



# RIZA BEYANI

Çalışma Raporu 03/2017

---

IAB Avrupa  
GDPR (Genel Veri Koruma Yönetmeliği)  
Uygulama Çalışma Grubu



Sürüm 1.0

28 Kasım 2017

**iab**.europe

# IAB Avrupa Hakkında

IAB Avrupa, dijital iş dünyasının sesi ve interaktif reklamcılık ekosisteminin Avrupa seviyesindeki öncü sektör kuruluşudur. Misyonu, mevzuata tabi ortamı şekillendirmek, araştırma ve eğitime yatırım yapmak ve iş standartlarının benimsenmesini kolaylaştırmak suretiyle bu yenilikçi sektörün gelişimini teşvik etmektir.

## GDPR Uygulama Grubu Hakkında

IAB Avrupa GDPR Uygulama Grubu, Avrupa Birliği'nin yeni veri koruma yasası üzerine görüşmeler yapmak, en iyi uygulamaları paylaşmak ve sektörle ilgili kritik meselelerde ortak yorum ve sektör konumlandırmasına ilişkin mutabakat sağlamak üzere, dijital medya ve reklam dünyasının önde gelen uzmanlarını bir araya getirmektedir. GDPR Uygulama Grubu, tartışma ve düşünce liderliği konularında üye odaklı bir forumdur. Dijital reklam endüstrisinin GDPR'a uyum çabalarına yaptığı önemli katkı, ancak çok sayıda katılımcı üyesinin çalışmaları ve liderliği sayesinde mümkün olabilmektedir.

## Teşekkür

Verilerin Korunması Genel Yönetmeliği kapsamındaki rıza beyanı hakkındaki bu Çalışma Raporu, IAB Avrupa GDPR Uygulama Grubu üyeleri tarafından *MediaMath* öncülüğünde hazırlanmıştır.

## İletişim

**Matthias Matthiesen** ([matthiesen@iabeurope.eu](mailto:matthiesen@iabeurope.eu))

Kıdemli Müdür - Gizlilik ve Kamu Politikaları, IAB Avrupa

**Chris Hartsuiker** ([hartsuiker@iabeurope.eu](mailto:hartsuiker@iabeurope.eu))

Kamu Politikaları Görevlisi, IAB Avrupa

# İÇİNDEKİLER

Yönetici Özeti.....	4
Genel Bakış .....	5
Rıza Beyanı ile Kişisel Verilerin İşlenmesi .....	5
GDPR Kapsamında Rıza Beyanı .....	5
Rıza beyanı ne zaman gereklidir? .....	6
Rıza Talebi İçin Doğru Bilgilerin Açıklanması.....	7
Bir Hizmete Erişim Koşulu Olarak Rıza .....	8
Rızanın Ayrıntılılığı.....	9
Rıza Kapsamı.....	9
Uyumluluğun İspatı için Rıza Kaydı Yapılması .....	10
Rızayı Geri Çekme Hakkı .....	11
Birinci ve Üçüncü Tarafların Sorumlulukları .....	12
Onaylayıcı Rıza olarak Nitelendirilen İfadeler veya Hareketler.....	12
Uygulamada Geçerli Onaylayıcı Rıza Alınması .....	13
Eski Rıza: GDPR Öncesinde Toplanan Rızaların Geçerliliği.....	14
16 Yaş Altı Çocukların Rızası .....	14

# Yönetici Özeti

- Rıza beyanı, GDPR kapsamında kişisel verilerin işlenmesi için altı yasal dayanaktan biridir. Kişisel verilerin işlenmesini gerekçelendirmek için hangi yasal dayanağın kullanılacağına seçimi, bağlama özel bir analiz gerektirir. Önemli bir bağlamsal faktör de, diğer yasalardır. Örnek: Son kullanıcı cihazlarındaki bilgilerin saklanması veya bilgiye erişilmesi için rıza gerektiren e-Privacy Direktifi.
- Kullanıcıların, rıza verdiklerini belirtmek üzere onaylayıcı bir eylemde bulduklarını kanıtlamak için rıza beyanı almaya yönelik mevcut birçok yaklaşım yeterli değildir. Geçmişten farklı olarak, rızaya dayalı veri işlemeye, rıza onayı alınmadan başlanılmamalıdır.
- Rıza alınırken veri işleme amacı, işlenecek veri türleri, sorumlu veri kontrolörleri gibi ayrıntıları içeren doğru bilginin veri sahibine bildirilmesi önemlidir. Bu, çok sayıda bilgi anlamına geleceğinden, önce ana bilginin sağlandığı ve daha ayrıntılı bilgi için bir bağlantının sunulduğu katmanlı bir yaklaşımdan yararlanmanızı öneririz.
- Birinci taraflar, kullanıcılara bilgi sunma ve rıza beyanı alma konusunda en iyi konumdadır ve bu nedenle de çoğunlukla gerekli açıklamaları yapmak ve rıza almak konusunda sorumluluk üstlenirler. Üçüncü taraflar da rızanın kendi adlarına geçerli olacak şekilde alınmasını konusunda sorumludur.
- Veri sahiplerinin rızasına bağlı olarak özel şirketlerin, hizmetlerine erişim yapılmasına izin verilmektedir. GDPR, rızanın serbestçe verilip verilmediğini tespit ederek hesaba alınmasını gerektirir, ancak uygulamayı yasaklamaz. Ayrıca, ePrivacy Direktifi, hizmetlerin benzer şekilde rızaya bağlı olarak verilebileceğini açıklamaktadır.
- Uygun durumlarda, veri sahibinin verilerin işlenmesine rıza verdiği amaçlar ayrıntılı olmalıdır. Birinci taraflar, tüm amaçlar için toplu halde ya da tek bir amaç için rıza talep etmeye karar verebilir. Bir amacın diğerine bağlı olduğu durumlarda bu amaçlara yönelik onayın birlikte alındığından emin olunmalıdır.
- Rıza, bir hizmete özel veya “toplu” olabilir; ikincisi, aynı kontrolör için, farklı web siteleri ve hizmetler arasında rızanın geçerli olduğu bir duruma atıfta bulunur. Talep edilen rızanın kapsamını belirlemek birinci taraflara düşer. Rıza, üçüncü taraf ortakları adına birinci taraflarca alınabilir.
- Kontrolörler rıza kayıtlarını tutmalıdır. IAB Avrupa, dijital reklam tedarik zinciri aracılığıyla ilgili bilgileri ileten otomatik bir mekanizmanın benimsenmesini önermektedir.
- Rıza, verildiği kadar kolay geri çekilebilmelidir, ancak geri çekilmeden önce gerçekleşen işleme yasaldır. Bu verilerin işlenmesi için alternatif bir yasal zemin olmadıkça, rıza alınmadan önce toplanan veriler, rızanın geri çekilmesinden sonra işlenemez.
- IAB Avrupa'nın GDPR Uygulama Grubu, birinci ve üçüncü taraflar arasında bilgi alışverişini kolaylaştıracak, açıklamaların yapılmasına yardımcı olabilecek, rıza verilmiş kayıtlar oluşturabilecek ve bu bilgileri dijital reklam tedarik zinciri boyunca aktarabilecek bir teknik standart geliştirmektedir.

# Genel Bakış

27 Nisan 2016'da Avrupa Birliği, Genel Veri Koruma Yönetmeliğini ("GDPR")<sup>1</sup> kabul etmiştir. GDPR, 25 Mayıs 2018'de Avrupa Birliği ("AB") ve Avrupa Ekonomik Alanı'nda ("AEA") yürürlüğe girmiş ve halihazırda yürürlükte olan ulusal veri koruma yasalarının yerine geçmiştir.

GDPR, genel olarak tanımlanmış ya da tanımlanabilir gerçek bir kişiyle ilgili herhangi bir bilgi olarak tarif edilen kişisel verilerin işlenmesini düzenlemekte, gerçek kişiyi ayırt etmek için kullanılacak online ve cihaz tanımlayıcılarını içermektedir.<sup>2</sup> Kişisel veri işlemenin yasal olması için, işlem için altı kanuni dayanaktan en az biri tarafından gerekçelendirilmelidir. Bu belge, IAB Avrupa GDPR Uygulama Grubu üyeleri tarafından, bir veri sahibinin rızasına dayalı olarak kişisel verileri işlemek isteyen ya da yasalarca işlemesi gereken şirketlere rehberlik sağlamak amacıyla hazırlanmıştır.

## Rıza Beyanı ile Kişisel Verilerin İşlenmesi

### GDPR Kapsamında Rıza Beyanı

GDPR kapsamında rıza beyanı, mevcut Avrupa Veri Koruma Direktifi kapsamındaki rızadan çok daha güçlü bir kavramdır. Avrupa Veri Koruma Direktifi'nden farklı olarak GDPR, rızaya ilişkin gerekliliklerin açıklanmasında çok açıktır ve eski yasaya dayalı belli rıza yorum ve uygulamalarını net bir şekilde sona erdirmektedir. Bu, en başta, bir kullanıcının herhangi bir aksiyon almaması nedeniyle bir talebe rıza verdiği düşünülen "zımni rıza" kavramları için geçerlidir, çünkü GDPR kapsamında rıza onaylayıcı bir eylem gerektirir.

Rıza, GDPR Madde 4 (11)'de şu şekilde tanımlanır:

"'rıza', veri sahibinin bir beyan yoluyla ya da açık bir onaylayıcı eylemle, kendisine ait kişisel verilerin işlenmesine dair mutabakatını özgür iradesiyle vermiş olduğunu, spesifik, bilgilendirici ve belirsizliğe mahal vermeyecek şekilde belirtmesi anlamına gelir."<sup>3</sup>

Yukarıda tanımlanan (basit) rızaya ek olarak, GDPR ikinci bir onay türü de sunar: açık rıza. Açık rıza, GDPR'de tanımlanmamıştır, ancak genel olarak, veri sahibinin rızasını daha açık bir onaylayıcı eylem veya ifadeyle belirtmesi gerekliliği gibi, daha katı şartlar içeren daha yüksek bir standart olarak yorumlanır. Rızanın söz konusu olduğu durumlarda, GDPR genellikle basit rızayı gerektirmekte ve açık rıza uygulaması daha sınırlı kalmaktadır.

<sup>1</sup> Gerçek kişilerin kişisel verilerinin işlenmesi ve bu verinin serbestçe taşınması sırasında korunması hakkında Avrupa Parlamentosu ve Konseyi'nin 24 Nisan 2016 tarihli 2016/679 sayılı regülasyonu <http://eur-lex.europa.eu/eli/reg/2016/679/oj/>

<sup>2</sup> <https://www.iabeurope.eu/policy/gig-workingpaper-on-the-definition-of-personal-data/> adresinde bulunan kişisel verilerin tanımı ile ilgili IAB Avrupa belgesine bakınız.

<sup>3</sup> GDPR Madde 4(11)

## Rıza beyanı ne zaman gereklidir?

Kişisel verileri işlemek isteyen kuruluşlar, AB hukukuna göre işleme sürecini gerekçelendirmelidir. GDPR, bunun için altı yasal dayanak sunmaktadır ve en az biri uygulanmalıdır.<sup>4</sup> Veri sahibinin, kendisi ile ilgili kişisel verilerin işlenmesine yönelik rızası, bu tarz bir yasal dayanaktır. Özellikle, tüm yasal dayanaklar eşittir ve hiçbir yasal dayanak diğerinden daha yüksek bir statüye sahip değildir. Bir şirketin, kişisel verilerin işlenmesi için en uygun yasal dayanak konusundaki tercihi, GDPR ve diğer yasalarda bulunan tüm ilgili kurallar dikkate alındığında, içerik özelinde bir değerlendirmeye tabi olmalıdır.

GDPR veri sahibinin açık rızası gibi, Madde 9 (2) 'de yer alan daha katı şartlar yerine getirilmediği sürece işlenemeyen belli özel kişisel veri kategorilerini ayırt etmektedir. Ayrıca, kişisel veriler, AB sınırları dışında, yeterli düzeyde koruma sağlamadığı kabul edilen ya da yalnızca, yasal veya benzeri önemli etkiler üreten, otomatik işlemlere dayalı kararlar<sup>5</sup> gibi konularda daha sıkı şartlara tabidir. Özel kategorilerdeki kişisel verileri işlemek isteyen veya belirli bir düzenlemeye tabi işleme faaliyetlerine katılan şirketler, daha sıkı işleme şartlarına uyduklarından emin olmalıdır.

Ayrıca, diğer yasalar, hangi yasal dayanağın en uygun veya gerekli olduğuna dair kararı etkileyebilir. Özellikle, e-Privacy Direktifinin “çerez hükmü” maddesinde aşağıdaki ifade bulunmaktadır:

“[...] Bir abonenin veya kullanıcının terminal cihazında bilginin depolanmasına ya da halihazırda depolanmış bilgiye erişimin sağlanmasına, [GDPR]'yle<sup>6</sup> uyumlu olacak şekilde diğerlerine ilaveten, işlemenin amaçları hakkında açıkça ve kapsamlı bir şekilde bilgilendirilen abonenin ya da kullanıcının rıza vermesi koşuluyla izin verilir.”

GDPR'nin ePrivacy Direktifi ile bağlantısı hakkındaki GDPR 95. Madde, ePrivacy Direktifi'nde bulunan daha spesifik kuralların GDPR'nin kuralları üzerinde hakim olduğunu ortaya koymaktadır. Bu nedenle, bilgileri (örneğin çerezlerde) depolayan veya bilgiye erişen şirketler (örneğin, AAID, IDFA gibi cihaz tanımlayıcıları ya da parmak izi teknikleriyle üretilen istatistiksel tanımlayıcılar gibi), veri işleme için uygun yasal dayanak seçerken, ePrivacy Direktifini uygulayan ilgili ulusal yasaları dikkate almalıdır<sup>7</sup>. Şirketler ayrıca, Mayıs 2018'den sonraki bir tarihte mevcut ePrivacy Direktifi kurallarının yerine geçmesi ve değiştirilmesi beklenen ePrivacy Tüzüğü için süregelen görüşmeleri de takip etmelidir. Genellikle bir direktifin (ePrivacy Direktifi gibi) şirketler için yasal zorunluluklar oluşturmadan önce üye

<sup>4</sup> Bkz. Madde 6 GDPR: GDPR şu şartlarda işleme izin verir (a) veri sahibi rıza verdiği; (b) bir sözleşmenin ifası veya bir sözleşme yapılması için gerekli olması durumunda; (c) yasal bir zorunluluğa uymak için gerektiğinde; (d) veri sahibinin veya başka bir gerçek kişinin hayatı çıkarlarını korumak için gerektiğinde; (e) kamu çıkarlarını ilgilendiren bir görev için gerektiğinde; (f) işlemenin, kontrolörün veya üçüncü bir tarafın takip ettiği meşru menfaatler (söz konusu menfaatlerin veri sahibinin çıkarlarına ve temel haklarına zarar vermeyecek şekilde) gerektirdiğinde.

<sup>5</sup> Avrupa Birliği dışına veri transferi için başka yöntemlerin de mevcut olduğunu unutmayın. Örneğin, Avrupa Komisyonu tarafından belirlenen “AB dışına veri transferleri”ne bakınız:

[http://ec.europa.eu/justice/data-protection/internationaltransfers/index\\_en.htm](http://ec.europa.eu/justice/data-protection/internationaltransfers/index_en.htm).

<sup>6</sup> ePrivacy Direktifi, Veri Koruma Direktifi Madde 94 (2)'de bulunan rıza tanımına dayanmaktadır. GDPR, Veri Koruma Direktifi'ne yapılan tüm atıfların “[GDPR] için referans olarak yorumlanacağını” şart koşar. Sonuç olarak, ePrivacy Direktifi'nde bulunan rıza şartı, GDPR'de de geçerli olacaktır.

<sup>7</sup> Ulusal “çerez” kurallarına genel bakış için, <http://www.iabeurope.eu/eucookie laws> adresinde bulunan IAB Avrupa ePrivacy Direktifi Uygulama Merkezi'ne bakınız.

devletler tarafından ulusal hukuka aktarılması söz konusuysen, bir yönetmelik (GDPR ve önerilen ePrivacy Tüzüğü gibi) üye devletlerin ulusal hukuka aktarmasına gerek olmadan doğrudan AB'nin tamamında uygulanabilir.

## Rıza Talebi İçin Doğru Bilgilerin Açıklanması

GDPR, veri sahibinin, en azından kontrolörün kimliği ve kişisel verilerin işleneceği amaçlar hakkında bilgilendirilmesi gerekliliğini şart koşar.<sup>8</sup> Dahası, rıza açıkça anlaşılabilir olmalı ve açık bir şekilde, işlemin kapsamı ve sonuçlarına atıfta bulunmalıdır. 29. Maddeye göre, “bu, uygulamada, veri sahibi tarafından verilen rızanın, bir eylemin gerçeklerinin ve çağrıştırdıklarının tamamen farkında olarak anlaşılmasına dayanması gerektiği anlamına gelir. İlgili kişiye, ilgili tüm konuların açık ve anlaşılabilir bir şekilde, doğru ve eksiksiz olarak sunulması gerekir”.<sup>9</sup>

Bu nedenle, rıza talepleri ve bilgilerin geçerli olabilmesi için, (1) hükümler ve koşullar gibi diğer bilgilerden belirgin ve ayrı olarak verilmelidir;<sup>10</sup> (2) anlaşılması kolay sade bir dilde sunulmalıdır;<sup>11</sup> (3) işlenen kişisel verilerin doğasını (ör. Rastgele tanımlayıcılar, tarama verileri) açıklamalıdır;<sup>12</sup> (4) işlemin amacını veya nedenini açıklamalıdır;<sup>13</sup> (5) işlemin (varsa) sonuçlarını açıklamalıdır;<sup>14</sup> (6) kişisel verileri işlemek için rızayı dikkate alacak olan kontrolörü veya çeşitli kontrolörleri ismiyle listelemelidir;<sup>15</sup> (7) kullanıcılara onaylarını geri çekme hakları bulunduğunu aktarmalı ve bunun nasıl yapılacağına ilişkin bilgi vermelidir;<sup>16</sup> ve (8) kullanıcılar, işleme gerçekleştirilmediğinde karşılaşacakları sonuçlar hakkında bilgilendirmelidir, örneğin kısıtlı kullanıcı deneyimi veya bir siteyi veya hizmeti kullanma engeli.<sup>17</sup>

GDPR, bu rıza taleplerinde, verileri bir kontrolör adına işleyecek işlemcilerin isimlerinin listelenmesini gerektirmez. İşlemci bunu, kontrolöre verilen rıza bazında yapabilir.

GDPR'nin gerektirdiği ve aynı anda tüm ayrıntıları vermeyi imkansız kılan veya pratik olmayan kapsamlı bilgi açıklamaları şartı için IAB Avrupa, söz konusu tüm bilgilerin açıklanması için “katmanlı bir yaklaşım”ın kullanılmasını tavsiye etmektedir. İngiltere'nin veri koruma yetkili kurumu ICO'ya göre, katmanlı yaklaşımlar dijital içerik bağlamı gibi online bir ortamda “çok iyi” çalışmaktadır.

“Katmanlı yaklaşım, temel gizlilik bilgisini anında sağlamanıza ve isteyenler için başka bir yerde daha ayrıntılı bilgileri buldurmanıza imkan verdiği için yararlı

<sup>8</sup> Madde 7(2) GDPR; Mütalaa 42 GDPR.

<sup>9</sup> Aynı yerde.

<sup>10</sup> Madde 7(2) GDPR; Mütalaa 42 GDPR.

<sup>11</sup> Madde 7(2) GDPR; Mütalaa 42 GDPR.

<sup>12</sup> Madde 29 rıza tanımına ilişkin Çalışma Grubu Görüşü 187, s. 19,

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf) adresinden erişilebilir.

<sup>13</sup> Mütalaa 42 GDPR.

<sup>14</sup> Madde 29 rıza tanımına ilişkin Çalışma Grubu Görüşü 187, s. 19,

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf) adresinden erişilebilir.

<sup>15</sup> Mütalaa 42 GDPR.

<sup>16</sup> Madde 7(3) GDPR.

<sup>17</sup> Madde 29 rıza tanımına ilişkin Çalışma Grubu Görüşü 187, s. 19,

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf) adresinden erişilebilir.

olabilir. Bu, daha fazla ayrıntı sunmak için yeterince yer olmadığı veya özellikle karmaşık bir bilgi sistemini kişilere açıklamanız gerektiğinde kullanılır."

Genellikle, kuruluşun kimliği ve kişisel bilgileri nasıl kullanacağınız gibi önemli bilgileri içeren kısa bir bildirimden oluşur. Her bir bölümü tam sürümüne genişleten bağlantılar veya daha ayrıntılı bilgi sağlayan daha uzun ikinci bir bildirim giden tek bir bağlantı içerebilir. Bu da, bilginin polise ifşa edilebileceği durumlar gibi belirli konuları açıklayan başka materyallere bağlantılar içerebilir."<sup>18</sup>

Aşağıdaki "Uygulamada Geçerli Onaylayıcı Rıza Alınması" başlıklı bölümde pratik öneriler sunulmaktadır.

## Bir Hizmete Erişim Koşulu Olarak Rıza

GDPR rızanın özgür iradeyle verilir vermediğini belirlerken, diğerlerinin yanı sıra, bir hizmet sunulurken, hizmetin sunulması için gerekli olmayan işlemlere rıza gösterilmesi konusunda "azami dikkat"<sup>19</sup> şart koşar. Gerekçe 43 bu şartı şu şekilde açıklar: "Eğer bir hizmetin sunulması da dahil olmak üzere bir sözleşmenin performansı, böyle bir performans için gerekli görülmediği halde rızaya bağlı ise, rıza özgür iradeyle verilmemiş olarak kabul edilir."

Önemli bir konu da GDPR'nin, bağlama özel değerlendirme gerektirmesine rağmen, rızaya bağlı bir hizmete erişim yasağı koymamasıdır.

ePrivacy Direktifi, "web sitesi içeriğine erişimin, çerezlerin detaylı bilgilendirme içeren kabulü şartıyla yapılmasına"<sup>20</sup> ve benzer izleme teknolojilerinin kullanılmasına açıklık getirmektedir. Sonuç olarak, web siteleri veya uygulamalar gibi dijital hizmetlerin, bir hizmeti sunmadan önce kullanıcılardan çerezler ya da benzer teknolojilerle kişisel bilgilerinin toplanmasına rıza vermelerini talep etmeleri genellikle mümkündür.

29. Madde Çalışma Grubu, şirketlerin erişimi rıza şartlı yapmamalarını tavsiye etmekte, özel mülkiyete ait hizmetlere erişimin çerezlerin kabulü şartıyla yapılabileceğini ve İsveç'te olduğu gibi, belirli üye devletlerde kanunun bu imkanı açıkça sağladığını kabul etmektedir.<sup>21</sup> Bununla birlikte, kurallar kamuya ait hizmetler konusunda daha sınırlayıcı olabilmektedir.<sup>22</sup> Hollanda Ticaret Kurumu, "çerezlerin kullanımını kabul etmek istemeyen kullanıcıları reddeden çözümlere sahip olmanın yasadışı olmadığını"<sup>23</sup> ve "çerezlerin reddedilmesinin, kullanıcının tek seçeneğinin siteden ayrılmak olduğu anlamına gelebileceğini"<sup>24</sup> düşünmektedir. Yine,

---

<sup>18</sup>Gizlilikle ilgili bildirimler, şeffaflık ve gizlilik bilgilerinin bireylere nerede sunulması gerektiği konuları hakkında Bilgi Komisyonu'nun uygulama pratiğine bakınız. <https://ico.org.uk/for-organisations/guide-to-dataprotection/privacy-notice-transparency-and-control/where-should-you-deliver-privacy-information-to-individuals/> (erişim 20/11/2017, 12:10 CET)

<sup>19</sup> Madde 7 (4) GDPR

<sup>20</sup> Mütalaa 25 ePD

<sup>21</sup> Madde 29 Çalışma Grubu Çalışma Belgesi 02/2013, çerezler için rıza alma konusunda rehberlik sağlar, s. 5, bilgiye [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2013/wp208\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2013/wp208_en.pdf) adresinden erişebilirsiniz

<sup>22</sup> Aynı yerde., s. 6.

<sup>23</sup> Erhvervsstyrelsen, Son Kullanıcı Terminal Ekipmanlarında Bilginin Saklanması ve Bilgilere Erişilmesi Durumunda Gerekli Bilgi ve Rıza için Kararname Kılavuzu ("Çerez Hükümü"), s. 20, <https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf> adresinden erişebilirsiniz.

<sup>24</sup> Aynı yerde.



düzenleyiciler, kamu tarafından finanse edilen hizmetlere farklı kuralların uygulanabileceği görüşünü kabul etmiştir. ePrivacy Direktifi'ni uygulayan Hollanda Tüketici ve Piyasalar Kurumu, çerezleri kabul etmeyenlere web sitelerine erişim verilmesinin gerekmediğini ve bu nedenle çerezlere rıza verildikten sonra şartlı erişim izni verilebileceğini belirtmektedir. Düzenleyici ayrıca, web sitesi sahiplerinin, rıza şartlı erişime izin vermeyi seçmelerini sağlayacak başka çıkarılara sahip olabileceklerini göz önüne almaktadır. Buna, bir kullanıcının bir hizmete erişim için “ödeme yapması” şeklindeki hedefe yönelik reklamlar alması da dahildir.<sup>25</sup>

IAB Avrupa'nın bu konudaki görüşü, birlikte okunduğunda GDPR ve ePrivacy Direktifi'nin özel işletmelerin veri işlemeye rıza vermeyen kullanıcılara erişimi engellemelerine açıkça izin verildiği şeklindedir. Yayıncılar, kendilerine ait iş modellerine hangi rıza talebi yöntemlerinin en uygun olduğuna karar vermekte serbesttir. Bunlara hizmetlerine erişimin bu rızaya bağlı olup olmadığı ve/veya kullanıcı deneyimlerinin kullanıcının seçimlerine bağlı olarak değişip değişmeyeceği de dahildir.

## Rızanın Ayrıntılılığı

Rıza almak için yapılan bilgilendirmede, verilerin işleme amaçları tam olarak açıklanmalıdır.<sup>26</sup> İlâveten, rızanın özgür iradeyle verilmiş olması için, bir vakada bu tür bir ayrıntı “uygun”sa veri sahibi, farklı kişisel veri işleme işlemlerine ayrı olarak rıza verebilmelidir.<sup>27</sup> Bu, uygun durumlarda, bir kontrolör veri sahibine bu amaçların sadece bir altkütmesi konusunda mutabık kalma ihtimalini sunmadan, bir dizi amaç için bütün olarak onay isteyebilir ve alabilir anlamına gelmektedir. Diğer durumlarda, bir kontrolörün, bir kullanıcının farklı amaçlara ayrı ayrı rıza verebilmesini sağlayarak, daha ayrıntılı seçimler yapmasına imkan tanıması uygun olabilir. Yayıncılar, hizmetlerinin ve kontrollerinin nasıl yürüdüğüne ilişkin uzmanlıklarına dayanarak, ayrıntıların uygunluğu, bir hizmete erişmek için hangi koşulların uygun olduğu veya belirli bir kullanıcı deneyimi için hangi dayanakların kullanılması gerektiği konularını sonuçta kendileri belirler. Bir amacın başka bir amaca bağlı olduğu durumlarda, ikincisine de rıza göstermeden, ilkinde rıza gösterilmesi mümkün olmamalıdır. Örneğin, ilgi alanına dayalı reklamcılık, bir reklamın etkinliğini ölçmek için analitiğe dayanabilir. Bu nedenle, ilgi alanına dayalı reklamcılığa rıza veren bir kullanıcı, analitiğe de rıza vermelidir, çünkü ilki ikincisine dayalıdır.

## Rıza Kapsamı

Rızayı, birinci taraf kendisi ve ortakları (ve ortaklarının ortakları) adına “hizmete özel” veya “toplu” bazda alabilir. “Hizmete özel” rıza, belirli bir kontrolör için tek bir site veya hizmetle

---

<sup>25</sup> Autoriteit Consument en Markt (ACM), Hollanda cookie yasaı hakkında sık sorulan sorular Ekim 2016, s. 12, [https://www.acm.nl/sites/default/files/old\\_publication/publicaties/11917\\_veelgestelde-vragencookiebepaling-oktober-2016-engels-new.pdf](https://www.acm.nl/sites/default/files/old_publication/publicaties/11917_veelgestelde-vragencookiebepaling-oktober-2016-engels-new.pdf) adresinde bulunabilir.

<sup>26</sup> Mütalaa 42 GDPR.

<sup>27</sup> Mütalaa 43 GDPR.

sınırlı bir rıza durumunu tanımlar; oysa “toplu” rıza, belirli bir kontrolör için, bu rızanın nerede kullanılacağı konusunda sınırlama olmayan bir rıza durumunu tanımlar.

Madde 29 Çalışma Grubu, daha iyi bir kullanıcı deneyimi sunma bazında, toplu rıza ilkesini kabul etmiştir. Onlara göre, özellikle ortalama bir kullanıcı rızasını internette dolaşarak ifade ettiğinden, rıza taleplerinin sayısı zamanla azalacaktır, çünkü:

“[...] Bir web sitesindeki bir üçüncü taraf reklam ağı bir ODR çerezi için rıza aldığı anda, bu izin yalnızca aynı web sitesinin diğer sayfaları için değil, aynı ODR ağını paylaşan diğer web siteleri için de geçerli olacaktır.”<sup>28</sup>

Şirketler, rıza alınan veri toplama ve işleme alanlarının kapsamını belirleyen farklı bir tüzel kişi yoluyla (yani birinci taraf), ne tür bir rıza aldıklarını, yani genel mi yoksa hizmete özel mi olduğunu bilmek ister. Bu amaçla, birinci tarafların kendileri adına aldıkları rızaya dayanan üçüncü taraflar, amacı (ör. “ilgi alanına dayalı reklamcılık”) ve bunun yanı sıra kapsamı (ör. “küresel”) içeren teknik mekanizmalar da dahil olmak üzere, sözleşme maddelerini ve / veya diğer mekanizmaları dikkate almalıdır.

GDPR, rıza geçerliliği için bir zaman sınırı içermemektedir. Buna göre rıza, kişisel verilerin işlenmesinin amacını yerine getirmesi veya veri sahibinin rızasını geri çekmesi için gerekli olduğu sürece geçerli olur. Her durumda, geçerlilik süresine dair karar, işlemenin doğası ve süresi gibi tüm ilgili faktörler göz önünde bulundurularak bağlam özelinde bir değerlendirme ile desteklenmelidir. 29. Madde Çalışma Grubu, iyi uygulama konusu olarak, rızanın uygun aralıklarla gözden geçirilmesini ve yenilenmesini önermektedir. Ayrıca, rızaların ne sıklıkta yenilenmesi gerektiğini belirlemeye ilişkin başka yasalar, yönetmelikler veya kurallar da bulunabilir. Örneğin, Fransız veri koruma kurumu, izleme tanımlama bilgilerinin yalnızca 13 ay süreyle saklanabileceğini kabul etmektedir. Bu durum kontrolörlerin bir cihazda çerezleri saklamak veya onlara erişmek için en az 13 ayda bir kullanıcının rızasını almasını gerektirir.<sup>29</sup> Dolayısıyla şirketler, rızanın ne sıklıkla yenileneceğini belirlerken ilgili tüm faktörleri göz önünde bulundurmalıdır. Bununla birlikte kontrolör, kullanıcının önceden rıza vermiş olduğunu doğrulayamazsa, geçerli bir rıza olmadan işlem yapmamak için bir kullanıcıdan daha erken onay alabilir.

## Uyumluluğun İspatı için Rıza Kaydı Yapılması

GDPR, kontrolörlerin “veri sahibinin kendi kişisel verilerini işlemeye razı olduğunu ispatlayabilmelerini” gerektirmektedir.<sup>30</sup> Bu tüm kontrolörlerin (birinci taraflar ve üçüncü taraflar) rıza mekanizmasında kullanılan dil, ne zaman ve nasıl rıza verildiği de dahil olmak üzere, bireyin neye rıza verdiğinin kayıtlarını tutması gerektiği anlamına gelmektedir.

<sup>28</sup>[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp188\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp188_en.pdf) adresinde bulunan Online Davranışsal Reklamcılığa İlişkin EASA / IAB En İyi Uygulama Önerisi ile ilgili 16/2011 sayılı Madde 29 Çalışma Grubu Görüşü.

<sup>29</sup> CNIL, Cookies & traceurs: que dit la loi? (Çerezler & izleyiciler: Kanun ne diyor?), Fransızca olarak şu adreste mevcuttur, <https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi/> (erişim tarihi 15/09/2017, 10:50 CEST)

<sup>30</sup> Madde 7 (1) GDPR.

Bir kontrolörün başka bir kuruluş tarafından elde edilen rıza bazında veri işlediği durumlarda, kontrolör, bu yükümlülüğe uymak için rızanın alınmış olduğunu ispatlayan bir kayıt almalı ve saklamalıdır. Bu sebeple, tüm tarafların belgelenmiş bir denetim takibi yapılabilmesi için kullanıcı rızasının birinci taraftan ilgili tüm üçüncü taraflara yayılması esastır. IAB Avrupa, dijital reklam tedarik zincirine ilgili bilgileri ileten otomatik bir mekanizmanın benimsenmesini önerir.

Bu kayıtlar minimumda şunları içermelidir:

- Kullanıcının rıza verdiği tarih ve saat
- Kullanıcının rıza verdiği URL
- Kullanıcının rızasını belirtmek için yaptığı eylem
- Kullanıcının rıza verdiği amaçlar
- Kullanıcının rıza verdiği kontrolör veya kontrolörler
- Rıza vermeden önce kullanıcıya sunulan bilgiler
- Kontrolörün her bir rızayı ilgili kullanıcıya bağlaması için bir tanımlayıcı

## Rızayı Geri Çekme Hakkı

Veri sahiplerinin her zaman rızalarını geri çekme hakları vardır, ki bu da öncelikle rıza vermek kadar kolay olmalıdır.<sup>31</sup> Bir veri sahibi rızasını geri çektiğinde, bunun öncesinde rızası temelinde gerçekleşen işlemin yasalılığı etkilenmez.<sup>32</sup> Ancak, daha önce toplanan veya gelecekte toplanacak olan verilerin yasal olarak işlenmesi için alternatif bir yasal dayanak gerekir.

Ayrıca, kullanıcının belirli bir veri işleme faaliyeti için rızasını geri çektiği ve işlemin devam ettirilmesi için başka yasal dayanağın bulunmadığı hallerde, kullanıcı, kendisiyle ilgili kişisel verilerin silinmesini (veya anonimleştirilmesini) talep etme hakkına sahiptir.<sup>33</sup>

Bir kontrolör verinin silinmesi için böyle bir talep aldığı anda, verilerin (1) ifade özgürlüğü hakkını kullanmak için; (2) yasal zorunluluğa uyum için; (3) halk sağlığı konusunda kamu yararı için; (4) kamu yararı, bilimsel veya tarihsel araştırmalar ve istatistiksel amaçlar için; veya (5) yasal taleplerin oluşturulması, uygulanması veya savunulması için gerekli olması durumları dışında, talebi "gereksiz gecikme olmadan" yerine getirmelidir.<sup>34</sup>

Son olarak, verileri diğer kontrolörlere açıklayan kontrolörlerin, kullanıcının silme talebini diğer kontrolörlere iletme için "makul adımlar" atmaları gerekir.<sup>35</sup>

---

<sup>31</sup> Madde 17(3) GDPR

<sup>32</sup> Madde 17(3) GDPR

<sup>33</sup> Madde 17(1)(b) GDPR.

<sup>34</sup> Madde 17(3) GDPR

<sup>35</sup> Madde 19 GDPR.

## Birinci ve Üçüncü Tarafların Sorumlulukları<sup>36</sup>

Birinci taraflar, (ve genellikle dijital reklam tedarik zincirindeki kuruluşlar) kullanıcılara bilgi sağlamak ve rızalarını alabilmek için en iyi konumdadır. Birinci taraflar, bir kullanıcının siteye, uygulamaya ya da başka bir hizmete erişmesi sonucunda ortaya çıkan veri işleme durumu hakkında gerekli açıklamaları yapmalı, hem sorumlu oldukları veri işleme hem de üçüncü taraflarca gerçekleştirilen veri işleme için kullanıcı rızası talep etmelidir.

Ancak, üçüncü tarafların açıklama yapamadığı ve rıza alamadığı durumlarda, birinci parti tarafından yapılan bilgilendirmenin ve alınan rızanın yasal olarak geçerliliği yoksa üçüncü parti yasaya uyum sağlamamış kabul edilir.<sup>37</sup> Dolayısıyla dijital reklamcılık ekosisteminin, her bir şirketin GDPR kapsamında uygun açıklamaları yapma ve geçerli rıza alma yükümlülüklerini yerine getirmesi için işbirliği yapması son derece önemlidir.

## Onaylayıcı Rıza Olarak Nitelendirilen İfadeler veya Hareketler

29. Madde Çalışma Grubu, "Prensip olarak, rızanın formuna dair herhangi bir sınırlama yoktur, bu bir işaret de olabilir"<sup>38</sup> demektedir. GDPR Mütalaa 32 "açık onaylayıcı eylem" ile kastedilene ve kastedilmeyeni şöyle izah etmektedir:

"Bu, bir internet sitesini ziyaret ederken bir kutuyu işaretlemeyi, bilgi toplumu hizmetleri için teknik ayarları seçmeyi veya bu bağlamda, veri sahibinin kendi kişisel verilerinin önerilen amaçla işlenmesini kabul ettiğini açıkça belirten başka bir ifade veya hareketi içerebilir. Bu nedenle sessizlik, önceden işaretlenmiş kutular veya hareketsizlik rıza olarak kabul edilmemelidir."<sup>39</sup>

ePrivacy Direktifi'nin uygulanması sonucunda, dijital reklam ve analitik amacıyla çerezler üzerinden kişisel verilerin toplanması için rıza alınması konusunda, birçok AB Üyesi devlette, sayfanın en üstünde veya altında rıza talebi içeren açıklamaları içeren "rıza banner'i" fikrine odaklanılmıştır.

Rıza banner'ları, bilgi verilmesi ve GDPR kapsamında geçerli bir rıza alınması için hala yararlı bir araç olsa da, zımni rıza olarak adlandırılan mevcut pek çok uygulama, kullanıcının izin vermeyi reddetme olasılığını kullanmadığı gerçeğinden ötürü değişiklik gerektirecektir.

---

<sup>36</sup> 29. Madde Çalışma Grubu'na göre, üçüncü bir taraf, herhangi bir zamanda "kullanıcı tarafından erişilen [hizmeti] sunandan farklı bir veri kontrolörü"dür. Öte yandan, birinci taraf, kullanıcının eriştiği hizmeti sunan bir veri kontrolördür. Bu sınıflandırma, birinci ve üçüncü tarafların tamamen teknik sınıflandırmasından farklı olabilir.

Bkz. Madde 29 Çalışma Grubu Çerez Rızası İstisnası Görüşü, s. 4-5, [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2012/wp194\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2012/wp194_en.pdf) adresinden erişilebilir.

<sup>37</sup> Fransız veri koruma kurumu, yayıncıların üçüncü taraf çerezlerinden tek başına sorumlu tutulamayacağı sonucuna varmıştır, çünkü bunlar işlemeden sorumlu olan farklı bir şirketten kaynaklanmaktadır ve bunun sonucunda veri koruma yasasına uyumlu olmaları gerekmektedir. Bkz. CNIL, Çerezler: la CNIL etend ses controles au-dela des editeurs de sites (Çerezler: CNIL, denetimlerini site operatörlerinin ötesine taşır), <https://www.cnil.fr/fr/cookies-la-cnil-etendses-controles-au-dela-des-editeurs-de-sites/> (erişim 15/09/2017, 10:50 CEST).

<sup>38</sup> Madde 29 Çalışma Grubu Rıza Tanımına İlişkin Görüşü 187, s. 11,

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf) adresinde mevcuttur.

<sup>39</sup> Mütalaa 32 GDPR.

Veri Koruma Direktifi'nde olanın aksine, GDPR'da, herhangi bir kişisel verinin işlenmesinin, rıza olarak kabul edilen eylemden önce başlamaması gerektiği açıktır.

Çerezler yoluyla veri toplamada olduğu gibi kullanıcı rızası ile işlemenin, onaylayıcı eylemden önce başlamaması gerektiğinden, birinci taraflar rıza talebi için intersistial / tam ekran / consent wall görüntülemeyi tercih edebilir. Bu, kullanıcıların kullanım öncesinde hizmetin gerektirdiği işleme faaliyetlerini okudukları ve rıza verdikleri bilgisini garanti eder. Örneğin, bir "consent wall" yoluyla uygun bildirimler yapıldıktan sonra, bir hizmetin kullanımına devam edilmesiyle rıza alınsa da, açık bir şekilde saptanan pozitif bir hareketin tespit edilmesinden önce hiçbir veri toplama ve işlemenin gerçekleştirilmemesi önemlidir.

"Kullanıcıların çerezlere ilişkin rızalarını bildirebildikleri süreç, bu eylemin neyi temsil ettiği konusunda tam olarak bilgilendirilmeleri şartıyla, onaylayıcı hareket veya diğer aktif davranışlar yoluyla gerçekleşecektir. Bu nedenle kullanıcılar, bir tuşu veya bağlantıyı tıklayarak ya da bilginin sunulduğu alanın içinde veya yakınında bir kutuyu işaretleyerek (hareket çerezlerin kullanımı hakkında sağlanan bilgilerle birlikte gerçekleşirse) veya web sitesi operatörünün, spesifik ve bilgilendirilmiş rıza olduğu sonucuna kesin olarak varabileceği diğer herhangi bir aktif davranış ile rızalarını gösterebilir."<sup>40</sup>

Madde 29 Çalışma Grubu, "aktif davranışı", "web sitesine yönelik izlenebilir bir kullanıcı talebine dayanan" bir kullanıcı eylemi olarak tanımlar.<sup>41</sup> Grup ayrıca, "kullanıcı hareketi çerezlerin kullanımına ilişkin verilen bilgiyle birlikte ele alındığında, makul olarak kullanıcı isteğinin göstergesi şeklinde yorumlanabileceğini" düşünmektedir.<sup>42</sup> Fransız veri koruma kurumu, buna "ziyaret edilen web sayfasını kaydırarak ifade edilebilir" ifadesini de eklemektedir.<sup>43</sup>

## Uygulamada Geçerli Onaylayıcı Rıza Alınması

IAB Avrupa GDPR Uygulama Grubu, birinci ve üçüncü taraflar arasında bilgi alışverişini kolaylaştırmak için bir teknik standart geliştirmektedir. Bu teknik standart (1) birinci tarafların, üçüncü taraflarla toplama ve işleme amaçlarını dinamik olarak göstermelerini sağlar; (2) birinci tarafların, rıza seçeneklerini güncelleyebilecek ve rızalarını istedikleri zaman geri çekebilecek olan kullanıcılardan "global" veya "hizmete özel" rıza almasını sağlar; (3) üçüncü tarafların, bir kullanıcının rıza tercihleri hakkında birinci taraflardan bilgi almasını sağlar; (4) bir rıza kaydı ve denetim takibi oluşturulmasını sağlar.<sup>44</sup>

<sup>40</sup> Çerez rızası elde etmek için kılavuz niteliğindeki 2/2013 tarihli 29. Madde Çalışma Grubu Raporu s.4

<sup>41</sup> Aynı yerde

<sup>42</sup> Aynı yerde

<sup>43</sup> CNIL, Cookies: la CNIL etend ses controles au-dela des editeurs de sites (Çerezler: CNIL, denetimlerini site operatörlerinin ötesine taşıyor) <https://www.cnil.fr/fr/cookies-la-cnil-etend-ses-controles-au-dela-des-editeurs-de-sites> adresinden erişilebilir. (erişim 15/09/2017, 10:50 CEST).

<sup>44</sup> Daha fazla bilgi için [www.advertisingconsent.eu](http://www.advertisingconsent.eu) adresini ziyaret edin.

## Eski Rıza: GDPR Öncesinde Toplanan Rızaların Geçerliliği

Eski rıza, yani GDPR'nin uygulanmasından önce alınmış olan rıza, GDPR'ye uygun bir şekilde alınmış olması şartıyla geçerli olmaya devam eder.<sup>45</sup> Ancak eski rızaların, GDPR'de belirtilen yüksek standardı karşılamaması durumunda, GDPR'nin uygulamaya geçmesiyle devam eden işleme süreci için geçerliliğini yitirecektir. Bu gibi durumlarda, kontrolörün işlem için alternatif bir yasal dayanak bulması, GDPR'ye uygun olarak yeni bir rıza alması veya söz konusu işleme faaliyetini durdurması gerekir. Reklam ekosistemindeki çoğu şirketin, GDPR'nin kuralları doğrultusunda yeni rızalar alması gerekecektir.

## 16 Yaş Altı Çocukların Rızası

Bir internet hizmetinin doğrudan bir çocuğa sunulması durumunda, sadece çocuğun en az 16 yaşında olması durumunda, bu rıza yasal bir dayanak olacaktır; çocuğun daha küçük olduğu hallerde, ebeveyn rızası gereklidir. Üye devletler, 13 yaşın altında olmaması koşuluyla, bu eşiği düşürecek şekilde yasal düzenleme yapabilir. Ebeveyn onayının gerekli olduğu durumlarda, kontrolörler de bu rızayı doğrulamak için makul adımlar atmalıdır.

---

<sup>45</sup> Mütalaa 171 GDPR.

# IAB Avrupa GDPR Uygulama Çalışma Grubu Hakkında

---

IAB Avrupa GDPR Uygulama Grubu, Avrupa Birliği'nin yeni veri koruma yasası üzerine görüşmeler yapmak, en iyi uygulamaları paylaşmak ve sektörle ilgili kritik meselelerde ortak yorum ve sektör konumlandırmasına ilişkin mutabakat sağlamak üzere dijital reklam sektörünün önde gelen uzmanlarını bir araya getirir.

GDPR Uygulama Grubu, tartışma ve fikir liderliği konularında çalışan üye odaklı bir forumdur. Dijital reklam endüstrisinin GDPR'a uyum çabalarına yaptığı önemli katkı, ancak çok sayıda katılımcı üyesinin çalışmaları ve liderliği sayesinde mümkün olabilmektedir.

Daha fazla bilgi için:

**Matthias Matthiesen** ([matthiesen@iabeurope.eu](mailto:matthiesen@iabeurope.eu))

Kıdemli Müdür - Gizlilik ve Kamu Politikaları

IAB Avrupa

**Chris Hartsuiker** ([hartsuiker@iabeurope.eu](mailto:hartsuiker@iabeurope.eu))

Kamu Politikaları Görevlisi

IAB Avrupa

