DL | Avukatlık Bürosu

KİŞİSEL VERİLERİ KORUMA HUKUKU GÜNCEL GELİŞMELER
EKİM 2024

TÜRKİYE'DEKİ GELİŞMELER

Veri İhlal Bildirimleri

❖ **Lokman Hekim Üniversitesi**

Veri sorumlusu Lokman Hekim Üniversitesi, hosting hizmeti aldığı Natro isimli (http://www.natro.com) firmanın giriş bilgilerinin siber saldırganlarca ele geçirilmesi ve hesaba yetkisiz erişim sağlanması suretiyle gerçekleşen veri ihlalini ("**Veri İhlal**" veya "**İhlal**") Kişisel Verileri Koruma Kurulu'na ("**Kurul**") bildirmiştir. Yapılan bildirimde;

- İhlalin 05.10.2024 tarihinde başladığı,
- İhlalin 06.10.2024 tarihinde sona erdiği,
- İhlaldan etkilenen ilgili kişi gruplarının öğrenciler ve çalışanlar olduğu,
- İhlalden etkilenen kişisel verilerin; ad-soyad, T.C. kimlik numarası, adres, telefon numarası, e-posta adresi ve şifrelenmiş (MD5) web sitesi giriş şifreleri olduğu,
- İhlalden 2.308 kişinin etkilendiğini,
- İlgili kişilerin, veri sorumlusunun e-posta adresi ve çağrı merkezi aracılığla ihlal hakkında bilgi alabilecekleri bildirilmiştir.

❖ Bkz. https://www.kvkk.gov.tr/Icerik/8041/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Lokman-Hekim-Universitesi

❖ **Kilis 7 Aralık Üniversitesi**

Veri sorumlusu Kilis 7 Aralık Üniversitesi, kaynağı ve nasıl gerçekleştiği henüz belli olmayan yetkisiz erişim sonucu bazı kişisel verilere ("**Kişisel Veri**" veya "**Veri**") ulaşılması suretiyle gerçekleşen veri ihlalini Kurul'a bildirmiştir. Yapılan bildirimde;

- İhlalin başlangıç tarihinin bilinmediği,
- İhlalin 25.09.2024 tarihinde sona erdiği,
- İhlalin Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından gelen bildirim üzerine 24.09.2024 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin;
  - Yatay Geçiş Tablosu içinde yer alan T.C. kimlik numarası, ad, soyadı, adres, telefon numarası, Sağlık Kültür Spor Kayıt Tablosu içinde yer alan T.C. kimlik numarası, ad, soyadı, telefon numarası,
  - Halı Saha Rezervasyon Tablosu içinde yer alan ad, soyadı, mail, telefon numarası,
  - Formasyon Tabloları içinde yer alan T.C. kimlik numarası, ad, soyadı, telefon numarası verileri olduğu
- İhlalden etkilenen kişi gruplarının; öğrenciler, müşteriler ve potansiyel müşteriler olduğu,
- İhlale konu tablolarda 2.747 kişinin verilerin bulunduğu bildirilmiştir.

Bkz. https://www.kvkk.gov.tr/Icerik/8035/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Kilis-7-Aralik-Universitesi

❖ **Atılım Üniversitesi**

Veri sorumlusu Atılım Üniversitesi, siber saldırgan/saldırganların, veri sorumlusu sistemlerine yetkisiz erişim sağlayarak sistemde yer alan bir servis aracılıyla Yükseköğretim Kurulu Başkanlığı'na ait Yükseköğretim Bilgi Sistemi ("**YÖKSİS**") üzerinden bazı kişilerin eğitim bilgilerini sorgulamak suretiyle gerçekleşen veri ihlalini Kurul'a bildirmiştir. Yapılan bildirimde;

- İhlalin 09.05.2024 tarihinde başladığı,
- İhlalin 05.06.2024 tarihinde sona erdiği,
- İhlale konu servis üzerinden, sadece okumakta olan öğrencilerin YÖKSİS eğitim bilgilerinin T.C. kimlik numarası ile sorgulanabildiği,
- İhlalden etkilenen kişi sayısının net olarak tespit edilemediği bildirilmiştir.

Bkz. https://www.kvkk.gov.tr/Icerik/8034/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Atilim-Universitesi

Diğer Gelişmeler

❖ **Kişisel Verileri Koruma Kurumu ("Kurum"), çocuklara yönelik olarak kişisel verilerin korunmasına ilişkin Verican isimli bir süper kahramanın çizgi romanını yayımlamıştır.**

Kurum tarafından, kişisel verileri koruyan süper kahraman olan Verican ile kişisel veri mahremiyetine yönelik tehlikelere karşı çocuklar için eğitici ve öğretici bir çizgi roman serisi yayımlanmıştır. Bu seride, çocukların karşılaşabileceği senaryolara ilişkin altı (6) adet çizgi roman paylaşılarak özetle aşağıdaki hususlar vurgulanmaktadır:

- Kişisel veri kavramının anlamı ve kişisel verinin neler olduğu,
- Ebeveynlerin veri güvenliği ve sosyal medya paylaşımları bakımından dikkat etmeleri gerekenlerin hususlar,
- Herkesçe erişilebilen ortamlarda paylaşılan kişisel veriler hakkında ilgili kişi hakları ve izlenebilecek yollar,
- Çocukların siber zorbalığa maruz kalması durumunda hangi yollara başvurabileceği ve yapması gerekenler,
- Dijital oyun bağımlılığı ve dijital oyunlarda paylaşılan bilgilere ilişkin olarak dikkat edilmesi gerekenler,
- Sağlık verilerinin mahremiyetine ilişkin dikkat edilmesi gerekenler.

Bkz. https://www.kvkk.gov.tr/Icerik/8033/Verican-Ile-Kisisel-Verileri-Ogreniyorum

❖ **Kurum tarafından, kişisel verilerin yurtdışına aktarılmasına ilişkin değişiklikler kapsamında, standart sözleşme bildirimi hakkında kamuoyu duyurusu yayımlanmıştır.**

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**Kanun**") 9. maddesinin 4. fıkrasının (c) bendi kapsamında, "standart sözleşmeler" kişisel verilerin yurtdışına aktarılması bakımından uygun güvence yöntemlerinden olarak öngörülmüştür. Aynı maddenin 5. fıkrasında standart sözleşmelerin imzalamasından itibaren beş (5) iş günü içerisinde Kurum'a bildirilmesi gerektiği ifade edilmiştir.

Tüm bu bilgilere ek olarak, Kişisel Verileri Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin ("**Yönetmelik**") 14. Maddesinin 5. Fıkrası kapsamında, standart sözleşme bildiriminin fiziki olarak veya kayıtlı elektronik e-posta ("**KEP**") adresi ya da Kurul tarafından belirlenen diğer yöntemler aracılığıyla Kurum'a bildirilebileceği belirtilmiştir.

Söz konusu duyuruda; Kurul'un 17.10.2024 tarihli ve 2024/1793 sayılı kararı ile, standart sözleşmelere ilişkin bildirim yükümlülüğünün internet üzerinden daha hızlı bir şekilde gerçekleştirilebileceği belirtilerek "Standart Sözleşme Bildirim Modülü" kullanıma ve "Kişisel Verileri Koruma Kurumu Standart Sözleşme Bildirim Kılavuzu" incelemeye sunmuştur.

Bkz. https://www.kvkk.gov.tr/Icerik/8043/Standart-Sozlesme-Bildirim-Modulu-Hakkinda-Kamuoyu-Duyurusu

DÜNYADAKİ GELİŞMELER

Güncel Kararlar

❖ **Slovenya Veri Koruma Otoritesi tarafından; çalışanların görüntülerini hukuka aykırı olarak video kamera aracılığıyla kaydetmesi ve işbu kayıtları hukuka aykırı olarak çevrimiçi ortamda erişime sunması gerekçeleriyle veri sorumlusu işverene € 25.000 idari para cezası öngörülmüştür.**

Söz konusu kararda, veri sorumlusu tarafından çalışanların çalışma alanlarına doğrultulan kameralar da dahil olmak üzere başkaca kameraların da iş yerine yerleştirildiği belirtilmiştir. Söz konusu video kayıtlara ilişkin uyarıların iş yerinde belirsiz bir alana yerleştirildiği, bu sebeple çalışanlar tarafından açıkça görülebilir bir uyarı bulunmadığı ifade edilmiştir. Kamera kayıtları; şirket müdürü ve veri sorumlusu işverene, cep telefonları ve internet sitesi vasıtatasıyla erişime açılmışsa da ilgili kişiler söz konusu kayıtlara erişim sağlayamamıştır. Bununla birlikte, kayıtların kullanım amaçları ve üçüncü kişilere aktarılıp aktarılmayacağı hakkında ilgili kişilere bilgi verilmemiştir.

Slovenya Veri Koruma Otoritesi tarafından gerçekleştirilen inceleme sonucunda, yerleştirilen kameraların amacının çalışanları gözetlemek olduğu sonucuna varılmıştır. Slovenya Veri Koruma Otoritesi kararında, kameraların güvenliği sağlamak gibi meşru menfaate yönetlik amaçlar için konulmuş olması halinde, bu kameraların binanın girişi ve kasalara konulmasının yeterli olacağını, bu sebeple, söz konusu kameraların amacının gözetleme olduğuna hükmetmiştir. Ayrıca, çalışanların gözetlenmesinin işveren için meşru bir amaç olmadığı vurgulanmıştır. Tüm bu değerlendirmeler sonrasında, Slovenya Veri Koruma Otoritesi re'sen inceleme başlatarak veri sorumlusu işveren aleyhine € 25.000, şirket müdürü aleyhine € 1.750 idari para cezasına hükmetmiştir.

Bkz. https://gdprhub.eu/index.php?title=IP_(Slovenia)_-_0603_30_2023_12

❖ **Birleşik Krallık Veri Koruma Otoritesi ("ICO") tarafından, açıkça aranmak istenmeyen kişilere pazarlama araması yapılması sebebiyle WerepairUK ve Service Box Group Limited aleyhine £ 120.000 idari para cezası öngörülmüştür.**

Söz konusu şirketler; 50.000'e yakın sayıda, pazarlama yönünde talebi olmayan kişilere pazarlama amaçlı aramalar gerçekleştirmiştir. İlgili kişileri bu surette hedef alan yoğun şiddetteki pazarlama tekniklerini *(ICO bu hususu, predatory marketing calls, olarak ifade etmiştir.)* kullanan WerepairUK ve Service Box Group Limited şirketlerine ICO tarafından £ 120.000 idari para cezası uygulanması öngörülmüştür. ICO tarafından kararında; yoğun şiddetteki aramalara maruz kalan ilgili kişilerin, "telefona cevap vermeye korkar" hale geldikleri vurgulanarak özellikle yaşça büyük kişilerin defalarca arandığı tespit edilmiştir. Yetkililer, telefon numaralarının "Telephone Preference Service (TPS)"e kaydolmuş kişilerin olduğu ve o sistemden elde edildiğini bildirmişse de ICO tarafından söz konusu şirketlere toplamda £ 1.570.000 olmak üzere idari para cezası uygulanmıştır.

Bkz. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/10/120k-issued-in-fines-to-two-companies-for-predatory-marketing-campaigns/

- **29.500 satır kişisel veriyi hukuka aykırı şekilde kopyalayarak satan RAC Şirketi çağrı merkezi çalışanları Debbie Okparavero ve Maliha Islam aleyhine ertelenmiş (18 ay) hapis cezasına ve 150 saat ücretsiz kamu çalışması yapmalarına karar verilmiştir.**

RAC Şirketi'nin yeni güvenlik takip yazılımı kullanmaya başlamasıyla Debbie Okparavero ve Maliha Islam'ın trafik kazalarına karışmış kişilere ilişkin bilgileri hukuka aykırı şekilde erişerek kopyaladıkları tespit edilmiştir.

8 Ekim'de gerçekleşen duruşmada, Okparavero ve Islam aleyhine 6 ay hapis cezasına hükmedilmiş ancak ceza 18 ay ertelenmiştir. Ayrıca kişilerin, 150 saat ücretsiz çalışma yapmasına karar verilmiştir.

- Bkz. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/10/criminal-record-and-suspended-prison-sentence-handed-to-former-rac-employees/

- **ICO tarafından, Quick Tax Claims Limited ve National Debt Advice Limited şirketlerine toplamda £ 150.000 idari para cezası öngörülmüştür.**

Vergi iadesi üzerine danışmanlık sağlayan Quick Tax Claims Limited ile borç danışmanlık hizmeti sağlayan National Debt Advice Limited hakkında, bir ay içerisinde 7.863.547 adet spam mesajı insanları iletmeleri sebebiyle ICO'ya 66.793 adet ilgili kişi şikayeti ulaşmıştır. ICO'ya ulaşan şikayetlerin %93'ünde, mesaj almamak için bir seçeneğin kendilerine sunulmadığı, bir başka deyişle söz konusu şirketler tarafından iletilen mesajların opt-out seçeneğinden yoksun olarak sunulduğu belirtilmiştir.

Bununla birlikte; ICO tarafından gerçekleştirilen incelemeler sonucunda, söz konusu şirketlerin, üçüncü taraf tedarikçilerden kişisel veri satın aldığı, işbu kişisel verilerin ise geçersiz rızalara dayandığı tespit edilmiştir. Elde ettiği bilgisi üzerine Quick Tax Claims Limited adına £ 120.000 idari para cezasına hükmedilmiştir.

Ek olarak, National Debt Advice Limited'e, vatandaşların reddedilen kredi başvuru verileri de dahil olmak üzere, işbu kişisel verileri satın almalarının da tespit edilmesiyle birlikte £ 30.000 idari para cezası öngörülmüştür.

- Bkz. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/10/two-companies-fined-a-total-of-150k-after-bombarding-people-with-spam-texts-offering-financial-debt-services/

- **ICO tarafından, Kuzey İrlanda Polis Servisi (Police Service of Northern Ireland) aleyhine £ 750.000 idari para cezasına hükmedilmiştir.**

ICO tarafından yapılan incelemeler sonucunda, Kuzey İrlanda Polis Servisi'nde çalışan 9.483 memur ve personelin soyadı, baş harfleri, rütbeleri ve rollerinin bir veri ihlali sonucu halka açık hale geldiği tespit edilmiştir. Gerçekleştirilen incelemeler kapsamında, Kuzey İrlanda Polis Servisi'ne, özel sektöre uygulanan tarife üzerinden yaptırım uygulanmayarak kamu sektörü tarifesinden ceza uygulanmıştır. Aksi takdirde, söz konusu idari para cezasının £ 5.600.000 olacağı belirtilmiştir. Söz konusu ihlal, bilgi alma hakkı kapsamında WhatDoTheyKnow adlı bir internet sitesinden bir vatandaşın *"her rütbedeki memur sayısı ve her derecedeki personel sayısı ile kaç personelin esas / geçici / vekaleten olduğu"* hakkında soru sorması üzerine gerçekleşmiştir. Bilgi alma hakkı kapsamındaki başvuruyu yanıtlamak adına, söz konusu bilgiler SAP sistemi aracılığıyla excel olarak indirilmiş, incelenmiş ve ardından silinmiştir. Ancak dosyalardan bir tanesi soru sorulan site olan WhatDoTheyKnow'a sehven yüklenmiştir. Bu yükleme hemen fark edilmiş ve silinmiştir.

- Bkz. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/10/what-price-privacy-poor-psni-procedures-culminate-in-750k-fine/

❖ **İrlanda Veri Koruma Otoritesi tarafından, profil oluşturan kullanıcıların kişisel verilerini davranış analizi ve hedefli reklam amacıyla işlemesi sebebiyle LinkedIn Ireland Unlimited Company ("LinkedIn") aleyhine € 310.000.000 idari para cezası öngörülmüştür.**

İrlanda Veri Koruma Otoritesi'nin gerçekleştirmiş olduğu inceleme sonucunda LinkedIn üzerinden alınan açık rızanın; özgürce verilmediği, yeterince bilgilendirilmeden alındığı, spesifik veya açık olmadığı gerekçesiyle, davranış analizi ve hedefli reklam amacıyla kullanıcılarının 3. taraf bilgilerinin işlemek için GDPR'ın 6. maddesi uyarınca dayanaktan yoksun olduğu tespit edilmiştir.

Verilen kararda, 6. madde kapsamında üç işleme yönteminden söz edilmiştir. Bunlar; rıza, meşru menfaat ve sözleşmesel zorunluluk olmak üzere incelenmiştir. Ancak yapılan incelemeler sonucunda LinkedIn'in söz konusu kişisel verileri işlemek için hiçbir hukuki dayanağının olmadığı sonucuna varılmıştır.

Yürütülen incelemeler sonucunda LinkedIn'e kınama, toplamda € 310.000.000 olmak üzere üç idari para cezası verilmiş ve işleme şartlarını uygun hale getirmesi gerektiği talimatı verilmiştir.

❖ Bkz. https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million

Kamuoyu Duyuruları ve Haberler

❖ **ICO, halktan gelen çevresel bilgi taleplerini karşılamaması sebebiyle United Utilities'a ilişkin olarak uygulama tavsiyesi yayımlamıştır.**

Uygulama tavsiyesinde; Çevresel Bilgi Yönetmelikleri (Environmental Information Regulations) uyarınca, Birleşik Krallık'taki su şirketlerinin; halkı hem talep halinde hem de talep olmaksızın bilgilendirmek ile yükümlü olduğu belirtilmiştir.

Ayrıca, Avrupa Birliği Genel Veri Koruma Tüzüğü ("**GDPR**") uyarınca, ilgili kişilere kendi kişisel verilerine erişim hakkı sağlanmaktadır. Ancak, Çevresel Bilgi Yönetmeliklerinin kişilerin kendi kişisel verilerine erişim imkanı vermediği vurgulanmıştır.

Bu doğrultuda, söz konusu uygulama tavsiyesinde ICO tarafından, çevresel bilgi talebi alınması durumunda, su şirketlerinin bu hususu ilgili kişi başvurusu olarak değerlendirmesi gerektiğini ifade etmiştir. Bu değerlendirmeyi yaparken, Çevresel Bilgi Yönetmelikleri kapsamında şeffaflık ve açıklık ilkesi ile GDPR veri koruma ilkeleri arasındaki dengeyi kurmanın önem arz ettiği belirtilmiştir.

ICO'ya gerçekleştirilen şikayetler üzerine yürütülen araştırmalar sonucunda, bilgi taleplerine şirketlerin 20 iş günü içerisinde cevap vermesi gerekirken, United Utilities'ın söz konusu talepleri çevre konulu olmadığı gerekçesiyle cevaplandırmağı tespit edilmiştir. Uygulama tavsiyesinde, su şirketlerinin çevresel konuları daha geniş yorumlaması ve çevresel süreçlerde daha şeffaf olması tavsiyede bulunulmuştur.

Bu sene itibarıyla, ICO tarafından, 12 su şirketine uygulama tavsiyesindeki bu husus hakkında uyarıda bulunulmuştur. Çevresel konularda daha şeffaf olarak halkın bu konudaki güvenini kazanmaları gerektiği ve bu uyarıların dikkate alınmaması durumunda yaptırımlar ile karşılaşılabilecekleri vurgulanmıştır.

❖ Bkz. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/10/action-taken-against-united-utilities-over-transparency-failings/

❖ **Avustralya Veri Koruma Otoritesi tarafından, gizlilik ve üretken yapay zeka modellerinin geliştirmesi ve eğitilmesi konusunda bir rehber yayımlanmıştır.**

Söz konusu rehber, yapay zeka modelleri veya sistemlerini tasarlayan, oluşturan, eğiten uyarlayan veya birleştiren kişi veya kuruluşlar yani "geliştiriciler" için hazırlanmıştır. Rehber kapsamında 5 ana hedeften bahsedilmiştir:

- Geliştiriciler, yapay zeka bağlamında risk düzeyiyle orantılı olarak; yüksek kaliteli veri setleri kullanarak ve uygun testleri yaparak yapay zeka modellerinin doğruluğunu sağlamalıdır. Aynı zamanda, risk düzeyi yüksek durumlarda, yasal uyarı gibi ek önlemler alınması gerekmektedir.
- Yapay zekayı eğitirken kullanılan bilgiler kamuya açık olsa bile, kişisel bilgiler içerip içermediği kontrol etmeli ve gerekli gizlilik yükümlülükleri yerine getirilmelidir. Örneğin; bilgilerin silinmesi gerekiyorsa bu adımlar uygulandıktan sonra yapay zeka eğitiminde kullanılmalıdır.
- Toplanması için izin gerektiren bilgiler hususuna özellikle dikkatli edilmelidir. Geliştiricilerin, bu bilgilerin ilgili kişilerin rızası dışında alınmış olabileceğini veya internetten yeterli şekilde silinmemiş olabileceğini göz önünde bulundurması gerekmektedir.
- Geliştiricilerin, halihazırda ellerinde bulundurdukları kişisel verileri yapay zeka eğitiminde kullanmaları durumunda, kişisel veriyi birincil toplama amaçlarınnın bu olmaması halinde gerekli gizlilik yükümlülüklerini yerine getirmeleri gerekmektedir. İlgili kişilerden alınan açık rızadan ikincil bir amaçla kullanılacağı açıkça anlaşılması durumunda kullanılması uygun olacaktır.
- İlgili kişilerin sağladıkları açık rızada, kişisel verilerinin yapay zeka eğitilmesi için kullanılacağı açıkça anlaşılamıyorsa, geliştiricilerin bu hususta açık ve bilgilendirici şekilde ilgili kişilerin açık rızasını tekrar alması gerekmektedir. Bu alınan açık rızada, ilgili kişilerin kişisel verilerinin toplanmasından vazgeçmesi seçeneği bulundurulmalıdır.

Bkz. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models

❖ **Avrupa Komisyonu, yenilenmiş "Çocuklar için Daha İyi İnternet" (*Better Internet for Kids*) ("BIK") portalını yayımlamıştır.**

Çocuklara, ebeveynlere, eğitimcilere ve kanun koyuculara dijital ortamın güvenli ve sorumlu bir şekilde kullanılması için yol gösterici nitelikte olması amacıyla BIK yenilenerek kullanıma sunulmuştur.

Söz konusu portala, "öğretmen ve eğitici köşesi", "çocuk ve gençlik köşesi" ve "ebeveyn ve bakmakla yükümlü köşesi" eklenmiştir. İlgililere, popüler uygulamalar ve sosyal medya kullanımı hakkında öğrenme modülleri ve oturumlarla birlikte, gençlerin ve çocukların karşılaşabileceği dijital gerçekleri anlama konusunda yardımcı araçlar sunmaktadır.

Bkz. https://digital-strategy.ec.europa.eu/en/news/something-bik-has-happened

❖ **Avrupa Veri Koruma Kurulu ("EDPB") tarafından, meşru menfaat veri işleme şartına ilişkin içerik yayınlamıştır.**

GDPR kapsamında kişisel veri işleme şartlarından biri olarak meşru menfaat öngörülmüştür. EDPB, meşru menfaatn kabul edilebileceği durumlara; müşterilerle ilişkiler, doğrudan pazarlama, dolandırıcılığın önlenmesi ve emniyet ve güvenlik olmak üzere örnekler paylaşmıştır. Yayımlanan içerikte, meşru menfaatin varlığını tespit ederken üç aşamanın uygulanması öngörülmüştür.

- Meşru menfaatin varlığı incelenirken öncelikle menfaati olan kurum veya 3. kişinin faaliyetiyle ilgili ve Avrupa Birliği veya üye ülkelerlerin kanunlarıyla çelişmemesine dikkat edilmesi gerekmektedir. Aynı zamanda meşru menfaat, veri işleme zamanında açık ve kesin olmalıdır. Bu duruma örnek olarak dolandırıcılığın önlenmesi verilebilir.
- Kişisel veri işlemek için ilgili kişilerin hak ve özgürlüklerini daha az kısıtlayıcı yolların var olup olmadığı ve kişisel veri işlemenin gerçekten gerekli olup olmadığı incelenmelidir. Söz konusu kişisel veri işleme faaliyeti, yalnızca meşru menfaatin amaçları için gerekli olduğu ölçüde gerçekleştirilmelidir.
- Son olarak, meşru menfaatin bireylerin menfaatlerine veya temel hak ve özgürlüklerine üstün gelmemesi gerekmektedir. Bireylerin temel hak ve özgürlüklerinin arasında veri koruma ve mahremiyetin yanı sıra güvenlik hakkı, ifade özgürlüğü ve toplanma ve örgütlenme gibi özgürlüklerin de yer aldığı göz önünde bulundurulmalıdır.

Bkz. https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

❖ **EDPB tarafından, e-Gizlilik Direktifi Madde 5/3 kapsamındaki teknik işlenmelere ilişkin kılavuz yayımlamıştır.**

Söz konusu kılavuzda, çerezler gibi mevcut izleme araçları ve yeni izleme yöntemlerinin ortaya çıkmasıyla, veri koruma hususunda e-Gizlilik Direktifi'nin uygulanabilirliğinin önem arz ettiği vurgulanmıştır. Direktifin 5/3 maddesinin, mevcut izleme araçlarına uygulanabilirliği belirlenmiş olmakla birlikte, yeni izleme araçlarına ilişkin belirsizliklerin mevcut olduğu ifade edilmiştir.

Bu doğrultuda, Kılavuz'da uygulanabilirlik hususunda üç temel unsur belirlenerek detaylı olarak analiz edilmiştir: Bilgi, Abone veya kullanıcının terminal ekipmanı ve Bilgi, depolama ile depolanan bilgilere erişim.

Bkz. https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf