**Denetci.org**

**REFERANS İLKELERİ**

# Mahremiyet İlkeleri

**Rİ-GEN-3**

Sürüm 1.0 · 11.08.2026

www.denetci.org

# Mahremiyet İlkeleri

Mahremiyet, kişilerle ilişkilendirilebilen verinin yalnızca gizli tutulmasını değil; hangi amaçla elde edildiğini, nasıl kullanıldığını, kimlerle ilişkilendirildiğini, ne kadar süre yaşadığını ve kişiler üzerinde hangi sonuçları oluşturduğunu ele alır. Amaç belirli bir hukuk rejimini veya izin ekranını tarif etmek değil; kişisel verinin yaşamı boyunca açık amaç, sınırlı kullanım ve gerçek veri davranışı üzerinden korunmasını sağlayan tasarım anlayışını ortaya koymaktır.

**İlke 1: Kişisel veri açık ve meşru bir amaç olmadan toplanmamalıdır.**

Bir verinin teknik olarak elde edilebilir veya gelecekte yararlı olabilir olması tek başına toplanması için yeterli gerekçe değildir. Veri toplama, hangi gerçek ihtiyaca hizmet ettiğinin anlaşılabildiği bir amaca dayanmalıdır.

**İlke 2: Toplanan veri amacı için gerekli kapsamı aşmamalıdır.**

Belirli bir işlevi yerine getirmek için daha az veri yeterliyse daha ayrıntılı veya daha geniş veri toplamak varsayılan yaklaşım olmamalıdır. Veri miktarı ve ayrıntısı oluşturabileceği mahremiyet etkisiyle birlikte değerlendirilmelidir.

**İlke 3: Bir amaç için elde edilen veri ilgisiz kullanımlar için otomatik olarak serbest hale gelmemelidir.**

Verinin kuruluşun elinde bulunması her yeni kullanımın ilk gerekçeden meşruiyet kazanacağı anlamına gelmez. Yeni kullanım, başlangıç amacıyla ilişkisi ve insanlar üzerinde oluşturabileceği yeni etki bakımından ayrıca değerlendirilebilmelidir.

**İlke 4: Amaç değişikliği gerçek veri davranışında görünür olmalıdır.**

Bir verinin zamanla başka bir işlev için kullanılmaya başlanması yalnızca dokümantasyon değişikliği değildir. Yeni amaç, erişim alanını, saklama ihtiyacını, paylaşımı veya insanlar üzerindeki sonucu değiştiriyorsa bu değişiklik mahremiyet modelinin parçasıdır.

**İlke 5: Mahremiyet yalnızca verinin gizli kalması olarak görülmemelidir.**

Yetkisiz kişilere hiç açıklanmayan veri dahi gereksiz toplanabilir, amaç dışında kullanılabilir, yanlış bağlamda yorumlanabilir veya gereğinden uzun tutulabilir. Mahremiyet, gizliliğin yanında verinin kullanım ve yaşam sınırlarıyla ilgilidir.

**İlke 6: Veriye erişim ile veriyi kullanma yetkisi birbirine eşit kabul edilmemelidir.**

Bir tarafın görevi nedeniyle kişisel veriyi görebilmesi, veriyi başka analizler, kararlar veya amaçlar için kullanma hakkı doğurmaz. Teknik erişim ile meşru kullanım gerektiğinde ayrıştırılabilmelidir.

**İlke 7: Kişisel veri gerçek ihtiyaçtan daha fazla taraf ve sisteme yayılmamalıdır.**

Her yeni kopya ve entegrasyon yeni bir erişim, kullanım ve kayıp alanı oluşturabilir. Veri paylaşımı ve çoğaltılması operasyonel kolaylığın doğal sonucu haline gelmemelidir.

**İlke 8: Geçici veri kullanımı kalıcı veri varlığına dönüşmemelidir.**

Önbellekler, dışa aktarımlar, tanılama verileri, geçici işleme alanları ve benzeri kopyalar kısa süreli ihtiyaç için oluşturulabilir. Geçici olmaları onları yaşam döngüsü ve mahremiyet sınırlarının dışında bırakmamalıdır.

**İlke 9: Kişisel veri yalnızca gerçek ihtiyaç sürdüğü ölçüde yaşamaya devam etmelidir.**

Verinin geçmişte gerekli olması süresiz saklama gerekçesi değildir. Saklama; işlev, yükümlülük ve gerçek ihtiyacın devam ettiği süreyle ilişkilendirilebilmelidir.

**İlke 10: Verinin yaşamının sona ermesi yalnızca görünür ana kaydın kaldırılması anlamına gelmemelidir.**

Kopyalar, arşivler, yedekler, dışa aktarımlar ve üçüncü taraf sistemleri aynı veriyi taşımaya devam edebilir. “Silindi” veya “artık tutulmuyor” iddiası gerçek veri varlığıyla uyumlu olmalıdır.

**İlke 11: Yedekleme mahremiyet yaşam döngüsünün dışında tutulmamalıdır.**

Yedeklerin teknik yapısı verinin aynı anda silinmesini zorlaştırabilir; ancak bu durum verinin sınırsız süreyle ve amaçtan bağımsız kullanılabilmesini meşrulaştırmaz. Eski kopyaların hangi koşullarda yeniden aktif hale gelebileceği de değerlendirilmelidir.

**İlke 12: Veri doğruluğu kişi üzerinde oluşturabileceği etkiyle orantılı önem taşımalıdır.**

Yanlış veya eski bir bilgi kişi hakkında önemli karar verilmesine neden olabiliyorsa yalnızca kaynağından alınmış olması yeterli güvence değildir. Verinin güvenilirliği, kullanıldığı kararın gerçek sonucu ile birlikte ele alınmalıdır.

**İlke 13: Kişisel veri bağlamından koparılarak farklı bir anlam kazanmamalıdır.**

Bir davranışın, konumun veya kaydın anlamı elde edildiği koşullara bağlı olabilir. Veriyi başka bağlama taşımak insanların gerçek davranışı hakkında yanıltıcı çıkarımlar üretmemelidir.

**İlke 14: Çıkarım yoluyla üretilen bilgi de mahremiyet etkisi oluşturabilir.**

Kişi hakkında doğrudan toplanmamış bir özellik, farklı verilerden tahmin veya sınıflandırma yoluyla üretilebilir. Bilginin hesaplanmış olması kişi üzerindeki etkisini ve korunma ihtiyacını ortadan kaldırmaz.

**İlke 15: Profil oluşturma yalnızca teknik analiz faaliyeti olarak görülmemelidir.**

Birden fazla davranış ve özelliğin birleştirilmesi kişi hakkında başlangıçta paylaşmadığı yeni bilgiler ve karar imkanları oluşturabilir. Profilin mahremiyet etkisi tek tek kaynak verilerin hassasiyetinden daha geniş olabilir.

**İlke 16: İnsan üzerinde önemli sonuç doğuran veri kullanımı gereksiz veriye dayanmamalıdır.**

Karar için anlamlı olmayan özelliklerin modele, kurala veya değerlendirmeye dahil edilmesi hem mahremiyet etkisini hem de hatalı ilişkilendirme riskini artırabilir. Kullanılan veri, kararın meşru amacıyla ilişkilendirilebilmelidir.

**İlke 17: Rıza kullanıldığında gerçek ve anlaşılabilir seçim anlamı taşımalıdır.**

Bir kişinin teknik olarak bir kutuyu işaretlemesi, seçeneğin sonucunu anlayabildiğini veya reddetme imkanının gerçek olduğunu göstermez. Rızanın güven değeri, yapılan veri işleminin etkisi ve kişinin sahip olduğu gerçek seçim imkanıyla değerlendirilmelidir.

**İlke 18: Mahremiyet tercihleri karanlık tasarım veya tekrar eden baskıyla aşındırılmamalıdır.**

Reddetmek gereksiz biçimde zorlaştırılmamalı ve daha önce verilmiş tercih kullanıcı fark etmeden yeniden tersine çevrilmemelidir. Arayüz, kişinin kararını almak yerine kuruluşun istediği kararı üretmeye odaklanmamalıdır.

**İlke 19: Mahremiyet tercihleri sistemin gerçek davranışına yansıyabilmelidir.**

Bir tercih yalnızca kullanıcı arayüzünde saklanan bir değer olarak kalmamalıdır. İlgili veri toplama, kullanım, paylaşım veya saklama davranışını gerçekten değiştirebildiği ölçüde anlam taşır.

**İlke 20: Şeffaflık gerçek veri davranışıyla uyumlu olmalıdır.**

Kullanıcıya belirli verilerin hangi amaçla işlendiği açıklanırken arka plandaki sistemlerin daha geniş kullanım veya paylaşım yapması güven ilişkisini bozar. Açıklama sadeleştirilebilir; ancak önemli gerçekliği yanlış göstermemelidir.

**İlke 21: Kişisel verinin kaynağı gerektiğinde anlaşılabilir olmalıdır.**

Kişi hakkında kullanılan bir bilginin kullanıcıdan, başka sistemden, üçüncü taraftan veya çıkarımdan gelmesi güvenilirlik ve kullanım sınırını değiştirebilir. Veri kaynağı önemli karar bağlamında tamamen görünmez olmamalıdır.

**İlke 22: Kamuya açık olmak sınırsız kullanım izni anlamına gelmemelidir.**

Bir bilginin internetten veya başka açık kaynaktan elde edilebilmesi onun her amaç için toplanabileceğini, birleştirilebileceğini veya süresiz saklanabileceğini göstermez. Erişilebilirlik ile meşru kullanım birbirinden ayrılmalıdır.

**İlke 23: Veri kümelerinin birleştirilmesi yeni mahremiyet etkisi oluşturabilecek bir işlem olarak görülmelidir.**

Ayrı ayrı sınırlı bilgi taşıyan veri kümeleri bir araya geldiğinde kişinin kimliği, davranışı veya hassas özellikleri hakkında yeni çıkarımlar oluşabilir. Birleştirme, yalnızca teknik entegrasyon olarak değerlendirilmemelidir.

**İlke 24: Takma adlandırma ve benzeri teknikler anonimlik iddiasının yerine geçmemelidir.**

Doğrudan tanımlayıcıların kaldırılması, veri başka bilgilerle yeniden ilişkilendirilebiliyorsa kişisel etkiyi ortadan kaldırmaz. Kullanılan koruma, gerçek yeniden tanımlama imkanına göre değerlendirilmelidir.

**İlke 25: Anonimlik ve toplulaştırma iddiaları gerçek çıkarım imkanlarıyla sınanabilmelidir.**

Bir grubun içindeki tekil kişilerin yeterli ek bilgiyle ayırt edilebilmesi mümkün olabilir. "Anonim" veya "toplu" etiketi, kişinin artık hiçbir biçimde belirlenemeyeceğine dair sınırsız güven oluşturmamalıdır.

**İlke 26: Üçüncü tarafa veri verilmesi yeni bir güven ilişkisi olarak görülmelidir.**

Veri başka tarafa geçtiğinde yeni erişim, saklama, kullanım ve alt paylaşım alanları oluşabilir. İlk paylaşımın meşru olması sonraki bütün veri davranışlarının otomatik olarak uygun olduğu anlamına gelmemelidir.

**İlke 27: Üçüncü taraf yalnızca gerçek ihtiyacı kadar veriye erişebilmelidir.**

Bir dış tarafın belirli bir işlev sunması bütün veri kümesine veya bütün alanlara ihtiyaç duyduğunu göstermez. Veri paylaşımı hizmetin teknik imkanına değil gerçek amacına göre sınırlandırılmalıdır.

**İlke 28: Dolaylı veri alıcıları mahremiyet modelinin dışında kalmamalıdır.**

Alt yükleniciler, altyapı sağlayıcıları ve başka işleme tarafları kişiyle doğrudan ilişki kurmamış olsa da veriye erişebilir veya veri üzerinde işlem yapabilir. Veri zincirindeki gerçek taraflar gerektiğinde anlaşılabilir olmalıdır.

**İlke 29: Veri ilişkisi sona erdiğinde gereksiz dış erişim ve kopyalar da sona erebilmelidir.**

Bir hizmetin veya sözleşmenin bitmesi sonrasında üçüncü tarafın aktif erişimi, eski dışa aktarımları veya gereksiz veri kopyaları yaşamaya devam etmemelidir. İdari sona erme gerçek veri davranışında karşılık bulmalıdır.

**İlke 30: Veri başka ortama taşındığında mahremiyet varsayımları yeniden değerlendirilmelidir.**

Test, geliştirme, analiz, destek veya farklı ülke ve hizmet ortamları verinin erişim ve kullanım koşullarını değiştirebilir. Kaynak sistemdeki korumalar yeni ortamda otomatik olarak devam ediyor varsayılmamalıdır.

**İlke 31: Loglar ve güvenlik verileri mahremiyetin dışında kabul edilmemelidir.**

Güvenlik amacıyla toplanan kayıtlar insanların davranışları, konumları ve çalışma alışkanlıkları hakkında ayrıntılı bilgi içerebilir. Güvenlik amacı, bu verinin ilgisiz kullanım veya sınırsız saklama için serbest hale gelmesini gerektirmez.

**İlke 32: Mahremiyet ile güvenlik birbirinin zorunlu karşıtı olarak tasarlanmamalıdır.**

Bazı güvenlik amaçları veri ve görünürlük gerektirir; ancak gereksiz veri toplamak da yeni güvenlik ve mahremiyet riski oluşturabilir. Tasarım, ihtiyaç duyulan güvenliği mümkün olan en sınırlı kişisel veri etkisiyle sağlamaya çalışmalıdır.

**İlke 33: Mahremiyet ihlali yalnızca verinin kuruluş dışına çıkması olarak görülmemelidir.**

Yetkisiz iç kullanım, yanlış kişiye ilişkin karar, amaç dışı işleme, gereksiz izleme veya verinin geri döndürülemeyecek biçimde açığa çıkarılması da önemli mahremiyet kaybı oluşturabilir. Etki yalnızca kaç kaydın dışarı sızdığıyla ölçülmemelidir.

**İlke 34: Mahremiyet modeli sistem ve kullanım değiştikçe yeniden anlamlandırılmalıdır.**

Yeni entegrasyonlar, analizler, yapay zekâ kullanımları, veri kaynakları veya iş amaçları aynı verinin insanlar üzerindeki etkisini değiştirebilir. Geçmişte uygun görülen veri davranışı yeni bağlamda otomatik olarak uygun sayılmamalıdır.

**İlke 35: Mahremiyet güvencesi gerçek veri yaşamı ve kullanımı üzerinden doğrulanabilmelidir.**

Mahremiyet bildirimi, rıza ekranı, veri envanteri veya politika tek başına güvence oluşturmaz. Hangi kişisel verinin gerçekte toplandığı, nerelerde bulunduğu, hangi amaçlarla ve kimler tarafından kullanıldığı, kimlerle paylaşıldığı ve ihtiyaç sona erdiğinde veri ile erişimin gerçekten sona erdirilip erdirilemediği gerektiğinde gösterilebilmelidir.