Katılımcılara özeldir,
paylaşılamaz, çoğaltılamaz

31.07.2019

GDPR EĞİTİMİ

KVKK Karşılaştırmalı
&
AB Karar Örnekleriyle

Av. Dr. Çiğdem Ayözger Öngün
Av. Begüm Ertürk

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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 içi ve Sınır Ötesi Veri Aktarımı Süreci
7. GDPR Kapsamında Veri Mahremiyeti ve 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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

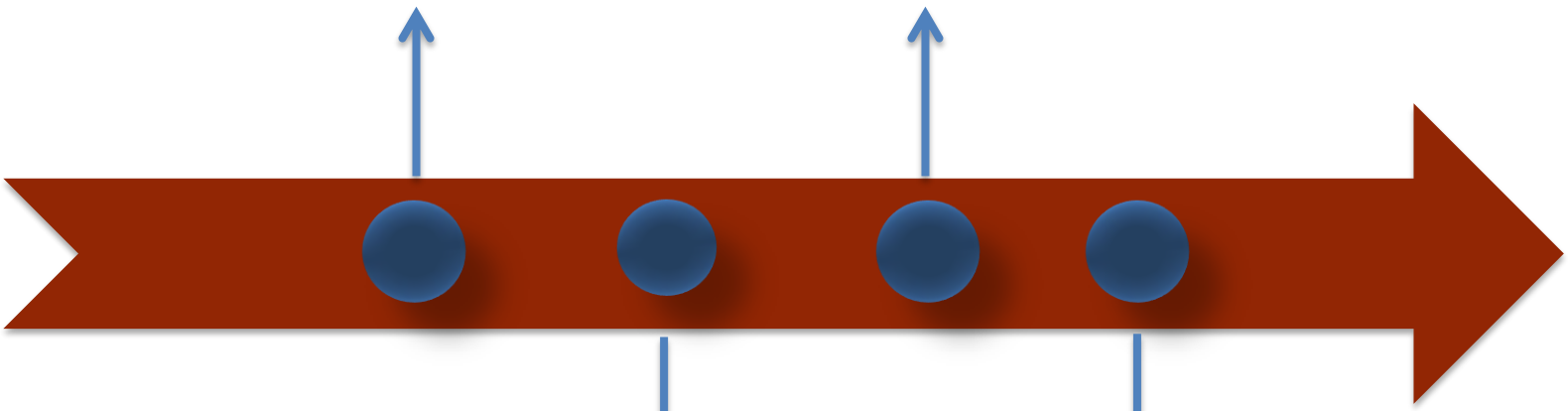
GDPR Yürürlük ve Uyum Süreci

Nisan 2016'da

Avrupa Parlamentosu tarafından onaylanarak kabul edildi.

25 Mayıs 2016

GDPR tam anlamıyla yürürlüğe girdi.



4 Mayıs 2016

Genel Veri Koruma Tüzüğü (GDPR) kabul edildi.

25 Mayıs 2018

Uygulanmaya başlandı.

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Yürürlük ve Uyum Süreci

Portekiz, Çek Cumhuriyeti, Romanya, Hırvatistan, Kıbrıs gibi bazı AB ülkeleri henüz yerel düzenlemelerini GDPR'a uyarlamamıştır.

Portekiz KVK Otoritesi (CNPD), **Avrupa Genel Veri Korumu Tüzüğü'nün (GDPR) ihlali sebebiyle bir hastaneye 400.000 avro para cezası verdi**. Yürütülen soruşturmada hastane çalışanlarının, psikolog, diyetisyen ve diğer uzmanların sahte hesaplar ile hasta kayıtlarına ulaştıkları tespit edilmiştir. Hastalara ait kişisel verilerin tutulduğu sistem incelendiğinde hastanede çalışan 296 doktor olmasına rağmen, sistemde 985 doktor profili bulunduğu görülmüştür. Bunun yanı sıra doktorların tüm hasta kayıtlarına herhangi bir kısıtlama – özellikle branş alanlarına göre bir sınırlama – olmaksızın erişebildikleri fark edilmiştir. Tüm bu bilgiler doğrultusunda Otorite, hastanenin; hasta verilerinin korunması için gerekli teknik ve idari tedbirleri almadığına karar vermiştir. Yukarıda yer alan karar, GDPR'ın uygulandığı ilk kararlardan biridir.

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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

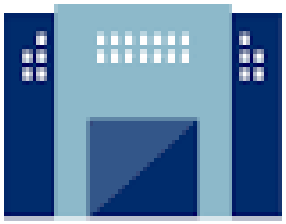
GDPR Kimlere Uygulanır?

Avrupa Birliğinde **bulunan**

kişisel verileri işlenen gerçek kişiler

AB'de yerleşik/ değil

Bu verileri işleyen gerçek veya tüzel kişiler



ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR’ın Getirdiği Başlıca Yenilikler

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR'ın Getirdiği 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 zorunluluğu
- Veri İhlali Bildiriminde Bulunma
- Bağlayıcı Şirket Kuralları
- Tazminat hakkı
- Yaptırımlar

GDPR’daki Aktörler ve Sorumlulukları

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

Veri Sorumlusu

Kimdir?

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

Sorumlulukları Nelerdir?

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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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 **sözleşme**nin düzenlenmesi

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

İlgili Kişi

Hakları

- Bilgi edinme hakkı
- Erişim hakkı
- Düzeltme hakkı
- Silme hakkı (unutulma hakkı)
- İşleme faaliyetini kısıtlama hakkı
- Ver taşıma hakkı
- İtiraz hakkı
- Otomatik karar verme süreçlerine ilişkin hakkı

Yükümlülüğü:

Kişisel verilerinin korunup korunmadığını DENETLEME

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında Kişisel Veri İşleme ve Şartları

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında Kişisel Veri İşleme

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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında Kişisel Veri İşleme Şartları

- Açık Rıza
- Sözleşme
- Hayati Çıkarlar
- Meşru Menfaat
- Kamu Çıkarları

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında Aydınlatma ve Açık Rıza

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

Aydınlatma Yükümlülüğü

İlgili Kişiden Elde Edilen Kişisel Veriler için

Aydınlatma Yükümlülüğü-nün Kapsamı

- Varsa, DPO irtibat bilgileri;
- Veri sorumlusunun ve varsa, temsilcisinin kimlik ve irtibat bilgileri;
- işlenme amaçları ve hukuki sebepleri
- Varsa, veri sorumlusunun meşru menfaatleri
- Mevcutsa alıcılar veya kişi kategoriler
- Yurtdışı aktarım olması halinde buna ilişkin bilgiler

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

Rıza Alma Yükümlülüğü

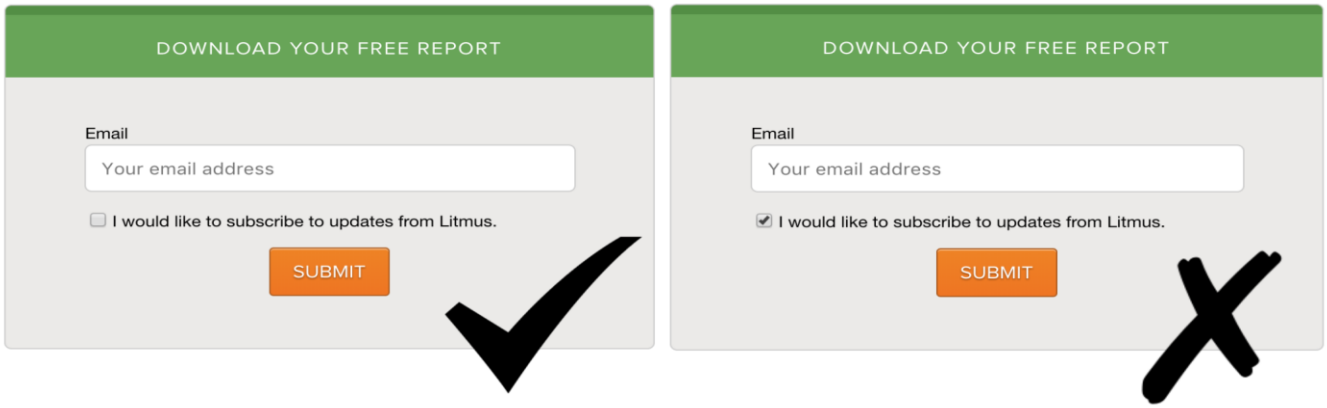
Rıza:
Hukuka uygunluk nedenlerinin mevcut olmadığı ve açık rıza gerektirmeyen diğer veri işleme faaliyetleri için

Açık Rıza:
Özel Nitelikli Kişisel Veriler, Profilleme ve Otomatik yöntemlerle ilgili kişiler hakkında karar verme amacıyla gerçekleştrilen 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.



GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci

Kişisel Verinin Paylaşılması	Kişisel Verinin Sınır Ötesi Aktarımı
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	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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında AB İçi ve Sınır Ötesi Veri Aktarımı Süreci

Kişisel Verinin Sınır Ötesi Aktarımının Şartları

Komisyonun yeterlilik kararına dayalı olarak yapılan aktarımlar

Güvenli ülkeler listesi	4 yılda bir gözden geçirilir

Uygun güvencelere tabi olarak yapılan aktarımlar

Kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge	Model hükümler, Bağlayıcı Şirket Kuralları ve sair şartlar kapsamında

Muafiyetler: Serbest veri aktarımı

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında
Veri Mahremiyeti ve Güvenliği

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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 işlemeye 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
- ***Kamu***nun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi hallerinde

SRP legal
strateji regülasyon politika

GDPR Kapsamında Veri Mahremiyeti ve Güvenliği

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 ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde uygun teknik ve idari tedbirleri uygular.

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

GDPR Kapsamında Veri Mahremiyeti ve Güvenliği

Düzeltme

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 yükümlülüğü bulunur:

- kişisel verilerin toplanma veya işlenme 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 olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe 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

- kişisel verilerde takma ad kullanımı ve şifreleme
- işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi
- fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi
- işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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, kapsamları 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.

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

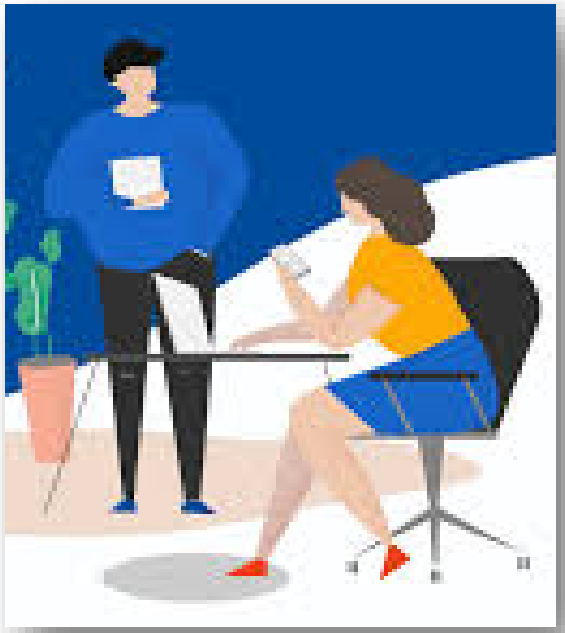
GDPR Kapsamında Otoriteye ve Komisyona Başvuru

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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 işleyenin bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması haricinde, böyle davalar ilgili kişinin mutat meskeninin bulunduğu üye devletin mahkemelerinde de açılabilecektir.

Veri Sorumlusu/İşleyenin Başvuru Hakkı

- Veri sorumlusunun veya veri işleyenin bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması haricinde, böyle davalar ilgili kişinin mutat meskeninin bulunduğu üye devletin mahkemelerinde de açılabilecektir.
- Her gerçek veya tüzel kişinin, başka bir idari veya adli olmayan çözüm yoluna halel 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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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.

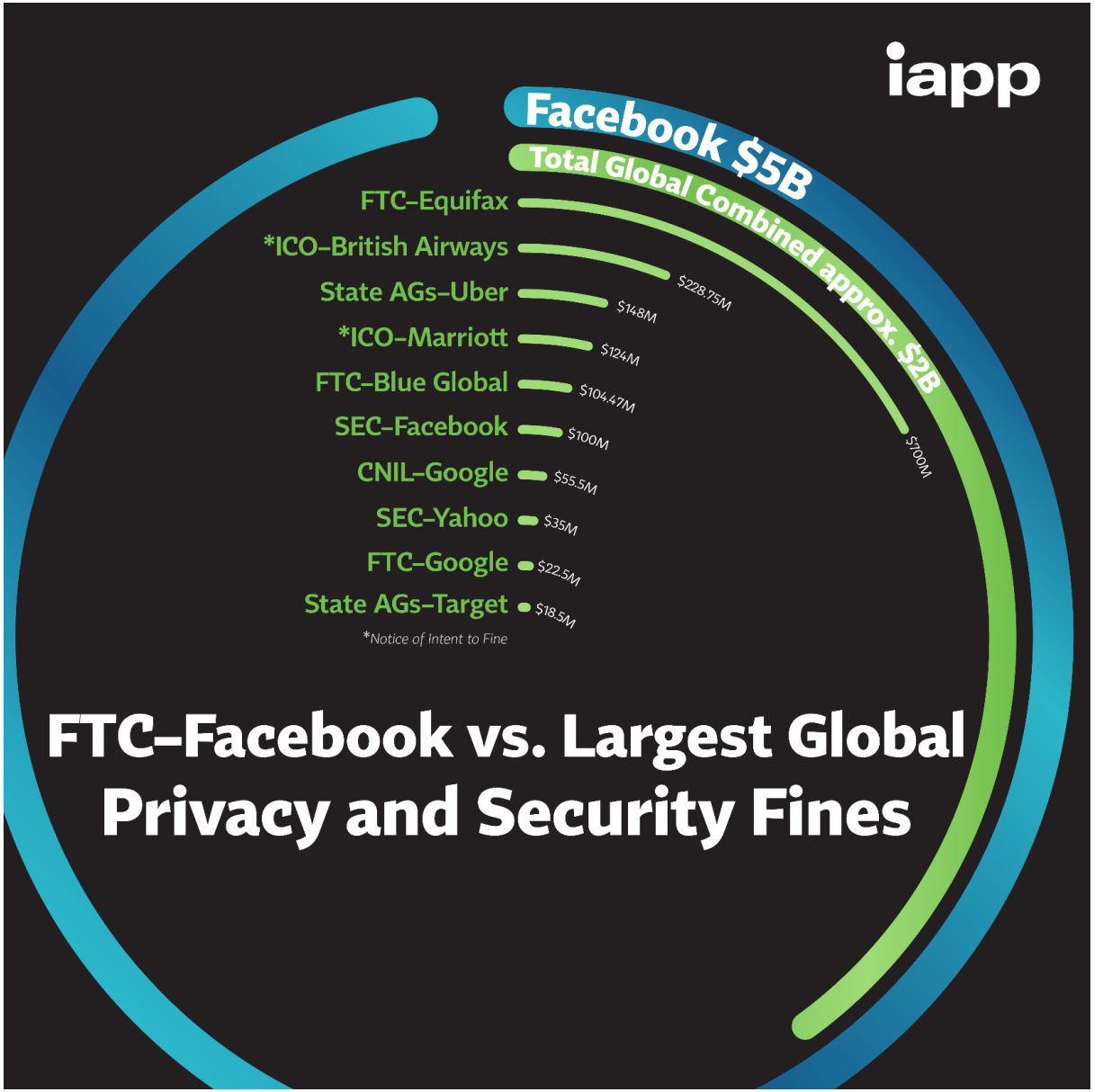
58(2) maddesinde atıfta bulunulduğu üzere bir emirle uyumlu hareket edilmemesi, 2. paragraf uyarınca, 20.000.000 Euro'ya kadar veya, bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir) tabidir.

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:

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika



ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

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

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika

Teşekkürler

Fikir ve Sanat Eserleri Kanunu gereği her türlü hakkı SRP-Legal'e aittir.

ÇAĞRI MERKEZLERİ DERNEĞİ
CALL CENTERS ASSOCIATION

SRP legal
strateji regülasyon politika