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 Aralık ayına aittir.

Bilgi Komisyonu Ofisi x Birleşik Krallık

Bilgi Komisyonu, Birleşik Krallık'ın önde gelen internet sitelerini veri koruma yasası uyarınca **çerez değişiklikleri yapmaları**, yapmadıkları takdirde yaptırımla karşı karşıya kalacakları konusunda uyardı.

Bazı internet siteleri, kullanıcılara kişiselleştirilmiş reklamcılık amacıyla izlenip izlenmeyecekleri konusunda adil seçenekler sunmuyor. Bilgi Komisyonu Ofisi (Information Commissioner's Office, "ICO") daha önce, kuruluşların kullanıcıların "Tümünü Reddet" reklam çerezlerini "Tümünü Kabul Et" kadar kolay hale getirmesi gerektiğine dair net bir kılavuz yayınlamıştı. Bu kılavuz, kullanıcılar tüm izlemeyi reddettiğinde internet sitelerinin reklam göstermeye devam edebileceğini ancak bunları göz atan kişiye göre uyarlamaması/kişiselleştirmemesi gerektiğini belirtmekte.

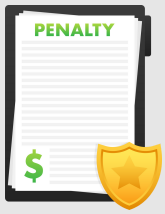
ICO, Birleşik Krallık'ın en çok ziyaret edilen internet sitelerinin çoğunu işleten şirketlere yönelik endişelerini belirttiği ve internet sitelerinin yasalara uygun olmasını sağlamak için 30 gün süre tanıdığı bir mektup gönderdi.

ICO Düzenleyici Risk Yönetici Direktörü Stephen Almond mektupta şunları söyledi: “Hepimiz, örneğin yurtdışında bir uçuş rezervasyonu yaptırdığımızda bizim için özel olarak tasarlanmış gibi görünen otel reklamı gördüğümüzde şaşırıyoruz. **Araştırmamız, şirketlerin kişisel verileri ilgililerin izni olmadan hedefli reklamcılık faaliyeti için kullanmalarından dolayı birçok kişinin endişe duyduğunu gösteriyor.**
Kumar bağımlıları, tarama kayıtlarına dayalı bahis teklifleriyle hedeflenebilir, kadınlar düşükten kısa bir süre sonra üzücü bebek reklamlarıyla hedeflenebilir ve cinselliklerini keşfeden birine cinsel yönelimlerini ifşa eden reklamlar sunulabilir.
En önde gelen internet sitelerinin çoğu uygulamaları doğru işletti fakat **bunu henüz başaramamış şirketlere net bir seçenek sunuyoruz: değişiklikleri şimdi yapın ya da sonuçlarıyla yüzleşin.”**

ICO, endişeleri gidermeyen şirketlerin ayrıntıları da dahil olmak üzere Ocak ayında bu çalışma hakkında bir güncelleme sunacak. Eylem, insanların haklarının çevrimiçi reklamcılık endüstrisi tarafından korunmasını sağlamaya yönelik daha kapsamlı çalışmaların bir parçası olacak.

GRC LEGAL Yorumu

E-ticaret başta olmak üzere pek çok farklı alanı ana faaliyet konusu edinmiş şirketlerin, internet siteleri aracılığıyla gerek GDPR gerekse de ulusal mevzuatlar çerçevesinde hukuka aykırı olarak yürüttüğü çerez uygulamaları, kişileri hedefli reklamcılık ve profilleme faaliyetlerine maruz bırakmakta ve bir temel hak olan kişisel verilerin korunması nosyonunu derinlemesine baltalamaktadır. Bugüne kadar yayımlanan birçok Rehber, Kılavuz ve idari otoritelerin kararları ile yasaklanan bu faaliyetlerin hala devam ediyor olmasının altında yatan en temel sebep ise öngörülen yaptırımların caydırıcı olmayışıdır.



Nitekim, bu şirketlerin çerez uygulamaları ile kazandığı gelirler göz önünde bulundurulduğunda tabi olacakları idari para cezaları kabul edilebilir risk olarak görülmektedir.
Şirketlere net bir mesaj gönderen ICO’nun, yasalara uyum sağlamayanlara ne derece caydırıcı bir yaptırım öngöreceği ve şirketlerin, kullanıcıların çevrimiçi ortamlarda kişisel verilerinin korunması adına faaliyetlerini ne yönde şekillendireceği şimdiden merak konusu.

Kanada x LockBit

Yetkililer yaptığı açıklamada Kanada hükümeti, ordusunu ve polis çalışanlarını etkileyen bir veri ihlalinin 24 yıllık kişisel ve finansal bilgileri içerebileceğini duyurdu.

Kanada Hazine Kurulu Sekreterliği, 1999'dan bu yana nakliye ve taşıma hizmetlerinde küresel ölçekte önde gelen şirketlerden SIRVA veya BGRS Kanada adlı devlet yüklenicilerinin sunduğu hizmetleri kullanan herkesi, verilerinin tehlikeye girmiş olabileceği konusunda uyaran bir bildiri yayınladı. Bu sırada, **fidye yazılımı çetesi LockBit de saldırının sorumluluğunu üstlendi.**

SIRVA/BGRS ihlali, ilk olarak 20 Ekim'de hükümet yetkilileri tarafından askeri ve sivil personele gönderilen ve saldırının kapsamı hakkında çok az bilgi içeren bir bildirimde kamuoyuna açıklandı. Kanada'nın devlet radyo ve televizyon yayıncısı olan CBC'ye göre bildirim, nakliye hizmetlerinin kesintiye uğraması ve BGRS'nin internet sitesinin 29 Eylül'de çevrimdışı olmasının ardından geldi. Yetkililer şimdi, Kanada'nın mevcut ve eski hükümeti, Kanada Silahlı Kuvvetleri ("**CAF**") ve Kanada Kraliyet Atlı Polisi ("**RCMP**") personelinden gelen bilgilerin muhtemelen ihlale karıştığını söylüyor.

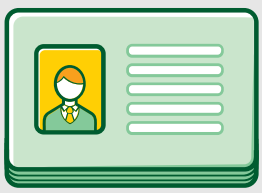
Hazine Kurulu yaptığı açıklamada, "Şu anda, değerlendirilen önemli miktarda veri göz önüne alındığında, etkilenen kişileri henüz belirleyemiyoruz" dedi. "Ancak, **ön bilgiler, ihlal edilen bilgilerin 1999 gibi geçmişe uzanan bir tarihte nakliye hizmetlerini kullanan herkese ait olabileceğini ve çalışanların şirketlere sağladığı finansal bilgileri içerebileceğini gösteriyor."**

Olay ayrıca Kanada Siber Güvenlik Merkezi, Gizlilik Komiseri Ofisi ve RCMP'ye de bildirildi. **Hükümet, olayı araştırmak ve saldırıda kullanılan güvenlik açıklarının ele alınmasını sağlamak için SIRVA/BGRS ile birlikte çalışıyor**. Kanada Hazine Kurulu Sekreterliği sözcüsü, SC Media'ya verdiği demeçte daha fazla ayrıntı veremeyeceklerini, ancak bu bilgiler elde edildikçe paylaşılmaya devam edeceğini söyledi.

LockBit, Kanada Hükümetinden 1,5 TB Veri Çaldığını İddia Ediyor!

Fidye yazılımı çetesi LockBit, BleepingComputer tarafından yayınlanan ekran görüntüsüne göre 17 Ekim'de dark internet sızıntı sitesinde yapılan saldırının sorumluluğunu üstlendi. Bu grup, **SIRVA'nın Avrupa, Kuzey Amerika ve Avustralya şubelerinden 1,5 TB'tan fazla belge ve "3 tam CRM yedeğini" çaldığını iddia ediyor.** 20 Kasım itibariyle, LockBit'in sitesinde grubun "mevcut tüm verileri" yayınladığını belirtti. Hükümet yetkilileri, failin kimliğini veya kamuoyuna yapılan açıklamalarda çalınan verilerin tam hacmini doğrulamadı.

Kanada hükümeti, 1995'ten beri BGRS'nin hizmetlerini kullanıyor. BGRS'nin internet sitesinde yer alan genel bir bakışa göre, yüklenici yılda 14.000'den fazla CAF üyesinin taşınmasını kolaylaştırıyor. Hükümet kayıtlarına göre, hükümet ayrıca 2009'dan beri SIRVA Canada ile de sözleşme imzalamış durumda. SIRVA ve BGRS, Ağustos 2022'de birleşti. SC Media, konu hakkında yorum almak için SIRVA'ya ulaştı ancak bir yanıt alamadı.



Hükümet; son 24 yılda BGRS veya SIRVA Kanada'ya taşınan tüm mevcut ve eski hükümet, CAF ve RCMP çalışanlarına kredi izleme ve pasaportların yeniden düzenlenmesi de dahil olmak üzere hizmetler sunuyor. **Yetkililer, ayrıca potansiyel olarak etkilenen kişileri oturum açma ve kimlik bilgilerini güncellemeye, çok faktörlü kimlik doğrulamayı etkinleştirmeye ve çevrimiçi hesaplarını olağandışı etkinliklere karşı izlemeye çağırdı.**

McNee, hükümetin tavsiyesine katılarak verilerin yaşının bazı ek önlemler gerektirdiğini ekledi. Ayrıca McNee, **“Vatandaşlara, kritik çevrimiçi hesaplarla ilgili güvenlik veya hesap kurtarma sorularının yanıtlarını değiştirmeyi düşünmelerini öneriyoruz;** çünkü '2005'te hangi sokakta yaşıyordunuz?' gibi soruların 'doğru' yanıtları da burada yani sızdırılan bilgilerde bulunabilir.” dedi.

GRC LEGAL Yorumu

Yaşanılan veri ihlalinin boyutu, bireylerin mahremiyeti ve güvenliği açısından ciddi bir tehdit oluşturmaktadır. İlgili veri ihlalinden hükümet, ordu ve polis teşkilatları gibi **kamu kurumlarının etkilenmesi, toplumun geniş kesimlerini potansiyel olarak tehlikeye sokmaktadır**. Buna ek olarak, pek çok insanın etkilendiği veri ihlalinde fidye yazılımı çetesi olan LockBit’in sorumluluk alması ise siber suçların organize bir hal aldığını göstermektedir.

Bu durumda **veri güvenliğini sağlamak amacıyla her türlü önlemin alınmasını gerektiğinin ve bu önlemlerinin güncel ve etkili olması gerekliliğinin** altını çizmek gerekmektedir. Bu kapsamda, hükümetin önerdiği **kullanıcı kimlik bilgilerini güncelleme, çok faktörlü kimlik doğrulamayı etkinleştirme ve çevrimiçi hesapları izleme önlemlerinin, kişisel veri güvenliğini arttırma yolunda atılabilecek en temel adımlardan olduğu kanaatindeyiz.**

Meta x Reşit Olmayan Kullanıcılar

Facebook ve Instagram gibi sosyal medya platformlarının ana şirketi olan Meta, devam eden bir federal davada ciddi iddialarla karşı karşıya. Açıklanan mahkeme belgeleri, Meta’nın en az 2019'dan bu yana, **13 yaşın altındaki çocuklara ait hesapların aktif kalmasına bilerek izin verme ve ebeveynlerinin izni olmadan kişisel bilgilerini toplamakla suçlandığını ortaya koydu.**

Bu açıklama, çevrimiçi gizlilik ve sosyal medyada küçüklerin korunmasına ilişkin endişelerin arttığı bir dönemde geldi.

Reşit Olmayan Kullanıcıların Raporları ve Yasal Sonuçları

33 eyalet savcısı, şirketin 2019'un başları ile 2023'ün ortası arasında ebeveynler ve topluluk üyeleri de dahil olmak üzere çeşitli kaynaklardan, Instagram’da reşit olmayan kullanıcılara ilişkin bir milyondan fazla rapor aldığını belirtti.

Bu raporlara rağmen, Meta'nın bu hesapların yalnızca bir kısmını devre dışı bıraktığı iddia ediliyor. Bu eylem veya eylemsizlik, şikâyetin temelini oluşturuyor. 54 suçlamayı kapsayan dava, Meta'nın eyalet bazlı bir dizi tüketiciyi koruma yasasını ve Çocukların Çevrimiçi Gizliliğini Koruma Yasası’nı (Children's Online Privacy Protection Act, **“COPPA”**) ihlal ettiğini iddia ediyor.

COPPA, şirketlerin ebeveyn izni olmadan 13 yaşın altındaki çocuklardan kişisel bilgi toplamasını yasaklıyor. Mahkeme belgesi, Meta'nın kayıtlarının Instagram'ın önemli sayıda küçük yaşta kullanıcıya sahip olmasının ve "13 yaşın altındaki milyonlarca çocuk" ve "yüz binlerce genç kullanıcının" platformda yoğun vakit geçirmesinin, reşit olmayan kullanıcı tabanının önemini ortaya koyduğunu vurguluyor.

Meta'nın Cevabı ve Yaş Doğrulamanın Zorluğu

Suçlamalara yanıt olarak Meta, Instagram kullanım şartlarının 13 yaş altı kullanıcıları yasakladığını ve şirketin bu tür hesapları kaldırmaya yönelik tedbirlerinin bulunduğunu belirtti.

Bununla birlikte Meta, çevrimiçi kullanıcıların, özellikle de kimlik bilgileri olmayanların yaşını doğrulamanın zorluğunu kabul ediyor. Meta CNN'e yaptığı açıklamada, uygulama mağazalarında 16 yaşın altındaki gençlerin uygulama indirmeleri için ebeveyn onayı almasını gerektiren federal yasayı desteklediğini de vurguladı.

Meta'ya göre bu yaklaşım, yaş doğrulaması için kimlik kartları gibi hassas bilgilerin elde edilmesi ihtiyacını azaltacaktır. **Dava ilerledikçe, çevrimiçi gizlilik, küçüklerin korunması ve teknoloji devlerinin platformlarını denetlemedeki sorumluluklar ile ilgili önemli endişeleri ortaya çıkarıyor.**

Yüz milyonlarca dolara varan olası hukuk cezaları ile bu dava, sosyal medya şirketlerinin reşit olmayan kullanıcıları ve veri gizliliğini nasıl ele aldıkları konusunda bir emsal teşkil edebilir.

GRC LEGAL Yorumu

Dünya çapında milyonlarca kullanıcı barındıran platformların sahibi olan Meta'nın, çocuklara yönelik gizlilik ihlalleri iddiasıyla karşı karşıya kalmasıyla birlikte küresel bir krizin gündeme geldiğini görüyoruz. Aslında Meta da 13 yaş altı kullanıcıları yasaklayarak çocukların çevrimiçi ortamda korunması kapsamında iyi uygulama örneği teşkil eden bir tedbir almadığının farkında. Bu anlamda söz konusu dava, sosyal medya şirketlerine bir emsal teşkil edebilecektir.

Bu haber, her ne kadar uluslararası mevzuatta GDPR ve sair düzenlemeler ile çocukların kişisel verilerine ilişkin bir mevzuat yürürlükte olsa da bizim mevzuatımızda çocuklara yönelik özel bir hüküm ve/veya Rehber bulunmaması hususunu tekrar gündeme getiriyor. Halihazırda Kurum tarafından çalışmalarına başlanmış olan çocuklara yönelik Rehber'in, tüm bu uluslararası mevzuatı ve gelişmeleri takip eden ve uygulamaya yön gösterebilecek nitelikte belirleyici düzenlemeler getirmesini temenni etmekteyiz.

CNIL x Groupe Canal +

Fransız Veri Koruma Kurumu **(“CNIL”),** medya şirketinin doğrudan pazarlama faaliyetleriyle ilgili duyulan endişeler nedeniyle Groupe Canal+ aleyhine **600.000 €** para cezası verdiğini duyurdu.

CNIL'e göre şirket hem GDPR hem de Fransız Gizlilik Yasası’nı ihlal ederek kullanıcılara onay almadan pazarlama e-postası gönderdi. **CNIL şirketin, kişisel bilgilerini Canal+'ya değil, Canal+ ortaklarından birine sağlamış olan kişilere pazarlama e-postaları gönderdiğini belirtti.**

Bunu yaparken kişilere, bilgilerin Canal+’ın pazarlama faaliyetleri için Canal+ ile paylaşılacağı ve Canal+ tarafından kullanılacağı söylenmedi. CNIL'e göre Groupe Canal+, grup şirketlerinin uygun rızayı almasını sağlamalıydı.

Buna ek olarak, şirket aleyhindeki karar, GDPR kapsamındaki diğer ihlal iddialarını da içeriyordu. Söz konusu iddialardan bir tanesi, şirketin gizlilik politikasında veri saklama süresinin açıklanmamasına ilişkin. Ayrıca, tüketicilerle telefonla iletişim kurarken gizlilik açıklamalarının yapılmaması ve tüketicilerden gelen hak taleplerine bir ay içinde yanıt verilmemesi de diğer iddialardan. CNIL, belirli tüketicilerin erişim taleplerine yanıt verilmediğini de belirtti.

Kararda, veri gizliliği endişelerinin yanı sıra veri güvenliği endişeleri de vurgulandı. CNIL'e göre şirket, çalışan şifrelerini depolarken uygun güvenlik önlemlerini almadı. Bunun yanında abone verilerinin CNIL'e bildirilmemesi, bu verilerin beş saat boyunca başkaları tarafından görülebilmesine neden oldu.

GRC LEGAL Yorumu

Özellikle pazarlama faaliyetlerinin yoğun olarak yürütüldüğü medya şirketlerine yönelik sıkı bir denetimin yapılması ve bu şirketlerin yüksek idari para cezalarına hükmedilmesi, açık rıza teminini gerektiren doğrudan pazarlama faaliyetlerinden kaynaklı veri ihlallerinin önüne geçilmesine fayda sağlayacaktır. Bu anlamda Groupe Canal+’ın hükmedildiği 600.000 Euro’luk para cezasının, tüm medya şirketleri açısından caydırıcılık sağlamasını temenni etmekteyiz.

Bu haber, her ne kadar uluslararası mevzuatta GDPR ve sair düzenlemeler ile çocukların kişisel verilerine ilişkin bir mevzuat yürürlükte olsa da bizim mevzuatımızda çocuklara yönelik özel bir hüküm ve/veya Rehber bulunmaması hususunu tekrar gündeme getiriyor. Halihazırda Kurum tarafından çalışmalarına başlanmış olan çocuklara yönelik Rehber’in, tüm bu uluslararası mevzuatı ve gelişmeleri takip eden ve uygulamaya yön gösterebilecek nitelikte belirleyici düzenlemeler getirmesini temenni etmekteyiz.

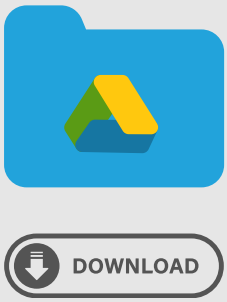
Booking.com x Siber Saldırganlar

Siber saldırganlar, dark internet forumlarında mağdurları bulmak için yardım isteyen reklamlar yayınlayarak Booking.com müşterilerine yönelik saldırılarını artırıyor.

Siber saldırganlar, otellerde konaklayan insanlara otellerin giriş bilgileri için 2.000 dolara (1.600 £) varan teklifler sunuyor. En azından **Mart ayından bu yana** müşteriler, siber saldırganlara para göndermeleri için kandırılıyor.

Siber güvenlik uzmanları, Booking.com'un kendisinin saldırıya uğramadığını ancak siber saldırganların, bu hizmeti kullanan otellerin yönetim portallarına girmenin yollarını bulduklarını söylüyor.

Siber güvenlik şirketi Secureworks araştırmacıları, siber saldırganların pasaportunu odasında unutmuş eski bir misafir gibi davranarak otel personelini Vidar Infostealer adlı kötü amaçlı bir yazılım indirmeleri için kandırdıklarını söylüyor.



Ardından, pasaportun resmini içerdiğini söyleyen bir Google Drive bağlantısı gönderiyor. İlgili bağlantı, kötü amaçlı yazılımları personelin bilgisayarlarına indirerek otomatik olarak otel bilgisayarlarında Booking.com erişimi için tarama gerçekleştiriyor. Bu sayede Booking.com portalına giriş yapılarak oda veya tatil rezervasyonu olan tüm müşteriler görüntülenebildiğinden siber saldırganlar müşterilere uygulamadan mesaj göndererek otel yerine kendilerine para ödemeleri için kandırabiliyor.

Bir Booking.com sözcüsü “Bu ihlal Booking.com'da olmasa da etkilenenler için ciddiyetin farkındayız; bu nedenle ekiplerimiz, ortaklarımızın sistemlerini mümkün olan en kısa sürede güvence altına almalarını ve potansiyel olarak etkilenmiş olanlara yardım etmelerini desteklemek için özenle çalışıyor. Buna müşterilerin, kaybedilen fonların kurtarılması da dahil.” dedi.

Siber güvenlik uzmanı Graham Cluley de suçluların yasa dışı giriş yapmasını zorlaştırmak için Booking.com otellerinin **çok faktörlü kimlik doğrulama uygulaması gerektiğini** söylüyor. Cluley, “Booking.com, sohbet pencerelerinin altında bir uyarı mesajı göstermeye başladı, ancak bundan çok daha fazlasını yapabilirler. Örneğin, birkaç günden daha kısa bir süre içinde faaliyet gösteren internet sitelerine giden bağlantıların sohbete dahil edilmesine izin vermemek müşterileri ödeme yapmaları için kandırmak amacıyla yeni oluşturulmuş sahte sitelerin kullanılmasını önleyecektir.” dedi.

GRC LEGAL Yorumu

Booking.com'da yer alan müşteri bilgilerine otellerin kendi yönetim portallarına saldırı gerçekleştirilerek erişildiği göz önünde bulundurulduğunda, veri sorumlusu otellerin çalışanlarına yönelik kişisel verilere ilişkin farkındalık eğitimlerinin sağlıyor olması bir idari tedbir olarak önem arz etmektedir. Buna ek olarak, otel personellerine iletilen bağlantılara kişiler tarafından tıklanılsa dahi bağlantıya erişimi güvenlik sebebi ile engelleyebilecek teknik birtakım tedbirlerin alınması da veri güvenliğine ilişkin aksiyonları pekiştirecek ve olası veri ihlallerinin önüne geçecektir.

Avrupa Veri Koruma Kurulu x Meta

Avrupa Veri Koruma Kurulu'nun (European Data Protection Board, "**EDPB**") 27 Ekim 2023 tarihli acil bağlayıcı kararının ardından İrlanda Veri Koruma Otoritesi (Irish Data Protection Authority, "**IE DPA**") 10 Kasım 2023 tarihinde Meta Ireland Limited'e karşı verdiği kararda ("**META IE**") sözleşme ve meşru menfaat hukuki sebeplerine dayanarak davranışsal reklamcılık amacıyla kişisel verilen işlenmesini yasakladı.

Bilgi Köşesi

Davranışsal reklamcılık, internet kullanıcılarının çevrimiçi davranışlarına dayanarak kişiselleştirilmiş reklamların oluşturulmasını ve sunulmasını ifade eden bir reklamcılık modeli anlamına gelmektedir. Bu reklam **türü, bireylerin çevrimiçi gezinme alışkanlıkları, arama terimleri, tıklama geçmişi ve diğer çevrimiçi etkileşimleri** gibi verileri analiz ederek, **kullanıcıların ilgi alanlarına ve davranışlarına uygun reklamları hedeflemeyi amaçlar**. Ancak, davranışsal reklamcılık aynı zamanda kullanıcı gizliliği ve veri güvenliği konularında endişelere yol açabilir. Bu tür reklamcılık modelleri, kullanıcı verilerini işleyerek kişisel profiller oluşturduğu için, bu verilerin nasıl kullanıldığı ve korunduğu konularında dikkatlice yönetilmesi gereken bir alanı temsil eder.

EDBP'nin acil bağlayıcı kararı, Norveç Veri Koruma Otoritesi'nin (Norwegian Data Protection Authority, "**NO DPA**") bu konuda tüm Avrupa Ekonomik Alanı'nda (European Economic Area, "EEA") etkili olacak nihai tedbirlerin alınmasına ilişkin talebinin ardından geldi.

EDBP Başkanı Anu Talus konuyla alakalı şunları söyledi: "Dikkatli bir değerlendirmenin ardından EDPB, IE DPA'ya Meta IE'ye yönelik olarak EEA çapında bir işleme yasağı getirmesi talimatını vermenin gerekli olduğunu düşündü. Aralık 2022'de EDPB Bağlayıcı Kararları, sözleşmenin Meta tarafından davranışsal reklamcılık için gerçekleştirilen kişisel verilerin işlenmesi hususu için uygun bir yasal dayanak olmadığını zaten açıklığa kavuşturmuştu. Buna ek olarak, Meta'nın IE DPA tarafından geçen yılın sonunda verilen emirlere uygunluk göstermediği de tespit edildi. Bu durum, olağan iş birliği prosedürüne bir istisna olan ve sadece olağanüstü durumlarda kullanılabilen GDPR'ın 66. maddesinin 1. fıkrasında düzenlenen acil durum prosedürünün kullanımına yol açtı."

14 Temmuz 2023 tarihinde **NO DPA**, sözleşme veya meşru menfaat hukuki temeline dayanarak davranışsal reklamcılık için Norveç'teki ilgili kişilerin kişisel verilerinin işlenmesine ilişkin olarak Meta IE ve Facebook Norway AS (**"Facebook Norway"**) hakkında GDPR'ın 66. maddesi kapsamında geçici bir yasak kararı almıştı. **Bu yasak, zamansal ve coğrafi kapsam açısından üç ay boyunca ve yalnızca Norveç sınırları içinde geçerliydi.** 26 Eylül 2023 tarihinde **NO DPA,** tüm EEA ülkelerinde kullanıcılar için geçerli olan nihai tedbirlerin alınması için EDPB'ye acil bir bağlayıcı karar verilmesi talebinde bulundu.

Bilgi Köşesi

GDPR madde 66 ile düzenlenen aciliyet usulü uyarınca, veri koruma otoriteleri kendi sınırları içerisindeki ilgili kişilerin hak ve özgürlüklerini korumak için acil olarak harekete geçilmesi gerektiğini tespit ettiği istisnai durumlarda, en fazla üç ay süreyle kendi sınırları içerisinde yasal etkisi olan geçici tedbirler alabilir.

Bu tedbirler, GDPR'ın tutarlılık mekanizmasından (GDPR Madde 63) veya Tek Yetkili Mercii mekanizmasından (GDPR Madde 60) derogasyon yoluyla kabul edilir. Bu istisnai hal, yetkililerin her zaman ve her koşulda kendi üye devletlerindeki bireylerin hak ve özgürlüklerini koruyabilecek konumda olmaları için tasarlanmıştır.

Bu tür geçici tedbirleri alan veri koruma otoritesi, bu tedbirleri ve bunları kabul etme nedenlerini gecikmeksizin ilgili diğer veri koruma otoritelerine, Avrupa Veri Koruma Kurulu'na ve Avrupa Komisyonu'na bildirmelidir.
Bu tür geçici tedbirleri almış olan veri koruma otoritesinin, nihai tedbirlerin acilen alınması gerektiğini tespit etmesi halinde standart iş birliği ve tutarlılık prosedürlerine istisna getirerek nihai tedbirlerin alınması için acil ihtiyaç nedenlerini sunarak EDPB'den acil bir görüş veya acil bir bağlayıcı karar talep edebilir.

EDPB, elde edilen kanıtlar sonucunda META IE'in davranışsal reklam amacıyla toplanan kişisel verilerin işlenmesinde sözleşme ve meşru menfaat hukuki sebeplerini uygunsuz kullanarak GDPR'ın 6/1. maddesini (işleme için hukuka uygunluk sebepleri) ihlal etmeye devam ettiğine ve özellikle IE DPA'in Aralık 2022'de verdiği nihai karar başta olmak üzere veri koruma otoritelerinin kararlarına uymayarak ihlallere devam ettiğine karar verdi.

Aciliyet sebebiyle EDPB, düzenli işbirliği mekanizmalarının olağan şekilde uygulanamayacağı ve nihai tedbirler alınmadan ilgili kişilere ciddi ve telafisi mümkün olmayan zararlar verilmesi riskleri ışığında nihai tedbirlerin alınmasına yönelik acil ihtiyacın olduğu sonucuna varmıştır.

Ayrıca EDPB, IE DPA'nın GDPR'da belirtilen süre içinde NO DPA'dan gelen karşılıklı yardım talebine cevap veremediğini de tespit ederek bu durumda GDPR'ın 61. maddesinin 8. fıkrasında düzenlenen aciliyet ön kabulünün geçerli olduğuna, olağan iş birliği ve tutarlılık mekanizmalarından sapmanın gerekliliğine dikkat çekti.

Sonuç olarak, EDPB IE DPA'ya, Meta ürünleri üzerinde toplanan kişisel verilerin sözleşmeye ve meşru menfaate dayalı davranışsal reklamcılık amacıyla işlenmesi için Meta IE'ye yönelik işleme yasağı talimatı vermesinin uygun, orantılı ve gerekli olduğunu değerlendirerek, söz konusu süreç bakımından nihai tedbirlerin IE DPA tarafından kabul edilmesi gerektiğine karar vermiştir. Bu acil bağlayıcı karar IE DPA, NO DPA ve diğer ilgili DPA'lara gönderilmiş olup IE DPA konuya ilişkin nihai kararını 10 Kasım 2023'te sonuca bağlamıştır.

GRC LEGAL Yorumu

İlgili kişileri kategorize etmeye/profillemeye müsait ve oldukça hassas kişisel verilerin toplanmasına olanak sağlayan davranışsal reklamcılık faaliyetlerinin, Meta tarafından GDPR'ın 6. maddesi kapsamında sözleşme ve meşru menfaat hukuki sebebi arkasına sığınarak hukuka aykırı bir şekilde yürütülmesinin önüne aciliyet usulü geçilmiştir. Bu olay, GDPR ihlalleri karşısında hızlı ve etkili müdahalenin ve ulusal otoriteler ile Avrupa düzeyindeki etkileşimlerin hayati önem taşıdığını gösteriyor. EDPB tarafından verilen kararın Meta üzerinde caydırıcı bir etkiye sebep olmasını ve davranışsal reklamcılık amacıyla veri toplayan şirketlere de örnek olmasını umuyoruz.

Avrupa Birliği Yüksek Mahkemesi x Puanlama Algoritmaları

Avrupa Adalet Divanı (Court of Justice of the European Union, **"CJEU"**) 7 Aralık Perşembe günü, **kişisel verileri kullanan puanlama sistemleriyle karar almanın hukuka aykırı olduğuna karar verdi** ve böylece GDPR'ın yürürlüğe girmesinden yıllar sonra, **CJEU otomatik münferit karar alma ile ilgili maddeye ilişkin ilk kararını yayımlamış oldu**. Bu kararın sosyal güvenlik ve kredi kurumları üzerinde önemli etkilere sahip olacağı düşünülüyor.

2018 ve 2021 yılları arasında Hollanda'da Mark Rutte'nin üçüncü hükümetinin istifasına yol açan skandal, hatalı bir risk puanlama algoritması nedeniyle vergi otoritelerinin binlerce kişiyi çocuk bakım yardımı programında sahtekarlık yapmakla suçlamasından kaynaklanmıştı. Mahkeme, herhangi bir türde otomatik puanlamanın, insanların yaşamlarını önemli ölçüde etkilemesi halinde yasak olduğuna hükmetti. **İnsanları kredibilitelerine göre bir puanla derecelendiren Almanya'nın en büyük özel kredi kuruluşu SCHUFA ile ilgili olan kararda, SCHUFA'nın müşterilerinin (bankalar gibi) sözleşmeye bağlı kararlarında SCHUFA'ya "belirleyici" bir rol atfetmesi halinde SCHUFA'nın puanlamasının GDPR'ı ihlal edeceği belirtiliyor.**

Bu kararın geniş kapsamlı sonuçları olabilir. Örneğin Fransa'da Ulusal Aile Ödeneği Fonu (National Family Allowance Fund, "**CNAF**") 2010'dan bu yana potansiyel dolandırıcılık şüpheleri üzerine ev denetimlerini başlatmak için otomatik bir risk puanlama algoritması kullanıyor. Le Monde ve Lighthouse Reports'a göre CNAF'ın veri madenciliği algoritması, kontrolleri önceliklendirmek için ayda 13,8 milyon haneyi analiz ederek puanlıyor. Bu algoritmada, bir risk katsayısının atfedildiği kişisel verilere dayalı yaklaşık 40 kriter kullanarak tüm yararlanıcıları her ay 0 ile 1 arasında puanlıyor. Hak sahiplerinin puanı 1'e ne kadar yakınsa, ev denetimi alma ihtimalleri de o kadar artıyor.

Fransız merkezci milletvekili ve CNIL'in üyesi Philippe Latombe Euractiv'e yaptığı açıklamada CNAF'ın algoritmasını sadece bir risk değerlendirme sistemi olarak gördüğünü, insanları verilerine göre filtrelediğini ve "kuruluşun ihtiyacı olan kişilere ödenek sağlama" amacı nedeniyle kişisel verileri kullandığını söyledi. Latombe sözlerine şöyle devam etti: "Her bir kriter ayrı ayrı ele alındığında dolandırıcılıkla mücadele amacıyla mantıklı görünse de kriterler birbiriyle ilişkilendirildiğinde toplamı ayrımcı olabilir."

Fransız Milletvekili Aurélien Taché şu yorumda bulundu: "Her zamanki gibi, hükümet yoksulluğun kendisinden ziyade yoksullarla mücadele ediyor ve sosyal puanlamayla özgürlüklerin ve mahremiyet hakkının savunulmasına ilişkin en temel ilkeleri bile gözetmiyor."

Puanlama Kısıtlamaları

GDPR yalnızca üç durumda kamu ve özel kuruluşlarını veri madenciliği algoritmalarını kullanmaktan muaf tutmaktadır. Bu durumlar; bireylerin açık rızası, sözleşme gerekliliği veya yasadan kaynaklanan yükümlülüklerdir. Bu kapsamda, kişisel verilerin puanlama algoritmalarına aktarılması AB'de artık çok daha sınırlı.

GRC LEGAL Yorumu

Puanlama algoritmaları, birçok kişisel veriyi birleştirerek kişi hakkında ayrımcılık yapılmasına veya kişinin mağduriyet yaşamasına yol açabilecek olmasının yansıra hatalı kullanımı halinde Hollanda'da yaşanan skandala benzer ciddi sonuçlara da yol açabilecektir. Bu sebeple, ilgili mahkeme kararı gibi kurum ve kuruluşların bu tür sistemleri nasıl kullanmaları gerektiği konusunda yol gösterici müdahaleleri önem taşımaktadır. Bu kararın, kişisel veri koruma standartlarını güçlendirmek, benzer algoritmik sistemleri daha dikkatli bir şekilde düzenlemek hususunda hem kurumlar hem de devletler açısından itici güç olacağını umuyoruz.