# GDPR NEDİR?

iab turkey

# GDPR Nedir?

Avrupa Birliği Genel Veri Koruma Düzenlemesi (GDPR), tüm Avrupa pazarlarındaki kişisel verinin kullanımı düzenleyen yeni bir yasal çerçevedir ve mevcut ulusal veri koruma kanunlarının yerine geçerek, 25 Mayıs 2018 tarihinden itibaren yürürlüğe girecektir.

Halen geçerli olan Avrupa Birliği Veri Koruma Çerçevesi'ni güncelleyen GDPR, tüketici bakış açısıyla bireylerin kendi kişisel bilgileri üzerinde daha fazla kontrol sahibi olmalarını hedeflemektedir.

Bu kapsamda şirketler, kişisel verileri işleyebilmek için yasal bir dayanağa ihtiyaç duyacaktır. Şu anda altı hukuki dayanak bulunmaktadır, ancak dijital reklamcılık sektöründe daha çok 'rıza' ve 'meşru menfaatler' kullanılmaktadır.

GDPR 'rıza' kavramının şartlarını daha da güçlendirecektir. Kişisel verinin işlenmesine yasal dayanak oluşturabilmesi için rızanın -Hüküm ve Koşullar'la birleştirilemeyecek- çok yüksek standartlar içermesi; ayrıca kullanıcının 'rıza'yı onaylayıcı bir eylemle ve açık bir şekilde vermesi gerekecektir. Irksal ve etnik köken ya da cinsel yönelim gibi 'hassas' kişisel verileri işleyebilmek için ise kullanıcının açık rıza vermesi şartı aranacaktır.

Tüm durumlarda geçerli olmak üzere, rızanın alındığına dair kanıt kayıt altına alınacak ve böylece kullanıcı ile doğrudan bir ilişkide olmayan şirketler rızayı dolaylı yollardan almanın yollarını bulmak zorunda kalacaktır.

GDPR ile yaptırımlar da artacaktır. Kanun ihlalleri halinde şirketler 20 milyon € ya da yıllık cirolarının %4'ü (hangisi yüksekse) kadar para cezasına çarptırılabilecektir.

## GDPR kimleri etkiliyor?

GDPR, şirketlerin veriyi toplama, paylaşma ve kullanma yöntemlerini de kapsamak üzere her türlü kişisel verinin kullanımını düzenlemektedir. Eğer bir şirket Avrupa Birliği'nde yaşayan bir bireyle ilgili kişisel veriyi işlerse (kişinin AB vatandaşı olması gerekmez), yasa işletmenin nerede kurulu olduğuna bakılmaksızın geçerli olacaktır.

Dijital reklamcılıkla ilintili tüm şirketler - reklamverenler, ajanslar, reklam networkleri, veri/teknoloji şirketleri ya da yayıncılar yasanın kapsamındadır.

Ayrıca GDPR çocukların kişisel bilgileri için de özel bir koruma sağlamaktadır. Eğer bir şirket 16 yaşın altındaki bir çocuğun bilgilerini toplayıp bu bilgileri işlemek isterse, çocuğun ailesinin ya da velisinin açık rızasını almak zorunda kalacaktır.

# GDPR Nedir?

## Tüm bunlar ne zaman değişecek?

Yeni GDPR çerçevesi 25 Mayıs 2018 itibariyle yürürlüğe girecektir. Dijital reklamcılıkla ilgili işletmelerin değişecek maddeleri ve anlamlarını kavrayarak, bu tarihten önce yol haritalarını geliştirmeleri ve uygulamaları önerilmektedir.

## IAB Türkiye bu konuda nasıl çalışmalar yürütüyor?

IAB Türkiye Kişisel Verileri Koruma Kanunu ile ilgili CDA Hukuk'tan Kağan Dora ve Mert Ulusoy ve BTS Legal avukatlarından Erdem Aslan'ın anlatımıyla 2 bilgilendirme toplantısı düzenlemiştir. Aynı şekilde Aralık 2017'de gerçekleştirilen Üye Bilgilendirme Toplantısı'nda 6698 numaralı Kişisel Verileri Koruma Kanunu (KVKK) ve GDPR konuları ele alınmıştır. Nisan ayında da KVKK ve GDPR konularına yönelik sektörü bilgilendirmeye yönelik kapsamlı bir toplantı daha yapılacak, BTS Legal avukatlarından Erdem Aslan konuyla ilgili ayrıntılı bilgi aktaracaktır.

Ayrıca IAB Türkiye Programatik Çalışma Grubu ve Endüstri Standartları Yürütme Kurulu da konu ile ilgili güncel gelişmeleri yakından takip etmektedir.

## GDPR Kontrol Listesi

Yeni düzenlemeye yönelik uyum süreçlerini yakından takip edebilmeniz için aşağıdaki adımları izlemeniz önerilmektedir:

1. Farkındalık
2. Uyum sürecini kayıt altına almak
3. Kişisel verilerin işlenmesi için yasal dayanak
4. Rıza
5. Bulanıklaştırma (Pseudonymisation)
6. Kişisel bilgileri tebliğ etmek
7. Bireylerin hakları
8. Veri kontrolörleri ve veri işleyicileri
9. Veri ihlalleri
10. Tasarımdan İtibaren Veri Koruması ve Kişisel Gizlilik Etki Değerlendirmesi
11. Veri Koruma Görevlileri
12. Uluslararası

# GDPR Nedir?

## 1. Farkındalık

GDPR beraberinde yüklü para cezalarını da - yıllık küresel cironun %4'üne varan- beraberinde getirmektedir. Bu, karar vericilerin yeni yasa hakkında bilgili olmalarını gerektiren tek neden değildir. Bazı süreçler -hatta bazı ürünler- GDPR nedeniyle değişime uğramak durumunda kalabilecektir. Dijital reklamcılık alanında hizmet veren birçok işletme, ilk kez GDPR kadar kapsamlı bir veri koruma kuralları kümesine uyum sağlamak zorunda kalacaktır.

Konu hakkındaki farkındalığın artması için farklı departmanların ve tüm paydaşların bir araya gelmesi ve hep birlikte bir uyumluluk yol haritası oluşturulması gerekmektedir. Şu da unutmamalıdır: GDPR'a yönelik tüm adımlar AB'de iş yapan tüm şirketleri ilgilendirmekte, bu nedenle yurt dışında iş yaptığınız çalışma ekibinizin de sürece tüm hızıyla dahil olması gerekmektedir.

## 2. Uyum sürecini kayıt altına almak

Hesap verme zorunluluğu GDPR'ın ana temasını oluşturmaktadır. Hesap verebilmek için ne tür kişisel verinin saklandığının kayıt altında olması ve oluşabilecek her türlü riskin önceden tanımlanması gerekmektedir. Öncelikle bu noktadan başlamak mümkündür. GDPR'da yer alan kişisel veri tanımı, kişisel olarak tanımlanabilir bilgiden daha fazlasını kapsamaktadır. Böylece mevcut veri koruma mevzuatının kapsamı dışında olan veri noktaları da GDPR'ın kapsamına dahil edilmektedir. Bu, tekil tanımlayıcıların (örn. Cookie ID ya da reklam IDsi) 'anonim' veri olarak kabul edilmemesi anlamına gelmektedir.

Bu nedenle, en basit çözümün tüm online tanımlayıcıların kişisel veri olarak değerlendirilmesi olduğu düşünülebilir, böylece verinin nereden geldiği ve kiminle paylaşılacağına dair resim daha net anlaşılabilecektir. Bu sürecin daha iyi çözümlenebilmesi için bilgi denetimi gerçekleştirilebilir ve veri uygulama süreçleri devamlı olarak takip edilebilir.

# GDPR Nedir?

## 3. Kişisel verilerin işlenmesi için yasal dayanak

GDPR kapsamında şirketlerin kişisel veriyi işlemesi için verinin toplanması da dahil olmak üzere yasal bir doğrulamaya sahip olmaları gerekmektedir. GDPR altı yasal dayanak sunmaktadır:

- Rıza
- Sözleşmeler
- Yasal uyumluluk (başka bir yasayla)
- Kişinin hayati çıkarlarının korunması
- Kamu menfaati
- Meşru menfaat

Dijital reklamcılıkta iki yasal dayanak sıklıkla kullanılmaktadır: Rıza ve meşru menfaat. Bu şekilde, verinin işlenmesine yönelik farklı yollar değerlendirilebilir ve hangi yasal dayanağın hangi yönteme daha uygun olduğu saptanabilir. Ne tür bir işlem tasarlandığına veya verinin farklı bir amaç için işlenip işlenmeyeceğine de bağlı olarak bazı koşullarda, rıza ve meşru menfaatin kombinasyonu da kullanılabilir.

Mevcut ePrivacy Yönetmeliği'ne (cookie yasası) göre kullanıcının cihazındaki veriye ulaşmak ya da veriyi saklamak için rıza alınması gerekmektedir. 25 Mayıs 2018 itibariyle, daha katı rıza gereksinimleri GDPR ile birlikte yürürlüğe girecek ve bu gibi durumlarda geçerli olacaktır.

## 4. Rıza

Rıza, GDPR'ın en önemli basamağını oluşturmaktadır. Her ne kadar rıza, şirketlerin kişisel verileri işlemesi için en çok kullanımda olan dayanak olsa da birçok durum için uygun bir dayanak oluşturmamaktadır. GDPR, mevcut kurallarla karşılaştırıldığında, rıza koşullarını daha da sertleştirmektedir. Genel olarak, rızanın özgürce verilmiş olması, spesifik, bilgilendirici ve belirsizliğe mahal vermeyecek şekilde olması gerekmektedir. Hassas kişisel verilerin işlenmesine yönelik durumlarda rızanın açıkça verilmiş olması şart koşulmaktadır.

Yukarıdakilerin hepsi, işletmelerin rızanın yasal olarak alındığına dair kanıtlama zorunluluğunu göstermektedir. Özellikle başka bir şirketin sizin adınıza rıza aldığı durumlarda, rızanın doğrulanması hukuki açıdan oldukça gerekli hale gelmektedir.

GDPR'ın rıza gereksinimlerinin hangi durumlarda geçerli olduğunu anlayabilmek için IAB Avrupa'nın, Avrupa dijital reklamcılık sektörüne yönelik açıkladığı teknik rıza kılavuzunu inceleyebilirsiniz. Konuyla ilgili detaylı bilgiye www.advertisingconsent.eu adresi üzerinden; ayrıca 12.12.17 tarihinde Avrupalı regülatörler tarafından yayınlanan kılavuzun taslağına da buradan ulaşabilirsiniz.

# GDPR Nedir?

## 5. Bulanıklaştırma - Pseudonymisation

Kişiyi tanımlayan verilerin, analitik amaçlar için belli bir algoritma ile farklılaştırılmasıdır. Anonimleştirmeden farkı, istendiğinde aynı algoritma kullanılarak orijinal verilere tekrar ulaşılabilmesidir.

GDPR ilk defa pseudonymisation kavramını AB Veri Koruma Kanunu'na dahil etmektedir.

Pseudonymisation, iki ilgili konseptin birleştirilmesi olarak tanımlanabilir. Pseudonymisation verinin bir bireyle doğrudan bağlı olmadan geçirdiği süreçler olabilir (örneğin, şifreleme, adresleme ya da şifre sistemi). Herhangi bir tanımlayıcı detay içermeyen kişisel veriler, veri toplama sürecinin herhangi bir noktasında bulanıklaştırılabilir. Örneğin, "rastgele" bir cookie ID'si, kullanıcıyı ayırt edebilir fakat direkt olarak tanımlayamaz.

Şirketlerin hangi bulanıklaştırma yöntemini kullandıklarına bakılmaksızın, her iki durumda da kullanılan verinin GDPR tarafından kişisel veri olarak tanımlandığı unutulmamalıdır. Bulanıklaştırma kavramının özellikle şirketlerin GDPR'ın bazı zorunluluklarını (ayrıntılar için madde 7- bireylerin hakları) kısmen gidermesinin yanı sıra, kişisel gizliliği ve güvenliği artırıcı birçok açık yararı bulunmaktadır. Bulanıklaştırma, her türlü kişisel veri işlemesinin meşru menfaat kapsamında değerlendirilmesinin istendiği durumlarda dengeleyici test olarak da işlev görebilir.

## 6. Kişisel bilgileri tebliğ etmek

GDPR'ın bir diğer ana elementi de şeffaflıktır. Kişisel gizlilik kuralları ve bildirimleri sektörümüzde uzun süredir kullanılmaktadır. GDPR, verinin doğrudan bireyin kendisinden toplanıp toplanmadığına kadar değişik seviyelerde detayı talep etmektedir. Bütün durumlarda, bildiriminizin -diğerlerine göre- kısa, kolayca ulaşılabilir ve temiz, sade bir dille yazılmış olması gerekmektedir. Ayrıca hangi yasal dayanağın kullanıldığı ve veriyi işlemedeki meşru menfaatin ne olduğu da açıkça belirtilmelidir.

İlk aşamada mevcut durumda kullanılan kişisel gizlilik bildirimlerinin ne olduğuna bakılması ve nelerin değişmesi gerektiğinin belirlenmesi önemli bir aşama olabilir. Veri toplama ve kullanma işinde olan tüm işletmelerin yayıncılardan başlayarak tüm ilgili üçüncü partilere bu bilgiyi tebliğ etmeleri gerekmektedir. ICO'nun kişisel gizlilik bildirimleri, şeffaflık ve kontrol konularına yönelik kılavuzu iyi bir başlangıç noktası olabilir. Ayrıca 'bilgilendirilme hakkı' bölümü de ICO'nun GDPR yorumuna ilişkin incelenmesi gereken konuların başında gelmektedir.

## 7. Bireylerin hakları

GDPR bireylerin haklarını daha kapsamlı hale getirmektedir. Bu haklar:

- Bilgilendirilme hakkı (bkz. Madde 6)
- Erişim hakkı
- Düzeltme hakkı
- Silinme hakkı (unutulma hakkı)
- İşlem sınırlama hakkı
- Veri taşınabilirliği hakkı
- İtiraz hakkı (çıkış hakkı)
- Otomatikleştirilmiş karar vermeye özne olmama hakkı

Bireylerden gelebilecek herhangi bir talebe yeterli düzeyde karşılık verebilmek için bu işlemlerin kontrol edildiğinden emin olmalısınız. Eğer veriyi bulanıklaştırırsanız; birey kendisini tanımlayabilmeniz adına sizin için aktif olarak ek bir bilgi sağlamadığı sürece erişim, düzeltme, terkin, işlem sınırlama ve veri taşınabilirliği haklarını sağlamaktan feragat edebilirsiniz.

## 8. Veri kontrolörleri ve veri işleyicileri

GDPR mevcut veri koruma kanununda yer alan ve kişisel veriyi işlemek için gerekli olan farklı görev tanımlarını ayrıştıran 'veri kontrolörleri' ve 'veri işleyicileri' kavramlarını aynen korumaktadır. Veri kontrolleri -tek başına ya da diğer kontrolörlerle ortak olarak- verinin kim tarafından ve neden işlendiğini kontrol eden şirketleri, veri işleyenler ise veri kontrolörleri adına çalışan şirketleri tanımlamaktadır. Mevcut kurallar altında veriyi işleyen değil sadece kontrolör, veri koruma uyumluluğundan sorumludur.

GDPR, veri işleyenleri kapsayan yasal zorunlulukları genişletmektedir. Böylece Mayıs 2018'den sonra veri işleyenler de Veri Koruma Makamları tarafından uygulanabilecek yasal işlemlere ve yaptırımlara (global yıllık cironun %4'üne varan) tabi olabilecektir. GDPR altında veri işleyenleri ilgilendiren zorunluluklar şunlardır:

- Veri anlaşmaları – veri işleyenler ile kontrolörler arasında yazılı bir anlaşma (veya başka bir hukuki tasarruf) bulunması gerekmektedir. Bu anlaşma konuyu, işlemin süresini, amacını, kişisel verinin cinsini, kategorisini, kontrolörün zorunluluklarını ve haklarını belirtir.
- Veri güvenliği – veri işleyenler gerekli güvenlik önlemlerini almalı ve herhangi bir gecikmeye mahal vermeden kontrolörleri bilgilendirmelidir.
- Yan-işlemciler – veri işleyenler sadece kontrolörün yazılı onayıyla yan-işlemcileri kullanabilir. Tedarikçiler de yan-işlemcilerin kullanımındaki değişikliklerle ilgili olarak veri kontrolörüne itiraz hakkı fırsatı vermelidir.
- Kontrolör yönergeleri – veri işleyenler kişisel veriyi sadece kontrolör yönergelerine uygun olarak işleyebilir.
- Hesap verilebilirlik – veri işleyenler tüm veri işleme eylemlerinin kayıtlarını tutmalı ve bunları Veri Koruma Makamları'nın taleplerine uygun olarak muhafaza etmelidir.
- Veri Koruma Görevlileri – veri işleyenler belirli durumlarda bir veri koruma görevlisi atayabilir.
- Sınır ötesi transferler – veri işleyenler sınır ötesi transferler ile ilintili kısıtlamalara uyum göstermelidir.

Veri kontrolörlerinin ve veri işleyenlerin GDPR ile beraber bazı yükümlülüklere tabi olacağını göz önünde bulundurarak, her iki tarafın da rolleri iyi belirlenmelidir. Bir markanın kampanyası sırasında bile, bu roller değişiklik gösterebilir.

Hedef kitle segmentasyonunda kendi rolünüzü belirleme gibi durumlarda ICO (Information Commissioner's Office) kılavuzunu incelemeniz önerilir. Bunu tek başınıza mı, yoksa markalar veya yayıncılardan gelen yönergelerle mi yapıyorsunuz? Müşteriden müşteriye değişkenlik gösteriyor mu? Her koşulda, iş ortaklarınızla birlikte sözleşmeler oluşturulması ve mevcut sözleşmelerin GDPR'ın getireceği gereksinimlerle uyumlu olup olmadıkları denetlenmelidir.

## 9. Veri ihlalleri

Kişisel veri ihlallerinin itibar ya da finansal açıdan birçok sonucu olabilir. Bu nedenle veri ihlallerinin tespiti, raporlanması ve araştırılması için çeşitli süreçler organize edilmelidir. Mevcut kurallardan farklı olarak, GDPR veri kontrolörleri bireylerin kimlik hırsızlığı ya da gizlilik ihlali yaşadığı durumları Veri Koruma Makamları'na bildirmelidir.

Herhangi bir ihlal durumunda veri işleyenler, veri kontrolörlerini herhangi bir gecikmeye mahal vermeden bilgilendirmelidir. Bilgilendirme gerektiren durumların önceden belirlenmesi bu konuda yapılabilecek adımların ilki olabilir.

## 10. Tasarımdan İtibaren Veri Koruması (Privacy by Design) ve Kişisel Gizlilik Etki Değerlendirmesi (PIA)

Kişisel Gizlilik Etki Değerlendirmesi - ya da GDPR'ın getireceği tanımla Veri Koruma Etki Değerlendirmesi - yeni kurallar içinde önemli bir rol oynamaktadır. Yeni kanunla birlikte yüksek risk içeren durumlarda bu değerlendirmelerin yapılması yasal bir zorunluluk olacaktır. Örneğin, yeni bir teknolojinin kullanıldığı ya da profilleme operasyonunun bireyleri etkileyebileceği durumlarda bu değerlendirmeler hayati önem taşıyacaktır. Bu zorunluluğun bulanıklaştırılmış veriyi kapsayıp kapsamayacağı henüz netleşmiş değildir. Ayrıntılı bilgi için: Privacy Impact Assessments (PIAs)

GDPR ayrıca tasarımdan itibaren veri koruması, privacy by design - geliştirilen projelerin başından itibaren gizlilik ve veri korumasına uygun sistematik geliştirilmesi ve uygulanması- ilkelerini de düzenlemektedir. Her iki durumda da, pazara sunmak istediğiniz yeni ürünler veya hizmetler için kişisel gizlilik etki değerlendirmelerinin gerçekleştirilmesi yararlı olacaktır.

# GDPR Nedir?

## 11. Veri Koruma Görevlileri

GDPR veri kontrolörünün ya da işleyenin temel aktivitelerinin doğaları, kapsamları ve/veya amaçları gereği düzenli ve sistematik olarak izlenmesini gerektiren durumlarda' bir veri kontrol görevlisinin görevlendirilmesini şart koşmaktadır.

Eğer bu durum şirketiniz için geçerliyse, GDPR uyumluluğunuzdan sorumlu olacak bir görevli atamalısınız. Ayrıca bu kişinin iş yapısının ve yönetimin neresine uyacağını belirlemek de önemlidir.

## 12. Uluslararası

Sektörümüzde birçok işletme operasyonlarını Avrupa genelinde gerçekleştirmektedir. Bu gibi durumlarda hangi Veri Koruma Makamı'nın ana merciiniz olduğunu belirlemelisiniz.

Daha da önemlisi, AB dışındaki ülkelere veri transferi seçeneklerini de değerlendirmelisiniz. Kişisel veriyi işlemeseniz bile bunu GDPR'dan önce yapmalısınız. GDPR, sınırlar arası veri transferi için çeşitli seçenekler önermektedir. Avrupa Komisyonu, bazı ülkelere yapılacak transferler için yeterli veri koruma standartları sağlamaktadır. Bu ülkelerin listesine buradan ulaşabilirsiniz. Standart sözleşme koşulları gibi diğer seçenekler de bir yandan geçerliliklerini sürdürmektedir.