

Dünyada Neler Oluyor?



Veri Koruma alanı ülkemizde ivme kazanan bir hızla gelişirken, dünya çapındaki yenilikler Kişisel Verileri Koruma Kurumu'nun ("Kurum") radarında kalmaya devam ediyor.



Daha önce defaten karşılaştığımız örneklerden Kurum'un Avrupa Veri Koruma Tüzüğü (General Data Protection Regulation, "GDPR") düzenlemeleri başta olmak üzere dünya gündemine ayak uydurduğuna ve hızlı hareket eden veri gizliliği dünyasının gereklerini yakalamaya çalıştığına şahit oluyoruz.

Dünya gündemini GRC LEGAL olarak yakından takip ediyor ve güncelden seçkileri bu içeriğimizle bilgilerinize sunuyoruz.

Aşağıda yer alan haberler 2023 Ocak ayına aittir.

The Data Act: “Veri Yasası”

Günümüzün dijital çağında veriyi yeni para birimi olarak nitelendirmek yanlış olmayacaktır. Avrupa Birliği (“AB”) de bunu dikkate alarak, bağlı cihazlar tarafından üretilen verilerin paylaşılma ve kullanılma biçiminde devrim yaratacak bir dizi yeni kural içeren The Data Act’i (“Veri Yasası”) yürürlüğe koydu.



Tüketiciler ve işletmeler cihazlarının verilerine erişebilecek, bunları satış sonrası ve katma değerli hizmetler için kullanabilecekler. Ticari ve endüstriyel oyuncular daha fazla veriye sahip olacak ve rekabetçi bir veri pazarından faydalanacaklar. Satış sonrası hizmet sağlayıcıları daha kişiselleştirilmiş hizmetler sunabilecek -ve üreticiler tarafından sunulan benzer hizmetlerle eşit düzeyde rekabet edebilecek- endüstriyel veriler de tamamen yeni dijital hizmetler geliştirmek için birleştirilebilecek. Yeni düzenleme, akıllı ev aletlerinden akıllı endüstriyel makinelere kadar uzanan bağlantılı cihaz kullanıcılarının, bu cihazların kullanımıyla elde edilen ve genellikle yalnızca üreticiler ve hizmet sağlayıcılar tarafından toplanan verilere erişim sağlamasına olanak tanıyacak.



Veri Yasası: Veri Yasası, sektörler ve paydaşlar arasında veri paylaşımını ve yeniden kullanımını kolaylaştırarak adil ve rekabetçi bir veri pazarı oluşturmayı amaçlayan yeni bir AB yasasıdır.

Veri paylaşımına ilişkin yükümlülükler: Veri Yasası, bağlı cihaz üreticilerine ve ilgili hizmet sağlayıcılarına, belirli koşullar ve istisnalar altında verileri kullanıcılar ve üçüncü taraflar için erişilebilir hale getirme yükümlülüğü getirmektedir.

Adil olmayan sözleşme şartları: Veri Yasası, tek taraflı olarak dayatılan ve iyi ticari uygulamalardan büyük ölçüde sapan sözleşme şartlarını yasaklamakta ve bu tür şartlara örnekler vermektedir.

Verilerin kamu sektörü kurumlarının kullanımına sunulması: Veri Yasası, verilerin belirli bir kamu yararı görevi için kullanılmasına yönelik istisnai bir ihtiyaç olması halinde, verilerin kamu sektörü kurumlarına ücretsiz olarak sunulmasına yönelik çerçeveyi belirlemektedir.

Bulut ve uç hizmetler arasında geçiş: Veri Yasası, müşterilerin farklı veri işleme sağlayıcıları arasında gereksiz gecikme veya maliyet olmadan geçiş yapmalarına, verilerini ve dijital varlıklarını başka bir sağlayıcıya veya kendi altyapılarına taşımalarına olanak tanıyan yeni kurallar içermektedir.

Kişisel olmayan verilerin uluslararası aktarımı: Veri Yasası, Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation, "GDPR") ve Schrems II kararı kapsamındaki uluslararası veri aktarımlarına ilişkin yükümlülükleri veri işleme hizmetleri sağlayıcılarına genişletmekte ve üçüncü devletler tarafından uyumsuz veya yasa dışı erişimi önlemek için uygun koruma önlemlerini uygulamalarını gerektirmektedir.



G
D
P
R

Herhangi bir veri paylaşım talebine uyabilmek için şirketler, bağlı cihazlarından herhangi bir veriyi (bu verileri tanımlayabilmek için gerekli meta veriler dahil) hızlı, güvenli, kapsamlı ve yapılandırılmış bir şekilde çıkarmak için uygun mekanizmalara ve politikalara sahip olduklarından emin olmalıdır. Şirketler ayrıca sözleşmelerini gözden geçirerek Veri Yasası uyarınca haksız sayılabilecek herhangi bir şart bulunmadığından emin olmalıdır.

RESMÎ GAZETE

VERİ YASASI

Veri Yasası, 22 Aralık 2023 tarihinde Resmî Gazete'de yayımlanmasının ardından 11 Ocak 2024 tarihinde yürürlüğe girdi. Bazı kurallar daha sonra yürürlüğe girecek olsa da 12 Eylül 2025'ten itibaren kurallarının çoğu uygulanmaya başlayacak ve bir sonraki sayfada yer alan tabloda belirtilen paydaşlar için geçerli olacaktır.

PAYDAŞLAR	AÇIKLAMA
Üreticiler ve sağlayıcılar	Kuruluş yerlerine bakılmaksızın, AB'de piyasaya sürülen bağlantılı ürünlerin üreticileri ve 'ilgili hizmetlerin' sağlayıcıları.
Kullanıcılar	Bağlı ürünlerin veya ilgili hizmetlerin AB'deki kullanıcıları.
Veri Sahipleri	Kuruluş yerlerine bakılmaksızın, AB'deki alıcılara veri sağlayan ilgili kişiler.
Veri alıcıları	Verilerin kullanıma sunulduğu AB'deki veri alıcıları.
Kamu sektörü kuruluşları	Kamu sektörü organları, Avrupa Komisyonu, Avrupa Merkez Bankası ve kamu yararına yürütülen belirli bir görevin yerine getirilmesi için bu verilere istisnai olarak ihtiyaç duyulması halinde veri sahiplerinden veri sunmalarını talep eden AB organları ve bu talebe cevaben bu verileri sağlayan veri sahipleri.
Bulut ve uç sağlayıcılar	Kuruluş yerlerine bakılmaksızın, AB'deki müşterilere bu tür hizmetler sağlayan veri işleme hizmetleri sağlayıcıları.
Diğer Paydaşlar	Veri alanlarındaki katılımcılar ve akıllı sözleşmeler kullanan uygulamaların satıcıları ve ticareti, işi veya mesleği bir anlaşmanın yürütülmesi bağlamında başkaları için akıllı sözleşmelerin konuşlandırılmasını içeren kişiler.

Veri Paylaşımı

**SATIN
AL**

Eski Sürümü Tut

Veri Yasası, veri sahiplerinin, örneğin kullanıcıya tarafsız olmayan bir şekilde seçenekler sunarak veya bir kullanıcı dijital arayüzünün yapısı, tasarımı, işlevi veya çalışma şekli yoluyla kullanıcının özerkliğini, karar verme veya seçim yapma iradesini olumsuz etkileyerek, kullanıcının verileriyle ilgili tercihlerini kullanmasını gereksiz yere zorlaştırmaması gerektiğini belirtmektedir.

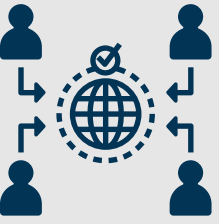
Veri Yasası, bir kullanıcının talebi üzerine veri alan üçüncü taraflara belirli yükümlülükler getirmektedir:

1. Alınan verileri yalnızca kullanıcı ile mutabık kalınan amaçlar için kullanmak ve bu amaçların ortadan kalkması, gerekli olmaması halinde verileri silmek.

2. Verilerin, Dijital Piyasalar Yasası (“Digital Markets Act”) uyarınca ‘geçit bekçisi’ olarak kabul edilen bir kuruluşa sunulmaması.
3. Verileri, bağlı ürünün veya ilgili hizmetlerin güvenliği üzerinde olumsuz bir etkisi olacak şekilde kullanmamak.
4. Tüketici olan kullanıcının, verileri diğer tarafların kullanımına sunmasını engellemek.

Dijital Piyasalar Yasası kapsamında geçit bekçisi olarak belirlenen büyük çevrimiçi platformlar uygun üçüncü taraflar değildir.

Mikro ve küçük ölçekli şirketler veri paylaşımı yükümlülüklerinin dışında tutulmuştur. Aynı durum, bir yıldan daha kısa bir süredir orta ölçekli işletme olarak nitelendirilen bir işletme tarafından üretilen bağlantılı ürünlerin veya sağlanan ilgili hizmetlerin kullanımı yoluyla üretilen veriler ve orta ölçekli bir işletme tarafından piyasaya sürüldükleri tarihten sonraki bir yıl boyunca bağlantılı ürünler için de geçerlidir.



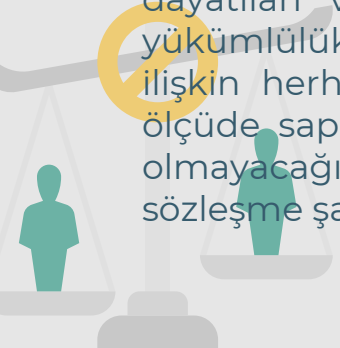
Veri paylaşımı kavramı, Veri Yasası'nın temel bir parçasını oluştururken, kullanıcıların ve veri sahiplerinin verilere erişimi, verilerin kullanımını veya verilerin paylaşımını kısıtlayabileceği veya yasaklayabileceği sınırlı durumlar vardır. Bu sınırlı durumlar, işletmeye bağlı ürünün güvenlik gereksinimlerini zayıflatabileceği ve gerçek kişilerin sağlığı, güvenliği veya emniyeti üzerinde ciddi bir olumsuz etkiye yol açabileceği durumları içerir.

AB Hukuku Uyarınca Verileri Erişime Açması Gereken Veri Sahiplerine Yönelik Yükümlülükler

İşletmeler arası ilişkilerde belirli durumlarda, ilgili kişiler veri alıcısı ile verilerin kullanıma sunulmasına ilişkin düzenlemeler üzerinde anlaşmaya varacak ve bunu adil, makul ve ayrımcı olmayan şartlar altında ve şeffaf bir şekilde yapacaktır. Ayrıca, bir veri sahibinin karşılaştırılabilir kategorilerdeki veri alıcıları arasında verilerin kullanıma sunulmasına ilişkin düzenlemeler bakımından ayrımcılık yapmaması gerektiği belirtilmektedir. Bir veri alıcısının, verilerin kendisine sunulduğu koşulların ayrımcı olduğunu düşünmesi halinde, veri sahibi, ayrımcılık yapılmadığını göstermek için veri alıcısına bilgi sağlayacaktır.

Adil Olmayan Sözleşme Şartları

Veri Yasası, mikro, küçük veya orta ölçekli bir kuruluşa tek taraflı olarak dayatılan verilere erişim ve verilerin kullanımına veya verilerle ilgili yükümlülüklerin ihlali veya feshine ilişkin sorumluluk ve çözüm yollarına ilişkin herhangi bir sözleşme şartının, iyi ticari uygulamalardan büyük ölçüde sapması ve bu nedenle haksız kabul edilmesi halinde bağlayıcı olmayacağını belirtmekte ve otomatik olarak haksız kabul edilecek sözleşme şartlarına örnekler vermektedir.



Örneğin, sözleşmeden doğan yükümlülüklerin yerine getirilmemesi durumunda çözüm yollarının uygunsuz bir şekilde sınırlandırılması, haksız sözleşme şartı olarak kabul edilerek geçersiz olacaktır.

Veri İşleme Hizmetleri Arasında Geçiş Yapma



Veri Yasası, müşterilerin farklı bulut ve uç hizmet sağlayıcıları arasında etkili bir şekilde geçiş yapmasına olanak tanıyan yeni kurallar içermektedir. Amaç, müşterileri engelleyen ticaret öncesi, ticari, teknik, sözleşmeye dayalı veya organizasyonel tüm engelleri ortadan kaldırmaktır. Bu kapsamda örnek vermek gerekirse, müşterinin aynı hizmet türünü kapsayan farklı bir veri işleme hizmeti sağlayıcısı ile yeni sözleşmeler akdetmesini engelleyen düzenlemeler bu kapsamda kabul edilecektir.

Veri Yasası, bir müşterinin başka bir hizmet sağlayıcıya geçmesine veya tüm ihraç edilebilir verilerin ve dijital varlıkların gereksiz gecikme olmaksızın -ve her durumda en fazla iki aylık bir bildirim süresinin sona ermesinden sonraki 30 gün içinde- geçiş sırasında tam destek ve hizmet sürekliliği ile taşınmasına izin vermesi gereken sözleşme gerekliliklerini sağlayarak bu sorunların üstesinden gelmeyi amaçlamaktadır.

Sözleşmeye dayalı tedbirlerine ek olarak Veri Yasası, veri işleme hizmetleri sağlayıcılarına getirilen bilgilendirme yükümlülüklerinin yanı sıra, başka bir hizmet sağlayıcısına geçişle ilgili ücretlerin kademeli olarak azaltılmasına yönelik bir çerçeve ortaya koymakta ve Veri Yasası'nın yürürlüğe girmesinden üç yıl sonra, sözde çıkış hizmetinin müşteriye ücretsiz olarak sunulmasını sağlamaktadır.

Kişisel Olmayan Verilerin Uluslararası Aktarımı

GDPR ile benzer bir rejimi benimseyen Veri Yasası, GDPR ve Avrupa Birliği Adalet Divanı'nın Schrems II kararı kapsamındaki uluslararası veri transferlerine ilişkin yükümlülükleri, endüstriyel verilerin uluslararası transferlerini veya AB veya ulusal mevzuatla uyumlu olmayan üçüncü bir devletin erişimini önlemek için uygun önlemleri uygulaması gereken veri işleme hizmetleri sağlayıcılarına genişletecektir.



Birlikte Çalışabilirlik



Veri Yasası, sektörler arasında yeniden kullanılacak endüstriyel veriler için birlikte çalışabilirlik standartlarının geliştirilmesini sağlamakta, endüstriyel verilerin, veri paylaşım mekanizmalarının ve hizmetlerinin birlikte çalışabilirliğini kolaylaştırmak için temel gerekliliklerin yanı sıra veri paylaşımına yönelik akıllı sözleşmelere ilişkin temel gereklilikleri tanımlamakta ve ortaya koymaktadır.

Ayrıca, erişim hakları ve rıza veya iznin teknik tercümesi gibi konularda veri paylaşımını teşvik eden taraflar arasındaki kuralları ve düzenlemeleri uygulayan mimari modeller ve teknik standartlar gibi açık birlikte çalışabilirlik spesifikasyonlarını ve sorunsuz birçok satıcılı bulut ortamını teşvik etmek için bulut hizmet sağlayıcılarının birlikte çalışabilirliğine yönelik Avrupa standartlarını düzenler.

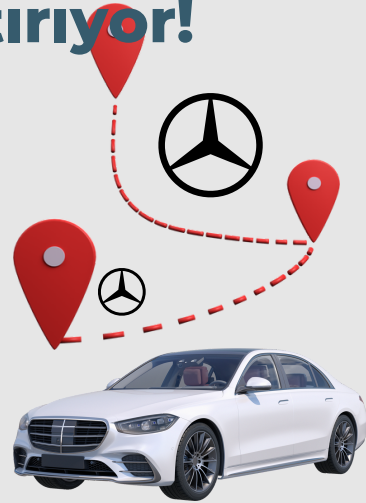
GRC LEGAL Yorumu

“Dünyada Neler Oluyor” serimizin on dördüncü sayısında da belirttiğimiz üzere; Veri Yasası, Avrupa Birliği'nde veri yönetimi konusunda önemli değişikliklere yol açarak bu alanda bir standardizasyon sağlamayı amaçlamaktadır. Bu kapsamda Yasa, kullanıcıların verilerine erişme hakkını; verilerin kolay, güvenli, kapsamlı ve yapılandırılmış bir şekilde sunulmasını sağlayarak ve kullanıcıların verilerini üçüncü taraflarla paylaşma hakkını, verilerin yalnızca kullanıcının izniyle paylaşılabilmesini sağlayarak güçlendirmektedir.

Ek olarak Veri Yasası; veri alıcılarının veri işleme faaliyetlerini düzenli olarak gözden geçirmesini ve gerekli önlemleri almasını da zorunlu kılmaktadır. Bu noktada, veri alıcılarının, verilerin güvenliğini ve gizliliğini korumak için gerekli adımları atması beklenmektedir. Veri Yasası'nın aşamalı olarak uygulamaya alınacağı ve adaptasyon süreci göz önüne alındığında, etkilerini tam olarak değerlendirmek şu aşamada mümkün olmasa da ilgili kişilerin verileri üzerindeki kontrolü güçlendireceği, veri işleme faaliyetlerinin şeffaflığını ve hesap verebilirliğini artırmaya yardımcı olacağı söylenebilecektir.

Araç Konum Verileri Aile İçi İstismar Mağdurları İçin Takip Riskini Artırıyor!

The New York Times'a göre, gizlilik savunucuları, modern araçların "tekerlekli akıllı telefonlar" haline geldiği ve aile içi şiddet mağdurlarını daha fazla riske attığı konusunda endişeli. Bunun nedeni, çok sayıda kişisel veriyi bilinmeyen kuruluşlara aktaran kameraların, ağırlık sensörlerinin ve akıllı telefona bağlı cihazların sayısı. Örneğin, boşanma davası devam eden bir kadının kocası tarafından "Mercedes Me" uygulaması kullanılarak izlendiğini ve kocasının başlangıçta araç kredisini ve ruhsatını aldığı için uygulamaya erişiminin Mercedes tarafından engellenemeyeceği bildirildi.



GRC LEGAL Yorumu

Mozilla'nın 2023 yılında gerçekleştirdiği "Privacy Not Included" projesindeki bulgulara göre büyük otomobil markalarının internete bağlı yeni modellerinde en temel gizlilik ve güvenlik standartlarına dahi uyulmadığı ve Mozilla'nın incelemiş olduğu 25 markanın yapılan testten geçemediği görülmüştü.

Teknoloji devi markaların sürücülerin ırk, yüz ifadeleri, kilo, sağlık bilgileri ve nerede araç kullandığı gibi verilere ek olarak test edilen araçlardan bazılarının cinsel aktivite, ırk ve göçmenlik durumuyla ilgili detaylar da dahil olmak üzere, araçların bilmesini beklemediğiniz verileri topladığı belirtilmişti.

Modern arabalarda mikrofonlar, kameralar ve sürücülerin arabalara bağladığı telefonlar da dahil olmak üzere çeşitli veri toplama araçlarını kullanan üreticilerin, aynı zamanda uygulamaları ve internet siteleri aracılığıyla da veri topladığı biliniyor. Yukarıdaki haberde de belirtildiği üzere söz konusu uygulamaların boşanma sürecinde olan bir çiftin sürecine dahi sirayet ettiği görülüyor. Bu anlamda bu markaların gizlilik süreçlerini büyük bir hassasiyet ve şeffaflıkla yürütmeleri önem arz ediyor. Fakat yine Mozilla'ya göre, birçok otomobil markasının “privacy washing” yöntemine başvurduğu ya da tüketicilere, tam tersi doğru olduğu halde gizlilik sorunları hakkında endişelenmelerine gerek olmadığını öne süren bilgiler sunduğu tespit edildi. Bu anlamda, içerisinde kendimizi evimizde gibi hissettiğimiz arabalarımızın içerisinde dahi mahremiyetimizin ihlal edildiğini söylemek oldukça mümkün.

Bilgi
Köşesi

'Privacy washing', aldatıcı reklam uygulamaları tiplerinden en kötüsü olabilir. Basit haliyle, bir şirketin veri gizliliği kurulumunu gerçekte takip etmeden şirket bünyesinde gizlilik nosyonunun çok yüksek olduğunu gösterme çabalarını ifade ediyor. Ürün ve/veya hizmetlerine 'gizlilik kılıfı' giydiren şirketler, yine de müşterilerin hassas/mahrem verilerini topluyor, paylaşıyor ve satıyor.

Google Chrome x Veri Takip Çerezleri

Google, şirketlerin kullanıcıları çevrimiçi ortamda izleyebilmelerine yönelik değişiklikleri test etmeye başladı. Chrome tarayıcısındaki yeni özellik, analitik verileri toplamak, çevrimiçi reklamları kişiselleştirmek ve gezinmeyi izlemek için cihazınızda depolanan küçük dosyalar olan üçüncü taraf çerezlerini devre dışı bırakacak. Başlangıçta bu özellik, küresel kullanıcıların % 1'i olan yaklaşık 30 milyon kişiye sunulacak.



Google, değişiklikleri bir test olarak tanımlıyor ve bu yılın ilerleyen dönemlerinde çerezleri ortadan kaldırmak için kapsamlı bir sürüm planlıyor. Ancak, bazı reklamcılar bunun sonucunda zarar göreceklarini söylüyor.

Çerezler; sitede yaptıklarınız, bulunduğunuz konum, kullandığınız cihaz ve daha sonra çevrimiçi olduğunuz yerler dahil olmak üzere kullanıcılar hakkında çeşitli verileri kaydetmek için kullanılabilir. Dünyanın en popüler internet tarayıcısı olan Chrome'dan çok daha az internet trafiğine sahip olan Safari ve Mozilla Firefox gibi rakipleri, bu verileri toplayan üçüncü taraf çerezlerini engelleme seçeneklerini halihazırda içeriyor.

Google, rastgele seçilen kullanıcılarına "tarayıcıda daha fazla gizlilikle gezinmek" isteyip istemediklerinin sorulacağını söylüyor. Google Başkan Yardımcısı Anthony Chavez "Chrome'daki üçüncü taraf çerezlerini aşamalı olarak kaldırmak için sorumlu bir yaklaşım izliyoruz. Bir site üçüncü taraf çerezleri olmadan çalışmazsa ve Chrome sorun yaşadığınızı fark ederse, bu internet sitesi için üçüncü taraf çerezlerini geçici olarak yeniden etkinleştirme seçeneği sunacağız." dedi.



Google, interneti daha özel hale getirmek için çalıştığını söylüyor ancak birçok internet sitesi açısından çerezler, bağlı oldukları reklamları satmanın hayati bir parçası. Bir internet sitesini ziyaret etmenin veya bir satın alma gerçekleştirmenin ardından ziyaret edilen tüm sitelerde ilgili reklamların görünmesi deneyimini yaşayan kullanıcılar göz önünde bulundurulduğunda, bu tür reklamların rahatsız edici bir boyutunun da bulunduğunu söylemek zor olmayacaktır.

GRC LEGAL Yorumu

Birçok türü bulunan çerezler, bir internet sayfası ziyaret edildiğinde kullanıcılara ilişkin bazı bilgilerin kullanıcıların cihazlarında depolanmasına izin veren düşük boyutlu zengin metin biçimli text formatları olarak tanımlanmakla birlikte reklam ve pazarlama çerezleri internet ortamında kullanıcıların çevrimiçi hareketlerinin takip edilmesiyle ilgi alanlarına yönelik reklam gösterilmesi için kullanılıyor.

Google'ın sunacağı yeni özellik ile de reklam ve pazarlama çerezlerinin devre dışı bırakılması hedefleniyor. Dünya genelinde en çok kullanılan tarayıcıya sahip Google'ın bu özelliği devreye sokması ile özellikle küresel boyutta yaygın olarak bu çerezlerden menfaat elde eden ve reklam/pazarlama faaliyetleri nedeniyle gündemden düşmeyen Meta, X gibi platformların olumsuz etkilenmesi mümkün olsa da atılan bu adım ile kullanıcıların/ilgili kişilerin sadece internet sitesine girmiş olması ile hedefli reklamcılığa maruz kalmaları engellenebilecektir.

ICO x İşletmeler

Bir siber güvenlik ve veri koruma danışmanı tarafından yapılan analize göre, 2023 yılında Bilgi Komiserliği Ofisi (Information Commissioner's Office, "ICO"), 18 işletmeye verileri kötüye kullanmaları nedeniyle 14,3 milyon pounddan fazla para cezası verdi. ICO ayrıca 36 şirkete kınama cezası verdi, 19 şirkete karşı icra emri gönderdi ve dört işletmeye bilgi hakları yükümlülüklerini yerine getirmediği için dava açtı.





Sosyal medya platformu TikTok, çocukların kişisel verilerinin hukuka uygun olarak kullanılmaması da dahil olmak üzere veri koruma yasasını ihlal ettiği için 12,7 milyon pound ile en yüksek para cezasına çarptırıldı. ICO'nun tahminine göre, Birleşik Krallık'ta 2020'de video paylaşma uygulamasını kullanabilen 1,4 milyon 13 yaş altı çocuk bulunmaktaydı.

Üç pazarlama firmasına, işletmelere toplamda 483,051 istenmeyen pazarlama araması yapmaktan ve iş arayanlara 107 milyon spam e-posta göndermekten toplamda **310 bin pound** para cezası verildi; iki enerji firmasına, Birleşik Krallık'ın 'aramayın' kaydındaki kişi ve işletmeleri yasadışı pazarlama aramalarıyla bombardımana tuttukları için toplam **250 bin pound** para cezası verildi; bir iş destek danışmanlığına, geçerli izin olmadan 558.354 doğrudan pazarlama SMS mesajı gönderdiği için **30 bin pound** para cezası verildi; ve bir cihaz servis ve onarım şirketine, 1.7 milyondan fazla istenmeyen doğrudan pazarlama araması yaptığı için **200 bin pound** para cezası verildi.



CSS Assure tarafından yapılan araştırmaya göre, yılın son altı ayında 10 şirket toplam 4.698.841 istenmeyen kısa mesaj, 39.906.342 e-posta gönderdikleri ve 1.937.028 rahatsız edici telefon görüşmesi yaptıkları için 800 bin pounddan fazla para cezasına çarptırıldı.

CSS Assure Teknoloji Bilgi Güvenliği Direktörü Charlotte Riley şunları söyledi:

"ICO tarafından 2023 yılında uygulanan para cezaları, verilerin kötüye kullanılmasının ciddi sonuçlarının altını çiziyor. Kişisel verilerin yanlış kullanımı yalnızca veri koruma yasalarını ihlal etmekle kalmıyor, aynı zamanda tüketiciler arasındaki güveni de sarsıyor.

TikTok'un 12,7 milyon poundluk cezası, kişisel verilerin hukuka uygun olarak kullanılmasının ve özellikle çocuklar söz konusu olduğunda uygun önlemlerin uygulanmasının önemini vurguluyor. TikTok büyük, tanınmış bir marka ve içerdiği veri miktarı nedeniyle cezası oldukça yüksekti. Ancak çok daha küçük KOBİ'ler de yaptırımlara maruz kaldı ve idari para cezalarına çarptırıldı.

İstenmeyen aramalar, kısa mesajlar ve spam e-postalar ile 'aramayın' kaydını dikkate almayan firmalara verilen cezalar, istilacı pazarlama uygulamalarının önemli etkisini göstermektedir. Bu cezalar, şirketlerin bireylerin gizlilik tercihlerine saygı göstermeleri ve onları istenmeyen iletişim bombardımanına tutmaktan kaçınmaları gerektiği yönünde açık bir mesaj göndermektedir."

Veri koruma yasalarına uyum amacıyla ICO'nun şirketleri idari para cezası yaptırımına tabi tutmaktan imtina etmediğini görmekteyiz. Küresel çapta kötü bir şöhrete sahip olan TikTok'a verilen ceza ile çocuklar gibi hassas ilgili kişi grupları nezdinde daha sıkı önlemlerin gerekliliği vurgulanırken; diğer şirketlerin tabi tutulduğu cezalar ile günümüzde tüm kullanıcıların öznesi olduğu istenmeyen pazarlama aramaları, spam e-postalar ve diğer istenmeyen iletişim biçimleriyle mücadele etme amacı güdüyor.

Cezaların büyüklüğü göz önünde bulundurulduğunda, küçük ve orta ölçekli işletmelerin bireylerin gizlilik haklarına saygı göstermeleri ve veri koruma standartlarına uymaları konusunda uyarı niteliğinde olduğu değerlendirilebilir.

Microsoft, Gizlilik Endişelerini Gidermek İçin Bulut Kullanıcılarının Kişisel Verilerini Avrupa'da Tutmasına İzin Veriyor



Microsoft Ocak ayında yaptığı açıklamada bulut bilişim hizmetini güncellediğini; müşterilerin tüm kişisel verilerinin ulusal gizlilik yasalarının bulunmadığı ABD'ye aktarılması yerine Avrupa Birliği içinde depolanmasına olanak tanıdığını duyurdu.

Bulut bilişim şirketleri, sıkı veri koruma yasalarına sahip Avrupa Birliği'nde artan gereklilikler nedeniyle veri depolama ve işleme süreçlerini yerelleştirmeye yöneliyor.

Eski Ulusal Güvenlik Ajansı çalışanı Edward Snowden'ın, Amerikan hükümetinin insanların çevrimiçi verilerini ve iletişimlerini dinlediğini ifşa etmesinin ardından Brüksel ve Washington, teknoloji şirketlerinin ABD'de depoladığı AB vatandaşlarının verilerinin güvenliği konusunda yıllarca tartışmıştı.

Microsoft, "AB Veri Sınırı çözümünün Avrupa uyumluluk gereksinimlerinin ötesine geçtiğini" söyledi. Şirket daha önce de müşterilerinin verilerinin AB dışına taşınmayacağı sözünü vermişti. Microsoft, geçtiğimiz yıl Avrupa içinde bazı verileri depolamaya ve işlemeye başlamışken şimdi bu kapsamı, çevrimiçi hizmetler çalıştırıldığında otomatik olarak oluşturulan, otomatik sistem günlüklerinde bulunan takma ad verilmiş (psödonomize edilmiş) veriler de dahil olmak üzere tüm kişisel verilere genişletiyor. Bu yılın sonuna doğru Microsoft, teknik destek verilerinin Avrupa'da tutulmasını sağlamaya başlayacak.

Psödonimizasyon, Türk mevzuatında tanımlanmamış olup kişisel bilgilerin gizliliğini korumak amacıyla kullanılan bir veri işleme yöntemidir. Bu yöntemde, kişisel verilerin doğrudan tanımlayıcı unsurları, psödonim adı verilen sahte veya değiştirilmiş değerlerle değiştirilir ve ilgili veriler anonim hale getirilmiş olmadığından KVKK'ya tabi olmaya devam eder.

Örneğin, bir sağlık araştırması için toplanan verilerde, bireylerin isimleri gerçek değerler yerine, belirli bir kodlama sistemi veya başka bir yöntemle değiştirilebilir. Bu, verilerin analiz edilmesi ve paylaşılmasını daha güvenli hale getirir, çünkü kişisel bilgilerin gerçek değerleri ortaya çıkmaz. Ancak araştırmacılar hala analizlerini gerçekleştirebilir ve genel eğilimleri anlayabilirler.

GRC LEGAL
Yorumu

Şirketlerin kişisel verileri Avrupa içinde depolamak için adım attıklarını görmekteyiz. Şirketler tarafından atılan adımlar, Avrupa Birliği'nde giderek sıkılaştıran veri gizliliği yasalarına uyum sağlama çabalarını yansıtmaktadır. Bu gelişmeler, teknoloji şirketlerinin, müşteri verilerini depolama ve işleme konusunda yerel düzenlemelere uyum sağlama ihtiyacını yansıtmakta olup kişisel verilerin işlenmesi hukuku bağlamında önemli bir adım olarak değerlendirilebilir. Kişisel veri güvenliği nosyonunun önümüzdeki süreçte tüm şirketler tarafından benimseniyor olması kişilik haklarına daha az müdahaleyi gerektirecek bir alt yapının kurulmasını kolaylaştıracaktır.

CNIL x Yahoo

Fransız Veri Koruma Kurumu (Commission Nationale De L'informatique Et Des Libertés, "CNIL"), "Yahoo.com" internet sitesinde çerezleri reddeden internet kullanıcılarının seçimine saygı göstermediği ve "Yahoo! Mail" mesajlaşma hizmeti kullanıcılarının çerezlere verdikleri izni serbestçe geri almalarına olanak tanımadığı gerekçeleriyle Yahoo Emea Şirketi'ne ("Yahoo" veya "Şirket") 10 milyon euro para cezası verdi.



Ne olmuştu?



Bilindiği üzere Yahoo, arama motoru ve e-posta hizmeti gibi çeşitli internet hizmetleri sunmaktadır. CNIL, çerezlerin reddedilmesinin dikkate alınmadığı ve depolanmasına ilişkin rızanın geri çekilmesinde karşılaşılan engelleri bildiren çok sayıda şikayet almış; Ekim 2020 ve Haziran 2021'de, Yahoo.com internet sitesi ve Yahoo! Mail mesajlaşma hizmetinde çeşitli çevrimiçi incelemeler gerçekleştirmişti.



İlgili cezanın verilmesinde etkili olan ihlal başlıkları ise şu şekilde;

1. Kullanıcının onayı olmaksızın yerleştirilen çerezler

Soruşturma sırasında CNIL; bir internet kullanıcısı “Yahoo.com” sitesini ziyaret ettiğinde görüntülenen çerez panelinin, çerezlerin depolanması için onay almak üzere tasarlanmış birçok düğme içeren bir sayfaya erişim sağladığını ve herhangi bir açık rıza verilmemesi senaryosunda bile, reklam amaçlı yaklaşık yirmi çerezin internet kullanıcısının terminaline yerleştirildiğini tespit etti.

2. Açık rızanın geri alınmamasına ilişkin yönlendirmeler

CNIL, “Yahoo! Mail” mesajlaşma hizmeti kullanıcılarının çerezlerle ilişkin onayı geri çekmek istemeleri halinde, artık *Şirket'in hizmetlerine erişemeyecekleri ve mesajlaşma hizmetlerine erişimlerini kaybedecekleri konusunda bir bilgilendirme ile karşılaştıklarını* kaydetti.

Rıza verilmemesi veya verilen rızanın geri çekilmesinin kullanıcıya negatif bir etki yaratmaması gerektiğini belirten CNIL, bu vakada rızasını geri çekmek isteyen kullanıcılara bir alternatif göstermeden sadece hizmetin kullanımından vazgeçme opsiyonunu sunan Şirket'in *rızanın özgür irade ile verilmesi unsurunu sakatladığını* dile getirdi.

CNIL'in bir başka değerlendirmesi; bir e-posta adresinin, kullanıcının alışveriş yapmasına, ağını geliştirmesine ve önemli kişisel veya mesleki konuşmaları arşivlemesine olanak tanıdığı ölçüde, kullanıcının özel hayatının bir unsuru olduğunu vurgulamak yönünde oldu. *Kullanıcıların e-posta adresleri nezdinde zamanla oluşturdukları bir arşiv de bulunduğundan, ilgili e-posta adresini değiştirme veya hizmetin kullanımını durdurma seçenekleri temelde kullanıcı yanlısı ve kolaylıkla uygulanabilecek çözümler olmamaktadır.*

Çerez uygulamalarının son dönemde veri koruma otoritelerinin gündeminde olduğu ve yanlış uygulamalar neticesinde şirketlerin yüksek cezalar ile karşı karşıya kaldığı gözlemlenebilmektedir. Yakın zamanda Kişisel Verileri Koruma Kurulu'nun da benzer şekilde çerez uygulamalarının doğru şekilde yürütülmemesinden dolayı bir çevrimiçi oyunun Türkiye'deki dağıtıcısı olan veri sorumlusuna 750.000 TL idari para cezası verdiği bilinmektedir. Bu kapsamda çerez panellerinin kullanıcı dostu olması, açık rıza gerektiren çerezlerin yalnızca görünürde değil arka planda da rıza doğrultusunda işlenmesi, opt-in mekanizmasının benimsenmesi son derece önem arz etmektedir.

GRC LEGAL
Yorumu