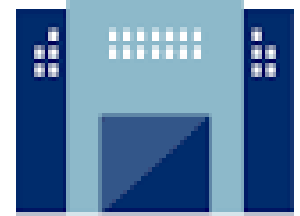
- Gerçek kişilerin;
 - temel hakları ve özgürlükleri ve özellikle kişisel verilerin korunması hakkının korunması,
 - kişisel verilerinin işlenmesiyle ilgili olarak korunmasına ilişkin kuralların belirlenmesi,
- Kişisel verilerin AB içerisinde serbest dolaşımının sağlanmasına yönelik kuralların belirlenmesi

GDPR Kimlere Uygulanır?

Avrupa Birliği'nde bulunan
Bir veri sorumlusu veya işleyenin faaliyetleri bağlamında kişisel verileri işlenen gerçek kişiler



Avrupa Birliği'nde mukim/değil
Bu verileri işleyen gerçek veya tüzel kişiler



GDPR'ın Getirdiđi Bařlıca Yenilikler

GDPR'ın Getirdiđi Temel Yenilikler

- Veri koruma etki analizi
- Çocuklara yönelik düzenlemeler
- Opt-in anlayışı
- Veri İşleyenin Sorumlulukları
- Privacy by design- privacy by default
- Yurt dışına veri aktarımı
- Veri taşınabilirliği hakkı
- Unutulma hakkı
- DPO atama zorunluluđu
- Veri İhlali Bildiriminde Bulunma
- Bağlayıcı Şirket Kuralları
- Tazminat hakkı
- Yaptırımlar

GDPR'daki Aktörler ve Sorumlulukları

Veri Sorumlusu

Kimdir?



Sorumlulukları Nelerdir?

Yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır

Veri işleme faaliyetlerinin GDPR'da yer alan düzenlemeler ile uygun şekilde gerçekleştirilmesini sağlama ve bunu sağlayabilme adına uygun teknik ve idari tedbirleri alma

Veri İşleyen

Kimdir?



Sorumlulukları Nelerdir?

Veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır

Veri işleme faaliyetinin gerekliliklerinin yerine getirilmesini ve ilgili kişinin haklarının korunmasını sağlayacak biçimde uygun teknik ve idari tedbirler uygulama hususunda yeterli güvenceler sağlayacaklardır

GDPR ile Gelen Yenilikler

- Veri sorumlusunun yanı sıra ***işleme faaliyetinin GDPR'a uyumlu*** olmasından sorumlu tutulması
- Veri sorumlusu ile arasında işleme faaliyetinin ***konusu ve süresi, işleme faaliyetinin mahiyeti ve amacı, kişisel verilerin türü ve veri sahiplerinin kategorileri ile veri sorumlusunun yükümlülükleri ve haklarının*** ortaya konduğu bir ***sözleşmenin*** düzenlenmesi

İlgili Kişi

Hakları

Bilgi edinme hakkı

Erişim hakkı

Düzeltilme hakkı

Silme hakkı (unutulma hakkı)

İşleme faaliyetini kısıtlama hakkı

Veri taşıma hakkı

İtiraz hakkı

Otomatik karar verme süreçlerine ilişkin hakkı



GDPR Kapsamında Kişisel Veri İşleme ve Şartları

GDPR Kapsamında Kişisel Veri İşleme



- Otomatik işleme
- Otomatik olmayan yollarla işleme
- **Kayıt sistemi:** “*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*”

GDPR Kapsamında Kişisel Veri İşleme Şartları



GDPR Kapsamında Aydınlatma ve Açık Rıza

Aydınlatma Yükümlülüğü



Rıza Alma Yükümlülüğü

Hukuka uygunluk nedenlerinin mevcut olmadığı ve açık rıza gerektirmeyen diğer veri işleme faaliyetleri için

Rıza

Açık Rıza

Özel Nitelikli Kişisel Veriler, Profilleme ve Otomatik yöntemlerle ilgili kişiler hakkında karar verme amacıyla gerçekleştirilen veri işleme faaliyetleri için

Opt-In Anlayışı

- GDPR kapsamındaki rıza- açık rıza anlayışı kişilerin «açık onay eylemi»ne dayanmaktadır.
- Bu kapsamda GDPR uyarınca kendiliğinden tiklenmiş onay kutucuklarının kullanıcıya sunulması ve kullanıcının onay vermeyi tercih etmiyor olması halinde tiki geri alması anlayışının yerine boş onay kutucuğunun kullanıcıya sunulması anlayışının benimsenmesi gerekmektedir.

The image shows two identical forms side-by-side, both titled "DOWNLOAD YOUR FREE REPORT". Each form has an "Email" field with the placeholder text "Your email address" and a checkbox labeled "I would like to subscribe to updates from Litmus." Below the checkbox is an orange "SUBMIT" button.

The left form has the checkbox unchecked, and a large black checkmark is placed to its right, indicating this is the correct, compliant approach.

The right form has the checkbox checked, and a large black 'X' is placed to its right, indicating this is the incorrect, non-compliant approach.

GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci

GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci



Kişisel Verinin Paylaşılması

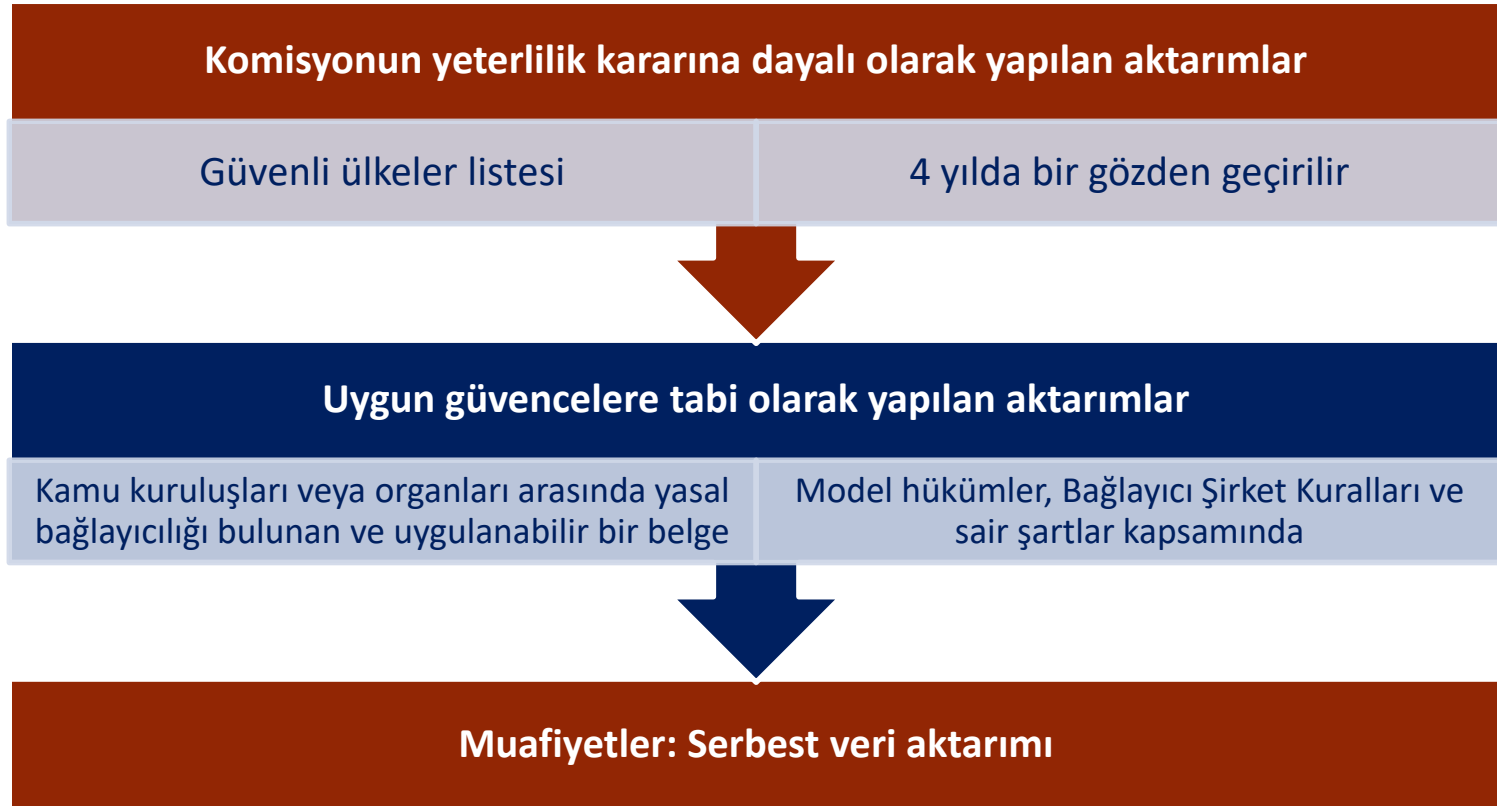
- AB içindeki kişisel verilerin paylaşılabilmesi için;
- **İlgili kişinin rızasının** alınmış veya diğer **hukuka uygun işleme şartlarının sağlanmış olması** aranmaktadır.
 - ***Rızanın istisnası:*** kamu yararı, meşru menfaat veya hukuki yükümlülük gibi hukuki gerekçelerin bulunması

Kişisel Verinin Sınır Ötesi Aktarımı

- AB dışına gerçekleşen kişisel veri aktarımı için ise kısaca;
- Hukuka uygun işleme şartlarının sağlanması
 - AB Komisyonu'nun yeterli koruma kararının bulunması veya uygun güvencelerin değerlendirilmesi gerekir

GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci

Kişisel Verinin Sınır Ötesi Aktarımının Şartları



GDPR Kapsamında Veri Mahremiyeti ve Güvenliđi

Veri Koruma Etki Analizi

Amaç ?

- Kurulacak bilişim sistemleri, çeşitli uygulamalar ya da belirlenecek olan politika ve prosedürlerden kaynaklanabilecek veri kayıplarını asgari düzeye çekerek potansiyel kişisel veri ihlallerine engel olmayı amaçlamaktadır.

Ne zaman?

- Kişisel veri işleme faaliyetinde kullanılacak teknoloji (sistem, uygulama) kurulmadan, bu teknoloji vasıtasıyla gerçekleştirilecek işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alınır.

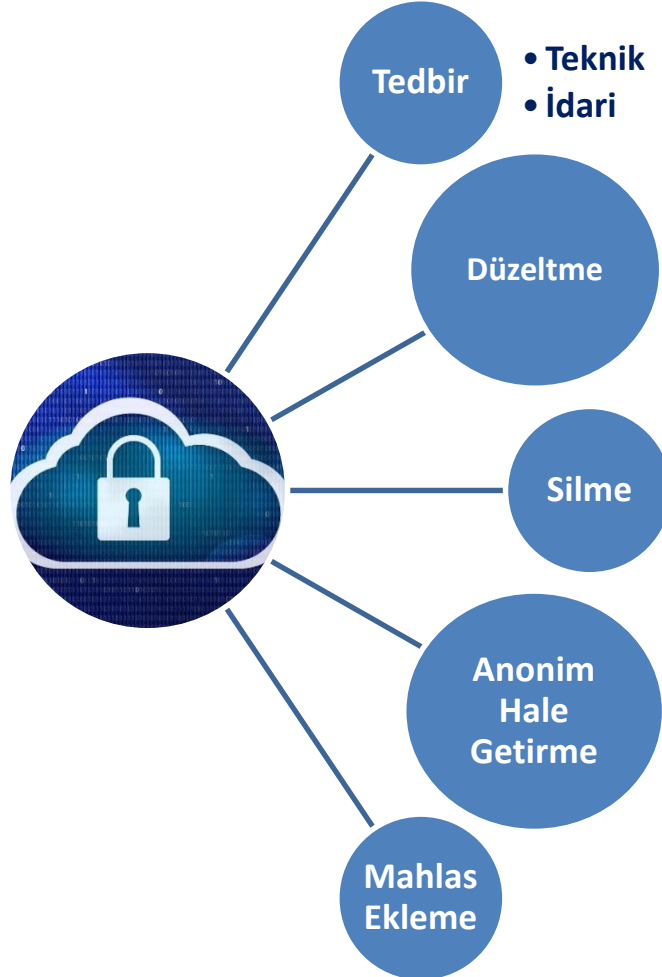
Hangi hallerde?

- Gerçek kişilerle ilgili kişisel özellikler hususunda profil çıkarma da dahil olmak üzere **otomatik işleme dayalı** olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya **gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı** sistematik ve kapsamlı bir değerlendirme;
- **Özel nitelikli kişisel** veriler veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi veya
- **Kamunun** erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi hallerinde



GDPR Kapsamında Veri Mahremiyeti ve Güvenliđi

Veri sorumlusu ve veri işleyen, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiye tlelere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduđu hallerde uygun teknik ve idari tedbirleri uygular.



GDPR Kapsamında Veri Mahremiyeti ve Güvenliđi

Düzeltilme

İlgili kişinin talebi üzerine veya re'sen



Silme (Unutulma Hakkı)

Aşağıdaki hallerden birinin geçerli olması durumunda, Veri Sorumlusu'nun kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüđü bulunur:

- kişisel verilerin toplanma veya işleme amaçlarıyla ilişkili olarak artık gerekli olmaması,
- Rızanın geri çekilmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;
- İlgili kişinin veri işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da ilgili kişinin işleme faaliyetine itirazda bulunması,
- kişisel verilerin yasa dışı biçimde işlenmiş olması,
- kontrolörün tabi olduđu Birlik veya üye devlet hukukundaki bir yasal yükümlülüđe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması.

Kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının silinmesi

Alınacak Başlıca Teknik ve İdari Tedbirler



DPO (Veri Koruma Görevlisi) Atama Zorunluluğu



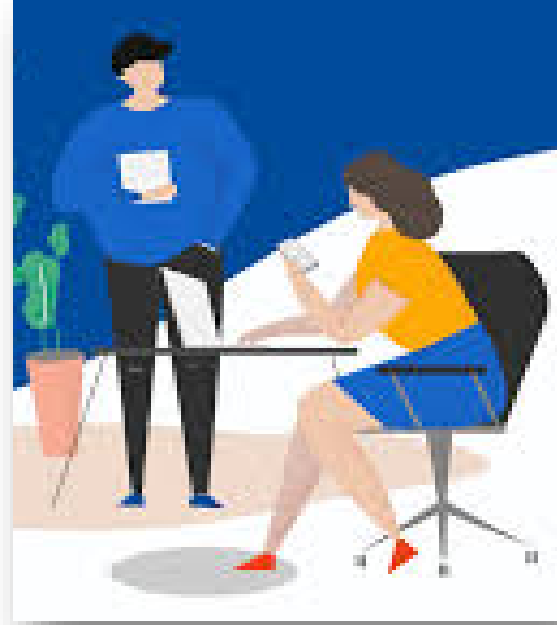
Aşağıdaki durumlarda **hem veri sorumlusu hem de veri işleyenin** DPO atama zorunluluğu vardır:

- İşleme faaliyetinin kendi yargı yetkisi çerçevesinde hareket eden mahkemeler haricindeki bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi;
- Veri sorumlusu veya veri işleyenin temel faaliyetlerinin yapıları, kapsamaları ve/veya amaçları gereği veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya
- Veri sorumlusu veya veri işleyenin temel faaliyetlerinin özel nitelikli verileri ve mahkumiyet kararları ile ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi.

GDPR Kapsamında Otoriteye ve Komisyona Başvuru

İlgili Kişinin Başvuru Hakkı

Her ilgili kişi, kendisi ile alakalı kişisel verilerin işlenmesinin GDPR'ı ihlal ettiğini düşündüğü hallerde, başka bir idari veya adli çözüm yoluna başvuru hakkı saklı kalmak üzere, ikamet adresinin, iş yerinin veya iddia edilen ihlalin olduğu yerdeki üye devletteki başta olmak üzere bir denetim makamına şikayette bulunma hakkına sahiptir.



Ayrıca, veri sorumlusunun veya veri işleyeninin bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması haricinde, böyle davalar ilgili kişinin mutlak meskeninin bulunduğu üye devletin mahkemelerinde de açılabilir.



Veri Sorumlusu/İşleyeninin Başvuru Hakkı

- Veri sorumlusunun veya veri işleyeninin bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması haricinde, böyle davalar ilgili kişinin mutlak meskeninin bulunduğu üye devletin mahkemelerinde de açılacaktır.
- Her gerçek veya tüzel kişinin, başka bir idari veya adli olmayan çözüm yoluna hânel getirmeksizin, bir denetim makamının kendileriyle ilgili yasal bağlayıcılığı olan bir kararına karşı etkili bir kanun yoluna başvurma hakkı vardır.
- Denetim makamına karşı açılacak davalar, denetim makamının kurulu bulunduğu üye devlet mahkemelerinde açılacaktır.



GDPR'da Düzenlenen Yaptırımlar ve Tazminat Hakkı

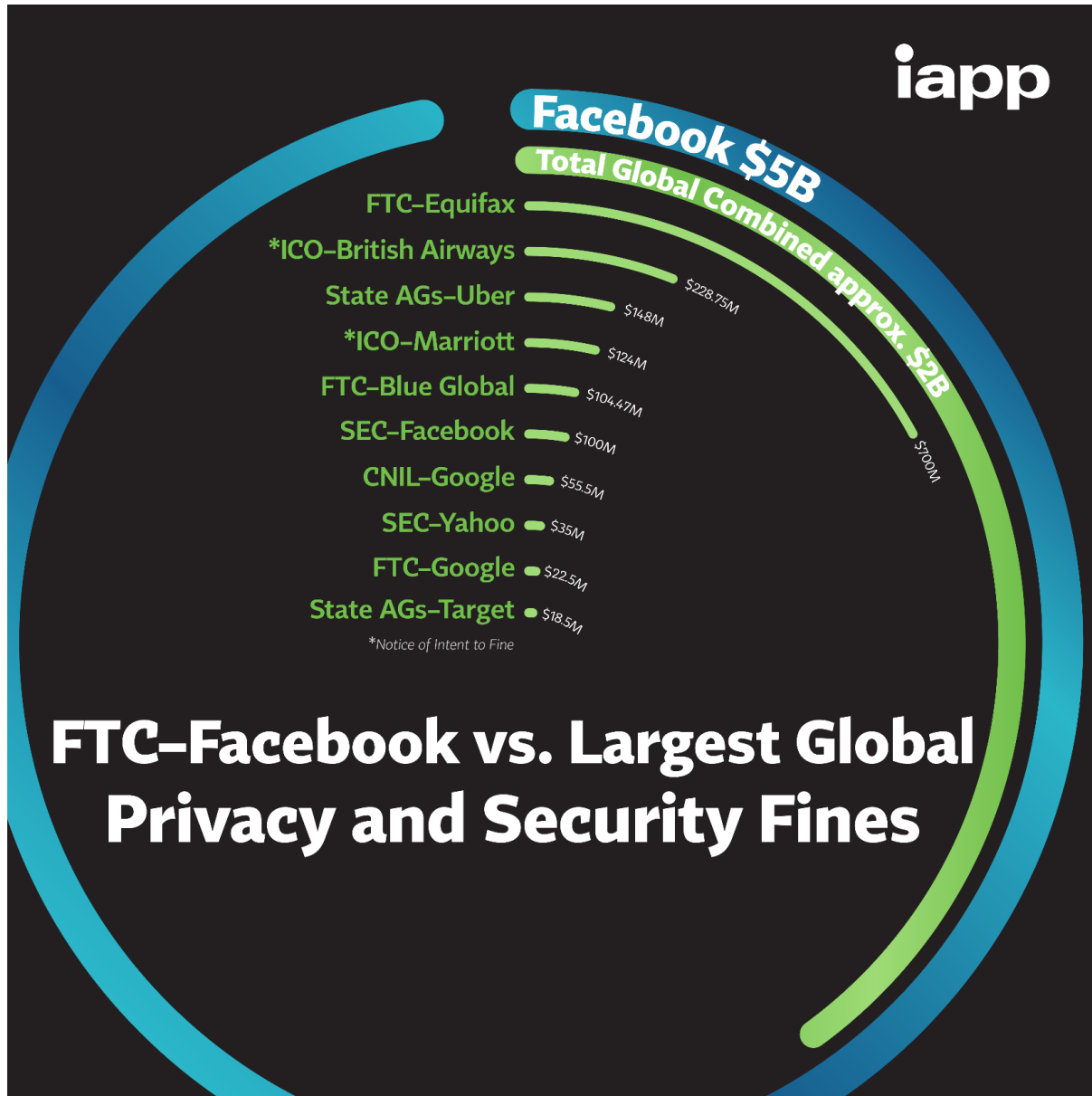
GDPR Yaptırımları

İdari para cezaları, her münferit durumun özelliklerine dayalı olarak, 58(2) maddesinin bentlerinde atıfta bulunulan tedbirlere ek olarak veya bu tedbirler yerine kesilir. Her münferit durumda bir idari para cezası kesilip kesilmeyeceğine karar verilirken ve idari para cezası meblağına karar verilirken somut olayın mahiyetine bakılır.

58(2) maddesinde atıfta bulunduğu üzere bir emirle uyumlu hareket edilmemesi, 2. paragraf uyarınca, 20.000.000 Euro'ya kadar veya, bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir) tabidir.

10.000.000 Euro'ya kadar veya, bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir) tabidir.

20.000.000 Euro'ya kadar veya, bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir) tabidir:



FTC-Facebook vs. Largest Global Privacy and Security Fines

Tazminat Hakkı



Hak ihlaline (hukuka aykırı işleme, veri sızıntısı gibi hallerde) uğrayan veri sahiplerine tazminat talebi imkanı tanınmıştır. Buna göre GDPR' ı ihlal eden veri sorumluları işleme faaliyetinin sebep olduğu zarardan sorumludur. Veri işleyenler ise ancak GDPR'ın özellikle kendilerine yönelik yükümlülüklerine uyum göstermediği veya veri sorumlusunun hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde, işleme faaliyetinin sebep olduğu zarardan sorumlu olacaklardır.

Şirketinizin GDPR'a Uyum Kapsamında Alması Gereken Aksiyonlar

Şirketinizin GDPR'a Uyum Kapsamında Alması Gereken Başlıca Aksiyonlar

Uçtan Uca GDPR Uyum Projesinin Temel Çıktı ve Aksiyonları

A. Temel Çıktılar

1. Veri Koruma Etki Analizi Süreci

2. Veri Koruma Uyum Süreci

VKEA Raporu kapsamında Kişisel Veri Envanteri, Aydınlatma Metinleri(Örneğin: Çalışan, Müşteri), Açık Rıza Metinleri gibi belgeler hazırlanmalıdır.

B. Temel Çıktılar



Teşekkürler

İşbu sunum, Çağrı Merkezi Derneği üyelerine özel olarak bilgilendirme amacıyla hazırlanmış olup; içeriğinde yer alan bilgi ve yorumlar, kişi ve kurumları bağlayıcı hukuki tavsiye veya görüş niteliği taşımamaktadır. Sunum içeriğindeki bilgilerin zaman içinde değişmesi ve/veya uygulanamaz hale gelmesinden dolayı SRP-Legal sorumluluk kabul etmemektedir.

Her hakkı SRP-Legal'e aittir. 5846 sayılı Fikir ve Sanat Eserleri Kanunu hükümleri uyarınca eser sahibinin izni olmaksızın işbu eserin hiçbir bölümü kısmen veya tamamen paylaşılamaz, çoğaltılamaz ve ticari maksatla veya kısmen de olsa amacı dışında kullanılamaz.

©2019, SRP-Legal Hukuk Ofisi, Tüm hakları saklıdır.