SAYI: 48

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

VERİ & TEKNOLOJİ HUKUKU BÜLTENİ

OCAK 2025

GÜNCEL HABERLER

- "Arabuluculuk Faaliyetleri Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmesine" İlişkin Kamuoyu Duyurusu Yayınlandı
- Ocak Ayı İçerisinde Bildirilen Kişisel Veri İhlali
- Bankacılıkta Kişisel Verilerin Korunmasına Dair Yeni Rehber Yayınlandı
- Kişisel Verilerin Yurt Dışına Aktarılması Rehberi Yayınlandı

GLOBAL GELİŞMELER

- Avusturya Veri Koruma Otoritesinden GDPR İhlali Nedeniyle 5.000 Euro Ceza
- AEPD, Çalışan Verilerinin İzinsiz İşlenmesi Nedeniyle Şirkete 10.000 Euro Ceza Verdi
- EDPB, Yapay Zeka ve Karmaşık Algoritmalar İçin Etkili Veri Koruma Denetimleri Rehberini Yayınladı
- LinkedIn, Müşteri Verilerini Yapay Zeka Eğitiminde Kullandığı Gerekçesiyle Dava Edildi
- CNIL, Veri Tabanlarının Yeniden Kullanımı İçin Uyulması Gereken Yasal Şartları Açıkladı

TARİHİ UZAY MİSYONU

Ocak 2025, uzay araştırmaları açısından önemli bir dönüm noktası oldu. SpaceX, Amerikan şirketi Firefly Aerospace ve Japon Ispace'in geliştirdiği iki uzay aracını, Falcon 9 roketiyle Ay'a gönderdi. 15 Ocak'ta Florida'daki Kennedy Uzay Merkezi'nden gerçekleşen bu fırlatma, özel sektörün uzay keşiflerindeki artan rolünü bir kez daha gözler önüne serdi. Uzay araçları, Ay yüzeyinde bilimsel araştırmalar yapmak ve gelecekteki insanlı görevler için veri toplamak amacıyla gönderildi.

Firefly Aerospace'in "Blue Ghost" adlı uzay aracı, Ay yüzeyinden toz örnekleri toplayarak jeolojik yapı hakkında bilgi edinmeyi hedefliyor. Ayrıca, yüzey sıcaklığını ölçmek ve Ay koşullarına uygun astronot kıyafetleri için testler yapmak gibi 10 farklı deney gerçekleştirecek. Japon şirket Ispace'in aracı ise Ay yüzeyine iniş teknolojilerini test edecek ve gelecek görevler için altyapı oluşturmayı amaçlıyor. Bu görevler, Ay'da kalıcı üslerin kurulması yolunda önemli adımlardan biri olarak değerlendiriliyor.

Bu başarılı fırlatma, uzay araştırmalarında devlet destekli projelerin yanı sıra özel şirketlerin de etkin bir şekilde yer alabileceğini gösterdi. Elde edilecek veriler, Ay'ın yüzey yapısını ve atmosfer koşullarını daha iyi anlamamızı sağlayacak. Aynı zamanda, Ay'a yönelik insanlı görevler için kritik bilgiler sunarak, Dünya dışı yaşam alanları oluşturma çalışmalarına katkıda bulunacak.

GÜNCEL HABERLER

"ARABULUCULUK FAALİYETLERİ KAPSAMINDA AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNE" İLİŞKİN KAMUOYU DUYURUSU YAYINLANDI

Kişisel Verileri Koruma Kurumu ("Kurum") tarafından 13/01/2025 tarihinde Arabuluculuk Faaliyetleri Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmesine ilişkin bir kamuoyu duyurusu yayımlandı. Duyuru kapsamında arabulucuların hem 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu ("Arabuluculuk Kanunu") uyarınca arabuluculuk sürecine ilişkin bilgilendirme yapmakla hem de 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") kapsamında kişisel verilerin işlenmesine dair ayrı bir aydınlatma yükümlülüğünü yerine getirmekle sorumlu olduğu vurgulanmıştır.

Arabuluculuk faaliyetleri, Arabuluculuk Kanunu'nda düzenlenmiş olup, bu faaliyetlerin etkin ve hukuka uygun şekilde yürütülmesi için tarafların bilgilendirilmesi büyük önem taşımaktadır. Bu çerçevede, arabulucuların hem arabuluculuk süreci hem de kişisel verilerin işlenmesi ile ilgili bilgilendirme yükümlülüklerini ayrı ayrı yerine getirmeleri gerektiği vurgulanmıştır.

Arabulucular, Arabuluculuk Kanunu'nun 11. maddesi uyarınca, arabuluculuk faaliyetinin başında tarafları, sürecin esasları, işleyişi ve sonuçları hakkında aydınlatmakla yükümlüdür. Bu bilgilendirme, tarafların süreci anlamalarını ve etkin katılım sağlamalarını hedeflemektedir.

Diğer yandan, arabulucular, KVKK uyarınca "veri sorumlusu" sıfatını haizdir. Bu kapsamda, kişisel verilerin işlenmesine ilişkin KVKK'nın 10. maddesinde belirtilen bilgilendirme yükümlülüğünü de yerine getirmekle sorumludur. Bu yükümlülük, kişisel verilerin işleme amacı, aktarım bilgileri ve ilgili kişilerin haklarını içermektedir.

Özellikle vurgulanması gereken husus, Arabuluculuk Kanunu uyarınca yapılan bilgilendirmenin, KVKK kapsamında gerekli olan aydınlatma yükümlülüğünü karşılamadığıdır. Arabulucular, kişisel veri işleme faaliyetleri için ayrıca aydınlatma yapmalı ve bu yükümlülüğün yerine getirildiğini ispat edebilmelidir.

Kamuoyunun bilgisine sunulan bu duyuruda, arabuluculuk süreçlerinin hukuka uygun şekilde yürütülmesi için tüm arabulucuların, ilgili mevzuatta yer alan yükümlülüklere eksiksiz şekilde riayet etmesi gerektiği bir kez daha hatırlatılmıştır.
İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

GÜNCEL HABERLER

OCAK AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Trabzon Üniversitesi Rektörlüğü

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun *"Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."* hükmünü amirdir.

Veri sorumlusu Trabzon Üniversitesi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusu personeli ve öğrencilerine ait bazı bilgilerin siber saldırganlar tarafından internet üzerindeki yasadışı platformlarda satışa sunulduğu,
- İhlalin 01.01.2025 tarihinde başladığı ve 06.01.2025 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin; kimlik (ad soyad, T.C. numarası, doğum tarihi, anne ve baba adı, doğum yeri), iletişim (e-posta adresi, telefon no (iş ve cep numarası)), özlük (kurumsal sicil no, unvan, öğretmen ve öğrenci ders programlarının bulunduğu dosyalar) ve lokasyon verileri olduğu,
- İhlalden etkilenen kayıt sayısının 25.237 olduğu,
- İhlalden etkilenen ilgili kişi grubunun; veri sorumlusu personeli ve öğrencileri olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.01.2025 tarih ve 2025/171 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

GÜNCEL HABERLER

BANKACILIKTA KİŞİSEL VERİLERİN KORUNMASINA DAİR YENİ REHBER YAYINLANDI

Kişisel Verileri Koruma Kurumu (KVKK) ve Türkiye Bankalar Birliği (TBB), bankacılık sektöründe kişisel verilerin korunmasına yönelik önemli bir adım attı. Ocak 2025'te yayımlanan "Bankacılık Sektörüne İlişkin Kişisel Verileri Koruma Rehberi", bankaların kişisel veri işleme süreçlerini 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili mevzuata uygun hale getirmesi için kapsamlı bir yol haritası sunuyor. Rehber, bankaların müşteri verilerini işleme, saklama, aktarma ve güvenliğini sağlama konularında uyması gereken temel ilkeleri belirliyor.

Rehberde özellikle veri sorumlusu ve veri işleyen kavramları, bankaların bu süreçlerdeki rolleri ve yükümlülükleri detaylandırılıyor. Açık rıza süreçleri, veri aktarımı, güvenlik tedbirleri ve bankacılık sektörüne özgü riskler ele alınıyor. Ayrıca, açık bankacılık, müşteri segmentasyonu ve risk yönetimi gibi modern bankacılık uygulamalarında veri işleme esaslarına ilişkin en iyi uygulamalar paylaşılıyor. Özel nitelikli kişisel verilerin işlenmesi konusunda da bankaların alması gereken tedbirler vurgulanıyor.

Banka müşterilerinin kimlik, iletişim, finansal geçmiş ve işlem bilgileri gibi kritik verilerinin korunması, rehberin en önemli başlıkları arasında yer alıyor. Şube, ATM, internet ve mobil bankacılık kanalları üzerinden elde edilen verilerin güvenli bir şekilde işlenmesi için bankaların teknik ve idari tedbirler alması gerektiği vurgulanıyor. Rehberde, müşteri rızası olmadan pazarlama faaliyetleri için veri işlenemeyeceği, müşteri bilgilerinin üçüncü taraflarla paylaşılması halinde sıkı düzenlemelere tabi olacağı belirtiliyor.

Bunun yanı sıra, uluslararası veri transferleri konusunda da önemli düzenlemeler getiriliyor. Bankaların müşteri verilerini yurt dışına aktarmak istemesi durumunda, KVKK ve ilgili düzenlemelerde belirtilen güvenlik kriterlerini karşılaması gerekiyor. Özellikle bulut bilişim hizmetleri, veri merkezleri ve uluslararası iş birlikleri gibi konularda bankaların KVKK'nın veri aktarımıyla ilgili hükümlerine tam uyum sağlaması bekleniyor.
Rehberin bir diğer önemli noktası, veri ihlali durumunda izlenmesi gereken prosedürler ile ilgili detaylı bilgilerin sunulması. Bankalar, bir veri ihlali tespit ettiğinde en kısa sürede KVKK'ya ve ilgili müşterilere bildirim yapmakla yükümlü olacak. Ayrıca, veri güvenliği ihlallerinin önüne geçmek için düzenli risk değerlendirmeleri ve siber güvenlik testleri yapılması gerektiği rehberde açıkça belirtiliyor.

Yeni rehber, finans sektöründe müşteri gizliliğini ve veri güvenliğini artırmayı amaçlıyor. Bankaların veri yönetimi süreçlerinde daha şeffaf ve güvenli bir yaklaşım benimsemesi beklenirken, rehberin aynı zamanda müşteri haklarını koruyarak güvenli finansal hizmetlerin yaygınlaşmasına katkı sağlaması hedefleniyor. Bankacılık sektöründeki aktörler için bir kılavuz niteliğindeki bu rehber, mevzuata uyum sürecini kolaylaştırarak olası veri ihlallerinin önüne geçmeyi amaçlıyor.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI REHBERİ YAYINLANDI

Kişisel Verileri Koruma Kurumu (KVKK), 2 Ocak 2025 tarihinde "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"ni yayımladı. Bu rehber, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinde yapılan değişikliklere uyum sağlamak amacıyla hazırlandı ve kişisel verilerin yurt dışına aktarılmasına ilişkin üç temel yöntemi ele alıyor:

- Yeterlilik Kararı: KVKK tarafından belirli bir ülkenin yeterli koruma düzeyine sahip olduğuna dair karar verilmesi durumunda, kişisel veriler bu ülkeye aktarılabilir.
- Uygun Güvenceler: Yeterlilik kararı bulunmayan durumlarda, veri sorumluları ve veri işleyenler arasında imzalanacak standart sözleşmeler veya bağlayıcı şirket kuralları gibi uygun güvenceler sağlanarak veri aktarımı gerçekleştirilebilir.
- İstisnai Aktarımlar: Belirli şartlar altında, açık rıza veya kanunda belirtilen diğer istisnalar kapsamında veri aktarımı yapılabilir.

Rehberde ayrıca, standart sözleşme eklerinin nasıl doldurulacağına dair detaylı açıklamalar da bulunmaktadır.

Bu rehber, veri sorumluları ve veri işleyenler için yurt dışına veri aktarımı süreçlerinde rehberlik etmeyi ve uygulamada karşılaşılan belirsizlikleri gidermeyi hedeflemektedir. Ayrıca, kişisel verilerin korunması konusunda uluslararası standartlara uyumu teşvik ederek, veri güvenliğinin artırılmasına katkı sağlamaktadır.

GLOBAL GELİŞMELER

AVUSTURYA VERİ KORUMA OTORİTESİNDEN GDPR İHLALİ NEDENİYLE 5.000 EURO CEZA

Avusturya Veri Koruma Otoritesi (DSB), büyük miktarda sağlık verisi işleyen bir şirketin genel müdürünü Veri Koruma Görevlisi (DPO) olarak atamasını, Genel Veri Koruma Tüzüğü'nün (GDPR) 38(6) maddesini ihlal eden bir çıkar çatışması olarak değerlendirdi. Yetkili otorite, bu durumun GDPR hükümlerine aykırı olduğunu belirterek şirkete 5.000 euro para cezası verdi.

Kararın Gerekçesi

Veri Koruma Otoritesi, kararında DPO'nun temel görevlerinin bağımsız olarak veri işleme faaliyetlerini izlemek ve GDPR'ye uygunluğu sağlamak olduğunu vurguladı. GDPR'nin 38(6) maddesine göre, DPO'nun şirket içinde veri işleme amaç ve araçlarını belirlemesi yasaktır. Ancak, söz konusu şirketin genel müdürü aynı zamanda DPO olarak atanarak hem veri işleme süreçlerini yöneten bir pozisyonda bulunmuş hem de bu süreçleri denetlemekle sorumlu tutulmuştur.

Bu durum, bağımsızlık ilkesine aykırı bir çıkar çatışması yarattığı için GDPR'ye aykırı bulundu. Otorite, DPO'nun rolünün, veri işlemeden sorumlu yöneticilerden ayrı olması gerektiğini ve herhangi bir yöneticinin bu pozisyona atanmasının bağımsızlığı zedeleyebileceğini belirtti.

Şirketler İçin Önemli Bir Uyarı

Bu karar, özellikle büyük ölçekli veri işleyen şirketlerin DPO atamalarında bağımsızlık ilkesine dikkat etmeleri gerektiğini bir kez daha gözler önüne serdi. Şirketlerin, GDPR'ye uygun hareket edebilmek adına DPO'nun tarafsız ve bağımsız bir pozisyonda çalışmasını sağlamaları gerektiği vurgulandı.

Bu karar, Avrupa'daki diğer veri koruma otoriteleri için de emsal teşkil edebilir ve benzer çıkar çatışmalarına yol açan atamaların önüne geçmek için daha sıkı denetimlere yol açabilir. GDPR'ye uyum sağlamak isteyen şirketler, veri koruma görevlisinin organizasyon içindeki konumunu titizlikle belirlemeli ve yöneticilerin bu pozisyona atanmasının önüne geçmelidir.

İlgili habere buradan ulaşabilirsiniz.

GLOBAL GELİŞMELER

AEPD, ÇALIŞAN VERİLERİNİN İZİNSİZ İŞLENMESİ NEDENİYLE ŞİRKETE 10.000 EURO CEZA VERDİ

İspanya Veri Koruma Otoritesi Agencia Española de Protección de Datos (AEPD), bir şirketin çalışanlarının kişisel verilerini izinsiz işlemesi nedeniyle Genel Veri Koruma Tüzüğü'nü (GDPR) ihlal ettiğine hükmetti. Bu ihlal nedeniyle şirkete 10.000 euro para cezası verildi.

İhlalin Detayları

AEPD'nin kararına göre, şirket çalışanların kişisel verilerini toplarken açık rıza almadı ve şeffaflık yükümlülüklerine uymadı. Şirketin çalışanlarının kişisel verilerini belirli bir amaç doğrultusunda işlemesine rağmen, bu verilerin nasıl kullanıldığına dair açık bir bilgilendirme yapılmadığı tespit edildi.

GDPR'nin 5(1)(a) maddesi uyarınca, kişisel verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi gerekir. Ancak AEPD, şirketin veri sahiplerini yeterince bilgilendirmediğini ve rızaya dayalı olmayan veri işleme faaliyetleri gerçekleştirdiğini belirledi.

AEPD'nin Kararında Öne Çıkan Noktalar

- Şirketin, çalışanlarının kişisel verilerini işlerken yeterli bilgilendirme yapmadığı tespit edildi.
- Veri işlemenin hukuki dayanağı açıkça belirtilmedi ve çalışanlardan açık rıza alınmadı.
- GDPR'nin temel ilkeleri ihlal edildiği için şirkete 10.000 euro para cezası uygulandı.

GLOBAL GELİŞMELER

EDPB, YAPAY ZEKA VE KARMAŞIK ALGORİTMALAR İÇİN ETKİLİ VERİ KORUMA DENETİMLERİ REHBERİNİ YAYINLADI

Avrupa Veri Koruma Kurulu (EDPB), yapay zeka (AI) sistemleri ve karmaşık algoritmaların Genel Veri Koruma Tüzüğü'ne (GDPR) uygun olarak denetlenmesi için bir rehber yayımladı. "Yapay Zeka, Karmaşık Algoritmalar ve Etkili Veri Koruma Denetimleri" başlıklı çalışma, AI sistemlerinin veri koruma açısından nasıl değerlendirilebileceğine dair önemli öneriler sunuyor.

Rehberin Öne Çıkan Başlıkları

📌 GDPR Uyumluluğunun Sağlanması: AI sistemleri ve otomatik karar alma mekanizmalarının GDPR'ye uygunluğunu değerlendirmek için şeffaflık, hesap verebilirlik ve adil işleme ilkeleri ön plana çıkarılıyor.
📌 Veri Koruma Etki Değerlendirmesi (DPIA): AI sistemleri için zorunlu hale gelebilecek veri koruma etki değerlendirmeleri nasıl yapılmalı? Rehber, DPIA süreçlerini detaylandırıyor.
📌 Otomatik Karar Alma ve Profil Oluşturma: AI tarafından alınan kararların bireyler üzerindeki etkileri ve veri sahiplerinin haklarını nasıl koruyabilecekleri konusunda öneriler sunuluyor.
📌 Denetim Mekanizmaları: Veri koruma otoritelerinin AI sistemlerini etkin bir şekilde denetleyebilmesi için uygulanabilir teknik ve yasal yöntemler açıklanıyor.

Yapay Zeka ve Veri Koruma Alanında Yeni Standartlar

Bu rehber, AI sistemlerinin GDPR'ye uygun şekilde geliştirilmesi ve denetlenmesi için Avrupa'daki veri koruma otoritelerine, şirketlere ve araştırmacılara yol göstermeyi amaçlıyor. EDPB, AI sistemlerinde hesap verebilirlik mekanizmalarının güçlendirilmesi gerektiğini ve veri sahiplerinin haklarının AI süreçlerinde nasıl korunabileceğinin daha net hale getirilmesi gerektiğini vurguluyor.

Bu yeni kılavuz, AI ve veri koruma arasındaki dengeyi sağlamaya yönelik bir adım olarak değerlendiriliyor ve AI geliştiren şirketler için önemli bir referans noktası oluşturuyor.

GLOBAL GELİŞMELER

LINKEDIN, MÜŞTERİ VERİLERİNİ YAPAY ZEKA EĞİTİMİNDE KULLANDIĞI GEREKÇESİYLE DAVA EDİLDİ

Microsoft'un sahibi olduğu profesyonel ağ platformu LinkedIn, kullanıcı verilerini yapay zeka (AI) modellerini eğitmek için izinsiz kullandığı iddiasıyla ABD'de toplu davayla karşı karşıya kaldı. Kaliforniya'da açılan dava, LinkedIn'in kullanıcıların kişisel bilgilerini onayları olmadan topladığı, işlediği ve AI eğitimi için üçüncü taraflarla paylaştığı iddiasına dayanıyor.

Davacılar, LinkedIn'in bu uygulamalarının ABD'deki tüketici gizliliği yasalarına aykırı olduğunu ve GDPR (Avrupa Veri Koruma Tüzüğü) gibi uluslararası düzenlemelere de ters düştüğünü öne sürüyor.

Davanın Temel İddiaları

- Kullanıcıların Açık Rızası Alınmadı: LinkedIn, AI modellerini eğitmek için kullanıcıların verilerini işledi ancak bu süreç hakkında yeterli şeffaflık sağlamadı.
- Gizlilik Politikaları Yetersiz: LinkedIn'in gizlilik politikalarında AI eğitimi için veri paylaşımı hakkında açık bir bilgilendirme bulunmadığı, bu nedenle kullanıcıların hangi verilerinin nasıl kullanıldığını bilmediği iddia ediliyor.
- AI Eğitimi İçin Üçüncü Taraflarla Paylaşım: LinkedIn'in kullanıcı bilgilerini Microsoft'un AI projeleri ve diğer üçüncü taraf AI geliştiricileriyle paylaştığı iddiası da davanın temel dayanaklarından biri olarak öne çıkıyor.

Dava, AI Etiği ve Veri Gizliliği Tartışmalarını Alevlendirdi

Bu dava, AI modellerinin eğitimi için kullanılan büyük veri kümelerinin etik ve yasal sınırlarını yeniden gündeme getirdi. Daha önce de teknoloji şirketleri, özellikle büyük dil modelleri (LLM) ve generatif AI sistemleri için kullanıcı verilerini izinsiz kullanmakla suçlanmıştı.

- Meta, OpenAI ve Google gibi şirketler de benzer suçlamalarla karşı karşıya. AI teknolojilerinin gelişmesiyle birlikte, kullanıcıların dijital haklarının nasıl korunacağı konusunda küresel çapta yeni düzenlemeler ve yasal mücadeleler artış gösteriyor.
- Dijital Hak Savunucuları ve Düzenleyici Kurumlar Devrede: AI sistemlerinin eğitiminde kullanılan verilerin hangi koşullarda toplanıp işlendiği konusunda artan düzenleyici baskılar, LinkedIn davasının seyrini etkileyebilir.

GLOBAL GELİŞMELER

CNIL, VERİ TABANLARININ YENİDEN KULLANIMI İÇİN UYULMASI GEREKEN YASAL ŞARTLARI AÇIKLADI

Fransa'nın veri koruma otoritesi CNIL (Commission Nationale de l'Informatique et des Libertés), şirketlerin ve kamu kurumlarının mevcut veri tabanlarını yeniden kullanırken Genel Veri Koruma Tüzüğü'ne (GDPR) ve yerel yasalara uygun hareket etmeleri için dikkate almaları gereken kriterleri açıkladı. CNIL, veri tabanlarının farklı amaçlarla yeniden kullanılması sırasında hukuki, teknik ve etik gerekliliklerin göz ardı edilmemesi gerektiğini vurguladı.

Veri Tabanlarının Yeniden Kullanımında Dikkat Edilmesi Gerekenler

1- Veri Toplama Amacı ile Kullanım Amacı Uyumluluğu:
Veriler, başlangıçta toplandıkları amaçla uyumlu bir şekilde kullanılmalıdır. Farklı bir amaç için yeniden kullanım gerekiyorsa, ilgili kişilerin açık rızasının alınması veya yeni bir hukuki dayanak sağlanması gerekir.

2- Şeffaflık ve Bilgilendirme Yükümlülüğü:
Veri sahipleri, kişisel verilerinin nasıl kullanılacağı konusunda açıkça bilgilendirilmelidir. Veri tabanının yeniden kullanılması halinde, ilgili kişilere güncellenmiş bir gizlilik bildirimi sunulmalıdır.

3- Meşru Menfaat Değerlendirmesi:
Eğer veriler meşru menfaat ilkesi çerçevesinde yeniden kullanılacaksa, bireylerin hak ve özgürlüklerine orantısız zarar vermemesi sağlanmalıdır.

4- Veri Güvenliği ve Anonimleştirme:
Kişisel veriler, gereksiz riskleri önlemek için anonimleştirilmeli veya gerektiğinde ek güvenlik önlemleri alınarak korunmalıdır.

5- Üçüncü Taraflarla Paylaşım ve Sözleşmeler:
Veri tabanı, başka şirketler veya hizmet sağlayıcılarla paylaşılacaksa, GDPR uyumlu veri işleme sözleşmeleri yapılmalı ve verilerin yalnızca izin verilen amaçlarla kullanılacağı garanti altına alınmalıdır.