ISO 27000 AÇISINDAN ANONİMLEŞTİRİLMİŞ VERİ
Teknik Yöntemler, Standartlar, Yeniden Tanımlama Riski ve KVKK Uyumu

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@solutionhome.net
Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Anahtar Kelimeler: *Anonimleştirme • ISO 27559 • k-Anonymity • Pseudonymization • KVKK • GDPR • Yeniden Tanımlama*

ÖZET

Veri ekonomisinin ivmelenmesiyle birlikte kişisel verilerin korunması ve aynı zamanda değerli veri kümelerinin araştırma, istatistik ve yapay zeka amacıyla kullanılabilir kılınması arasındaki denge giderek stratejik bir meseleye dönüşmektedir. Anonimleştirme, bu dengeyi sağlamanın temel teknik mekanizmasını oluşturmaktadır: Kişisel veriden bireysel bağı kalıcı biçimde koparark veriyi kişisel veri statüsünden çıkarmak ve KVKK/GDPR yükümlülüklerini sona erdirmek. Bununla birlikte 'anonim veri' kavramının teknik gerçekliği, hukuki tanımından çok daha karmaşıktır: Yeniden tanımlama (re-identification) saldırıları, birleşik veri setleri ve yapay zeka modellerinin güçlenmesiyle birlikte teorik olarak anonimleştirilmiş veriler bile yeniden kişisel veri statüsüne kavuşabilmektedir. Bu derleme makale; ISO/IEC 27001:2022 kapsamındaki A.8.11 ve A.8.12 kontrollerini, ISO/IEC 20889:2018 terminoloji standartını, ISO/IEC 27559:2022 de-kimlik belirleme çerçevesini, ISO/IEC 29100:2024 gizlilik çerçevesini, k-anonymity ve differansiyel gizlilik (differential privacy) gibi temel teknik yöntemleri, yeniden tanımlama risk değerlendirme metodolojisini, KVKK'nın anonimleştirme yaklaşımını ve Türkiye'deki pratik uygulama boyutlarını kapsamlı biçimde incelemektedir.

Anahtar Kelimeler: *anonimleştirme, pseudonymization, takma adlaştırma, k-anonymity, l-diversity, t-closeness, differential privacy, ISO/IEC 27559, ISO/IEC 20889, ISO/IEC 29100, yeniden tanımlama, re-identification, veri maskeleme, KVKK, GDPR, bilgi güvenliği*

ABSTRACT

With the acceleration of the data economy, the balance between protecting personal data and making valuable data sets available for research, statistics, and artificial intelligence purposes is increasingly becoming a strategic issue. Anonymization is the primary technical mechanism for achieving this balance: permanently severing the individual link from personal data to remove it from personal data status and end KVKK/GDPR obligations. However, the technical reality of the concept of 'anonymous data' is far more complex than its legal

definition: With re-identification attacks, combined datasets, and strengthened AI models, theoretically anonymized data can reacquire personal data status. This review article comprehensively examines controls A.8.11 and A.8.12 within ISO/IEC 27001:2022, the ISO/IEC 20889:2018 terminology standard, the ISO/IEC 27559:2022 de-identification framework, the ISO/IEC 29100:2024 privacy framework, core technical methods such as k-anonymity and differential privacy, re-identification risk assessment methodology, KVKK's anonymization approach, and practical implementation dimensions in Turkey.

Keywords: *anonymization, pseudonymization, k-anonymity, l-diversity, t-closeness, differential privacy, ISO 27559, ISO 20889, ISO 29100, re-identification, data masking, KVKK, GDPR, information security*

1. Giriş

Veri, 21. yüzyılın en değerli kaynağı olarak tanımlanmakta; ancak bu değerin gerçekleştirilmesi büyük ölçüde verinin serbestçe paylaşılıp analiz edilebilmesine bağlıdır. Öte yandan kişisel verilerin korunması, hem uluslararası insan hakları hukukunun hem de ulusal mevzuatın güçlü güvencesi altındadır. Bu iki gereklilik arasındaki gerilimi çözmenin en köklü teknik yolu anonimleştirmedir: Veriyi bireysel kimlikle bağından koparark hem kişisel veri koruması kapsamının dışına çıkarmak hem de analitik kullanım değerini korumak.

ISO/IEC 27001:2022'nin Ek A'sında yer alan A.8.11 (Veri Maskeleme) kontrolü, anonimleştirme ve pseudonymization tekniklerini BGYS kontrol setine resmen dahil etmiştir. Bu durum, anonimleştirmenin artık yalnızca veri koruma hukukunun değil; bilgi güvenliği yönetiminin de ayrılmaz bir bileşeni olduğunu uluslararası düzeyde teyit etmektedir. ISO ailesi içinde ise 2022'de yayımlanan ISO/IEC 27559, veri de-kimlik belirleme için ilk kapsamlı çerçeve standardını sunmuştur.

Bununla birlikte, anonimleştirmenin hukuki ve teknik anlamı arasındaki derin uçurum giderek daha kritik bir sorun haline gelmektedir. Netflix Prize veri seti ifşası, AOL arama geçmişi de-anonimizasyonu ve sağlık verisi yeniden tanımlama davaları, 'anonimleştirilmiş' etiketinin gerçek bir güvence olmadığını somut biçimde ortaya koymuştur. Yapay zekanın yükselişi bu riski daha da artırmaktadır: Büyük dil modelleri ve makine öğrenmesi sistemleri, birden fazla anonimleştirilmiş kaynaktan bağımsız görünen bilgileri sentezleyerek bireysel profiller oluşturabilmektedir (APPA, 2025).

Bu makalenin amacı, ISO 27000 ailesi perspektifinden anonimleştirmenin teknik yöntemlerini, standartlarını, risk değerlendirme metodolojisini ve hukuki boyutlarını sistematik biçimde ele almaktır. Makale; kavramsal çerçeve, ISO standartları ailesi, teknik yöntemler, yeniden tanımlama riskleri, BGYS entegrasyonu, KVKK ve GDPR bağlamı, sektörel uygulamalar ve yapay zekanın yarattığı yeni tehditler başlıklarında yapılandırılmıştır.

2. Kavramsal Çerçeve: Temel Tanımlar ve Ayrımlar

2.1 Anonimleştirme, Pseudonymization ve Veri Maskeleme Farkı

Anonimleştirme, pseudonymization ve veri maskeleme kavramları pratikte sıklıkla birbirinin yerine kullanılmakla birlikte teknik ve hukuki açıdan köklü farklılıklar taşımaktadır. Bu

farkların doğru anlaşılması, hem teknik tasarım hem de hukuki uyumluluk açısından belirleyici öneme sahiptir.

Anonimleştirme (Anonymization): Kişisel verinin, ek bilgilerin kullanılması dahil hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. KVKK'nın (tarihsiz) tanımına göre, 'kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.' Başarılı anonimleştirme sonucunda veri, kişisel veri statüsünü yitirir ve KVKK/GDPR kapsamının dışına çıkar.

Pseudonymization (Takma Adlaştırma): Kişisel verinin, ek bilgi kullanılmaksızın artık belirli bir veri öznesine atfedilemeyeceği şekilde işlenmesidir. Polymer HQ'nun (2024) açıklamasına göre 'kimlik belirleme amacıyla kullanılabilecek bilgilerin, kişinin ek bilgi kullanılmadan tanımlanamayacağı bir takma adla değiştirilmesidir.' Kritik fark şudur: Pseudonymization geri döndürülebilirdir. Ek bilgiye (yeniden tanımlama anahtarına) erişim sağlandığında veri yeniden kişisel veri haline gelmektedir. Bu nedenle pseudonymization, GDPR ve KVKK kapsamında hâlâ kişisel veri işleme faaliyeti sayılmaktadır; yalnızca güvenlik önlemi olarak değer taşır.

Veri Maskeleme (Data Masking): Hassas verinin yalnızca görüntüsünün gizlenmesidir. SPIDYA'nın (2026) örneğiyle: Bir kredi kartı numarasının ilk ve son hanelerinin gösterilip ortasının yıldızlanması maskeleme örneğidir. Bu yaklaşım, belirli senaryolarda yeterli olmakla birlikte çoğu zaman verinin orijinal haline geri dönülebilmesi mümkündür. Maskeleme, KVKK'dan kurtarmaz; yalnızca tam anonimleştirme veriyi yasa kapsamından çıkarır (Nesil Teknoloji, 2026).

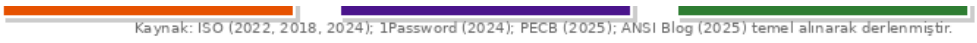
2.2 Quasi-Identifier ve Tanımlayıcı Kavramları

Anonimleştirme tasarımının merkezinde üç veri türü ayrımı yatmaktadır. Doğrudan tanımlayıcılar (direct identifiers), tek başına bir bireyi doğrudan tanımlayan veri öğeleridir: ad, soyad, TC kimlik numarası, pasaport numarası, e-posta adresi, telefon numarası. Bu öğelerin kaldırılması ya da dönüştürülmesi anonimleştirmenin zorunlu ilk adımıdır.

Quasi-identifier'lar (yarı tanımlayıcılar), tek başına tanımlayıcı olmayan ancak diğer verilerle birleştirildiğinde bireyin kimliğini açığa çıkaran öğelerdir. Yaş, cinsiyet, posta kodu, meslek ve hastalık türü bu kategorinin klasik örneklerini oluşturmaktadır. Sweeney'nin (1997) çarpıcı araştırması, posta kodu, cinsiyet ve doğum tarihi kombinasyonunun ABD nüfusunun yüzde seksenini benzersiz biçimde tanımladığını ortaya koymuştur. Bu bulgu, quasi-identifier tehlikesini somut biçimde göstermekte ve neden doğrudan tanımlayıcıların kaldırılmasının tek başına yeterli olmadığını açıklamaktadır (APPA, 2025).

Hassas nitelikler (sensitive attributes), korunması gereken ancak quasi-identifier olmayan bilgilerdir: hastalık türü, siyasi görüş, suç kaydı, dini inanç. Bu öğelerin gizliliği, anonimleştirme modelinin özellikle nitelik ifşası saldırılarına karşı korunmasını gerektirmektedir. k-Anonymity'nin sınırlılığı tam da bu noktada ortaya çıkmaktadır: Kimlik ifşasını önleyen k-anonymity, nitelik ifşasını engelleyememektedir.

3. ISO 27000 Ailesi: Anonimleştirme ile İlgili Standartlar



Şekil 1. *ISO 27000 Ailesi: Anonimleştirme ve Gizlilik ile İlgili Standartlar Haritası*

3.1 ISO/IEC 27001:2022 — A.8.11 Veri Maskeleme Kontrolü

ISO/IEC 27001:2022'nin Ek A'sında 2022 revizyonuyla eklenen A.8.11 Veri Maskeleme kontrolü, anonimleştirmeyi BGYS kontrol setinin resmi bir unsuru haline getirmiştir. Polymer HQ'nun (2024) aktarımına göre bu kontrol kapsamında 'verinizin gizlilik derecesine ve düzenleyici gereksinimlere göre veri maskeleme kurallarını ve erişim haklarını Bilgi Sınıflandırma Politikası, Erişim Kontrol Politikası ve Güvenli Geliştirme Politikasında belgelemeniz' tavsiye edilmektedir.

Kontrol kapsamındaki en yaygın teknikler şunlardır: Pseudonymization — kimlik belirleme amacıyla kullanılabilecek bilgilerin bir takma adla değiştirilmesi. Anonymization — verilerin kişiyi belirleyemez hale getirilmesi. Şifreleme — erişim kontrolü eşliğinde anahtara bağlı koruma. Obfuscation — veriyi kasıtlı olarak anlaşılması güç hale getirme. Bu teknikler arasında anonimleştirme ve pseudonymization, GDPR ve KVKK uyumu açısından en kritik olanlarıdır (Polymer HQ, 2024).

3.2 ISO/IEC 20889:2018 — Terminoloji ve Teknik Sınıflandırma

ISO/IEC 20889:2018, veri de-kimlik belirleme alanının terminoloji standardıdır ve ISO/IEC 27559:2022'nin temelini oluşturmaktadır. k2view'ın (2025) aktarımına göre standart 'veri anonimleştirme tekniklerini ve süreçlerini tanımlamakta; kuruluşların bireysel gizliliği korurken veri analizine ve paylaşımına olanak tanımasına yardımcı olmaktadır.'

Standart, anonimleştirme tekniklerini beş ana kategoride sınıflandırmaktadır: Bastırma (Suppression), Genelleştirme (Generalization), Rastgeleleştirme (Randomization), Takma Adlaştırma (Pseudonymization) ve Sentetik Veri Üretimi. Bu sınıflandırma, kuruluşların veri koruma amacına ve veri kullanım ihtiyacına göre doğru teknik kombinasyonunu seçmesine sistematik bir çerçeve sunmaktadır.

3.3 ISO/IEC 27559:2022 — De-Kimlik Belirleme Çerçevesi

ISO/IEC 27559:2022, 'Privacy Enhancing Data De-Identification Framework' başlığıyla anonimleştirme alanının ana çerçeve standardını oluşturmaktadır. IAPP'ın (2026) değerlendirmesine göre bu standart; 'de-kimlik belirleme sürecinde çeşitli riskleri tanımlamak ve bunları de-kimlik belirlenen verinin yaşam döngüsü boyunca azaltmak' amacıyla tasarlanmıştır.

Standart beş yıllık bir çalışma döneminin ürünüdür. IAPP'ın (2026) aktarımına göre 'dünyanın dört bir yanındaki rehberleri gözden geçiren bir çalışma dönemini, ISO/IEC 20889:2018 standardının temelini ve terminolojisini' kapsamaktadır. Standart; veri sorumlusu (custodian) ve veri alıcısı (data recipient) rolleriyle dört temel kullanım senaryosu tanımlamaktadır: İç kullanım (aynı organizasyon içinde), dış paylaşım (kontrollü ortamda), açık veri yayını (kamuya açık) ve araştırma paylaşımı (sözleşmeli üçüncü taraflarla).

APPA'nın (2025) kritik uyarısı özellikle dikkat çekicidir: 'ISO/IEC 27559, gizlilik yasalarına tabi bilgi (kişisel bilgi) ile kapsam dışı bilgi (anonimleştirilmiş bilgi) arasında katı ikili bir ayrım varsayımıyla yazılmıştır. İlk nesil gizlilik yasaları bu varsayımla çalışırken, daha modern gizlilik yasaları kişisel, 'de-kimlik belirlenen' ve anonimleştirilmiş bilgi arasında üçlü bir ayrım eğilimindedir.' Bu durum, ISO 27559 kapsamında 'anonimleştirilmiş' sayılan bilginin yerel mevzuat altında hâlâ pseudonymized (takma adlandırılmış) sayılabileceği anlamına gelmektedir.

3.4 ISO/IEC 29100:2024 — Gizlilik Çerçevesi

ISO/IEC 29100:2024, kişisel veri (PII) içeren herhangi bir sistem veya hizmet için uygulanabilen gizlilik çerçevesini tanımlamaktadır. ANSI Blog'un (2025) aktarımına göre standart, 'PII'nin kaldırılmasına duyulan ihtiyacı vurgulayan ve anonimleştirilmiş verinin yeniden kimlik belirlenmesini önleyecek şekilde gerçekleştirilmesine rehberlik eden' bir yapı sunmaktadır.

Standart, GDPR dahil pek çok gizlilik mevzuatıyla uyumlu gizlilik ilkelerini tanımlamaktadır. Bu ilkeler arasında Amaçla Sınırlılık (Purpose Limitation), Veri Minimizasyonu (Data Minimisation), Doğruluk, Depolama Sınırlaması ve Gizlilik Tasarımı (Privacy by Design) yer almaktadır. ISO/IEC 27701 ile entegre kullanıldığında ISO 27001 sertifikasını taşıyan kuruluşlar için KVKK/GDPR uyumunun teknik alt yapısını oluşturabilmektedir.

4. Temel Anonimleştirme Teknikleri

Kaynak: ISO/IEC 20889:2018; ISO/IEC 27559:2022; k2view.com (2025); Polymer HQ (2024) temel alınarak derlenmiştir.

Şekil 2. *ISO/IEC 20889:2018 Kapsamında Anonimleştirme Teknikleri Sınıflandırması*

4.1 Bastırma (Suppression)

Bastırma, verideki belirli alan veya değerlerin kaldırılmasıdır. Doğrudan tanımlayıcıların (ad, TC kimlik numarası, e-posta) veri setinden silinmesi en temel bastırma örneğini oluşturmaktadır. Daha gelişmiş bir bastırma biçimi olan kayıt bastırma (record suppression), belirli kriterleri karşılayan kayıtların — örneğin nadir hastalık tanısı alan bireylerin — veri setinden tamamen çıkarılmasıdır. Bu yöntem, küçük gruplara ait verilerin doğası gereği tanımlanabilir olduğu durumlarda uygulanır (ISO/IEC 20889:2018).

Bastırmanın temel sınırlılığı, verinin analitik değerini azaltmasıdır. Kayıt bastırma uygulandığında, veri setinin belirli alt grupları için istatistiksel geçerlilik tehlikeye girebilmektedir. Bu nedenle bastırma tek başına bir anonimleştirme yöntemi değil; diğer tekniklerle birleştirilen tamamlayıcı bir katman olarak değerlendirilmelidir.

4.2 Genelleştirme (Generalization)

Genelleştirme, spesifik değerlerin daha geniş kategorilerle değiştirilmesidir. Yaş değerinin (25) bir aralığa (20-30) dönüştürülmesi, posta kodunun son hanelerinin kaldırılması (34070 → 3407*) ve hastalık tanısının alt kategoriden üst kategoriye yükseltilmesi bu tekniğin yaygın

örneklerini oluşturmaktadır. Nesil Teknoloji'nin (2026) aktarımına göre 'değerleri genelleştirme (Yaş: 25 yerine Yaş: 20-30 aralığı)' KVKK uyumlu anonimleştirme yöntemleri arasında sayılmaktadır.

Genelleştirme, k-anonymity modelinin temel uygulama mekanizmasını oluşturmaktadır. Genelleştirme derecesi (granularity) ile anonimleştirme kalitesi arasında bir denge söz konusudur: Daha yüksek genelleştirme daha güçlü anonimlik sağlarken verinin analitik hassasiyetini düşürmektedir. Bu ödünleşimi yönetmek, anonimleştirme tasarımının en kritik mühendislik zorluklarından birini oluşturmaktadır.

4.3 Rastgeleleştirme (Randomization)

Rastgeleleştirme teknikleri, veriye istatistiksel gürültü ekleyerek ya da değerleri karıştırarak bireysel tanımlamayı güçleştirmektedir. Başlıca alt yöntemler şunlardır:

Gürültü Ekleme (Noise Addition): Sayısal değerlere küçük rastgele sapmalar eklenmektedir. Örneğin bir kişinin gelir bilgisine ±500 TL aralığında rastgele bir değer eklenerek gerçek değer gizlenmekte; ancak veri setinin istatistiksel dağılımı korunmaktadır. Differansiyel gizlilik (differential privacy), bu yaklaşımın matematiksel olarak güçlendirilmiş biçimini temsil etmektedir.

Permütasyon (Permutation): Hassas nitelik değerlerinin kayıtlar arasında rastgele yer değiştirmesidir. Örneğin bir veri setindeki maaş sütunundaki değerler başka bireylerle rastgele eşleştirilir; bu sayede maaş dağılımı korunurken kimlik-değer bağlantısı koparılır.

Veri Değiştirme (Data Swapping): Eşleştirilmiş bireylerin belirli nitelik değerlerinin birbiriyle takas edilmesidir. Coğrafi veri anonimleştirmesinde yaygın kullanılan bu teknik, istatistiksel marjinal dağılımları korurken bireysel değerleri örtmektedir.

4.4 Takma Adlaştırma (Pseudonymization)

Takma adlaştırma, doğrudan tanımlayıcıların tekrar tutarlı ama tanımlanamaz kodlarla değiştirilmesidir. SHA-256 gibi tek yönlü hash fonksiyonları, sembolik takma adlar veya şifreleme tabanlı tokenlar bu tekniğin araçlarını oluşturmaktadır. Deterministik pseudonymization — aynı girdi her zaman aynı takma adla eşleşir — bireylerin farklı veri setlerinde izlenmesine olanak tanır ve bu özelliği nedeniyle araştırma veri tabanlarında yaygın kullanım alanı bulur.

Pseudonymization'ın anonimleştirmeden temel farkı şudur: Orijinal verilerin anahtar veya eşleştirme tablosuyla yeniden birleştirilebilmesi mümkündür. Bu yapısal özellik, GDPR Madde 4(5)'te açıkça belirtilmiştir: Pseudonymize edilmiş veri, ek bilgiyle bir gerçek kişiye atfedilebileceğinden kişisel veri olmaya devam eder. Türkiye'de de KVKK kapsamında pseudonymization, anonimleştirme ile eşdeğer tutulmamakta; veri sorumlusunun yükümlülükleri devam etmektedir (Ersan Çetin, 2025).

4.5 Sentetik Veri Üretimi

Sentetik veri, gerçek bireylerden elde edilen birincil verinin istatistiksel özelliklerini koruyan ancak gerçek kişilerle hiçbir doğrudan bağlantı taşımayan yapay veri kümesidir. Üretici Çekişmeli Ağlar (Generative Adversarial Networks — GAN), Varyasyonel Oto-kodlayıcılar

(VAE) ve istatistiksel simülasyon modelleri bu alandaki başlıca üretim yöntemlerini oluşturmaktadır.

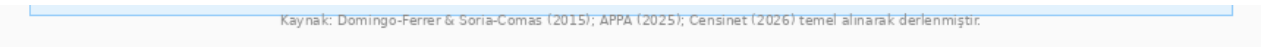
Naef ve diğerlerinin (2024) Cureus'ta yayımladığı dijital sağlık veri anonimleştirme çerçevesi, sentetik verinin hem büyük hem de küçük ölçekli veri setleri için uygulanabilirliğini analiz etmektedir. Sentetik verinin temel avantajı, re-identification saldırısı için kullanılabilecek gerçek kayıt bulunmamasıdır; temel sınırlılığı ise gerçek veriyle özdeş olmayan fidelity düzeyinin model eğitiminde ya da kritik karar destek sistemlerinde potansiyel sapmalara yol açmasıdır.

Tablo 1. *Anonimleştirme Tekniklerinin Karşılaştırmalı Değerlendirmesi*

Teknik	Geri Dönülebilirlik	Veri Kaybı	Analitik Değer	En Uygun Kullanım
Bastırma	Hayır	Yüksek	Azalır	Doğrudan tanımlayıcı kaldırma
Genelleştirme	Hayır	Orta	Korunur (kısmi)	k-Anonymity uygulamasi, veri paylaşımı
Gürültü Ekleme	Hayır	Düşük	Yüksek korunur	İstatistiksel yayınlar, AI eğitimi
Pseudonymization	Evet (anahtarla)	Yok	Tam korunur	Araştırma, klinik takip, loglama
Sentetik Veri	Hayır	Yok (yapay)	Yüksek (model bağımlı)	AI/ML eğitimi, test ortamları
Differential Privacy	Hayır	Düşük	Yüksek korunur	Büyük veri istatistikleri, AI

Not. Kaynak: ISO/IEC 20889:2018; Polymer HQ (2024); Censinet (2026); Naef et al. (2024) temel alınarak derlenmiştir.

5. k-Anonymity, l-Diversity, t-Closeness ve Differansiyel Gizlilik



Şekil 3. *k-Anonymity: Kavramsal Örnek — k=3 Uygulaması ile Anonimleştirme*

5.1 k-Anonymity: Temel Model ve Sınırlılıkları

k-Anonymity, 1998 yılında Latanya Sweeney tarafından geliştirilen ve bugün hâlâ en yaygın kullanılan anonimleştirme modelidir. Temel ilkesi şudur: Bir veri setinde her kayıt, quasi-identifier değerleri açısından en az (k-1) başka kayıtla özdeş olmalıdır. Bu koşul sağlandığında, bir bireyin kimliğini doğrudan tanımlamak en az k kayıt adayı arasından seçim yapmayı gerektirmekte; bu da re-identification olasılığını en fazla 1/k'ya indirmektedir.

Censinet'in (2026) aktarımına göre k-Anonymity, 'ISO/IEC 27559 ve ISO/IEC 20889 gibi uluslararası standartlar tarafından giderek artan biçimde atıfta bulunulmakta' ve GDPR'ın kişisel olmayan veri tanımıyla uyumluluk için kullanılabilmektedir. Bununla birlikte k-Anonymity'nin iki yapısal sınırlılığı vardır.

Homojenlik Saldırısı: k kişinin aynı quasi-identifier değerlerini paylaştığı bir grupta tüm bireyler aynı hassas niteliği taşıyorsa (örneğin tümü aynı hastalığa sahipse), saldırgan quasi-identifier bilgisinden hassas niteliği doğrudan çıkarabilir. Bu durum, kimlik gizlenmiş olsa bile nitelik ifşasına yol açmaktadır.

Arka Plan Bilgisi Saldırısı: Saldırganın hedef birey hakkında bağlamsal bilgiye sahip olduğu durumda k-anonymity koruması çökmektedir. Örneğin 'Ahmet'in bu veri setinde olduğunu biliyorum' ve 'bu gruptaki tüm kişiler kanser hastası' bilgilerini birleştiren bir saldırgan, doğrudan kimlik ifşası olmaksızın hassas niteliğe ulaşmaktadır.

5.2 l-Diversity: Homojenlik Saldırısına Yanıt

l-Diversity, k-anonymity'nin homojenlik saldırısı açığını kapatmak amacıyla Machanavajjhala ve diğerleri (2007) tarafından geliştirilmiştir. Model şu ek koşulu getirmektedir: Her quasi-identifier grubunda hassas nitelik açısından en az l adet 'iyi temsil edilmiş' farklı değer bulunmalıdır. Pratik olarak bu, bir gruptaki tüm bireylerin aynı hastalık, siyasi görüş ya da gelir düzeyine sahip olamayacağı anlamına gelmektedir.

l-Diversity de sınırlılıktan muaf değildir. En belirgin sorun, veri setindeki hassas niteliğin genel dağılımının (background distribution) çarpık olduğu durumlarda ortaya çıkmaktadır. Örneğin belirli bir hastalığın nüfusda yüzde bir oranında görüldüğü bilinen bir bağlamda, hastane veri setindeki yüzde yirmi oranı bile arka plan bilgisi ile birleştirildiğinde nitelik çıkarsamasına zemin hazırlamaktadır. Bu sorun t-closeness modeline yol açmıştır.

5.3 t-Closeness: Dağılım Güvencesi

t-Closeness, Li ve diğerleri (2007) tarafından geliştirilmiş olup her quasi-identifier grubundaki hassas niteliğin dağılımının, tüm veri setindeki genel dağılımdan en fazla t mesafesiyle farklılaşabileceğini zorunlu kılmaktadır. Domingo-Ferrer ve Soria-Comas'ın (2015) çalışması, t-closeness ile ε-differansiyel gizlilik arasındaki güçlü ilişkiyi matematiksel olarak ortaya koymuştur: 'ε-diferansiyel gizlilik gerektirir, ancak k-anonymity gerektirmez' şeklinde ifade edilebilecek bu ilişki, iki modelin tamamlayıcı nitelik taşıdığını göstermektedir.

5.4 Differansiyel Gizlilik (Differential Privacy)

Differansiyel gizlilik (DP), Dwork (2006) tarafından geliştirilen ve bugün matematiksel açıdan en güçlü gizlilik garantisi olarak kabul gören modeldir. Temel sezgisi şudur: Belirli bir bireyin veri setine dahil olup olmaması, istatistiksel çıktıyı ε parametresiyle kontrol edilen küçük bir ölçüde değiştirmelidir. Bu sayede hiç kimse, sonuçları inceleyerek belirli bir bireyin veri setinde olup olmadığını güvenilir biçimde çıkarsamaz.

Censinet'in (2026) aktarımına göre Differansiyel Gizlilik 'verilere matematiksel olarak re-identification risklerini sınırlayan gürültü ekler.' Apple, Google ve Meta gibi büyük teknoloji şirketleri DP'yi ürün istatistiklerinin toplanmasında fiilen uygulamaktadır. Apple, iOS 14'ten itibaren kullanım istatistiklerini DP ile toplamakta; Google'ın RAPPOR sistemi de DP tabanlı istemci tarafı gizlilik koruması uygulamaktadır. ABD Nüfus Sayım Birimi, 2020 sayımında nüfus istatistiklerini yayımlamak için DP metodolojisini benimsemiştir.

DP'nin en kritik avantajı, k-anonymity'nin aksine bağlamsal saldırılara karşı matematiksel güvence sunmasıdır: Saldırganın sahip olduğu arka plan bilgisinden bağımsız olarak ε parametresiyle kontrol edilen bilgi sızıntısının üst sınırı belirlenir. DP'nin uygulamadaki zorluğu ise ε-gizlilik bütçesinin doğru ayarlanmasıdır: Çok küçük ε aşırı gürültüye; çok büyük ε ise yetersiz gizlilik güvencesine yol açmaktadır.

6. Yeniden Tanımlama (Re-Identification) Riski



Şekil 4. *Yeniden Tanımlama Risk Matrisi: Olasılık × Etki (ISO/IEC 27559:2022 Çerçevesi)*

6.1 Tarihsel Yeniden Tanımlama Vakaları

Teorik olarak anonimleştirilmiş veri setlerinin yeniden tanımlandığı vakalar, bu tehdidin somut bir gerçekliğe karşılık geldiğini kanıtlamaktadır.

Netflix Prize (2007): Netflix, film öneri algoritması geliştirmek amacıyla 500.000 abonesine ait derecelendirme verilerini anonimleştirerek yayımladı. Araştırmacılar Narayanan ve Shmatikoff, IMDb'nin kamuya açık değerlendirmeleriyle Netflix verisini çapraz karşılaştırarak kullanıcıların önemli bir bölümünü yeniden tanımladı. Bu vaka, quasi-identifier'ların farklı kaynaklardan birleştirilebildiğinde nasıl dramatik biçimde güçlendiğini gösteren kritik bir referans noktası haline gelmiştir.

AOL Arama Geçmişi (2006): AOL, araştırma amacıyla 650.000 kullanıcıya ait arama geçmişini yayımladı. Kullanıcı adları kaldırılmış; yalnızca sayısal ID'ler kullanılmıştı. New York Times gazetecileri, arama içerikleri ve coğrafi referansları analiz ederek kullanıcılar 4417749 ve 927 gibi vakaları yeniden tanımladı. Bu vaka; 'isim yoksa tanımlanamaz' varsayımının ne denli yanıltıcı olduğunu göstererek bilgi mahremiyeti hukukunun gündemini kalıcı olarak değiştirmiştir.

6.2 ISO/IEC 27559 Risk Değerlendirme Metodolojisi

ISO/IEC 27559:2022, yeniden tanımlama riskini sistematik biçimde değerlendirmek için beş faktörlü bir çerçeve sunmaktadır: Motivasyon — olası saldırganın yeniden tanımlama için ne kadar güçlü motivasyonu var? Araç — saldırganın erişebileceği ek veri kaynakları ve hesaplama kapasitesi nedir? Fırsat — veri nasıl yayımlanıyor, kim erişebiliyor? Veri hassasiyeti — yeniden tanımlama başarılı olursa ne ölçüde zarar oluşur? Kapsam — kaç kişi etkilenebilir? (IAPP, 2026).

Bu beş faktörün değerlendirilmesi, yeniden tanımlama riskinin iki boyutunu — olasılık ve etki — sistematik biçimde tahmin etmeyi mümkün kılmaktadır. Risk yönetimi açısından kritik nokta, bu değerlendirmenin tek seferlik değil; veri yayım koşullarındaki değişiklikler ve yeni saldırı tekniklerinin gelişimine paralel olarak dönemsel şekilde yenilenmesidir.

6.3 Bağlantı Saldırıları ve Yapay Zeka Tehdidi

Bağlantı saldırıları (linkage attacks), saldırganın birden fazla anonimleştirilmiş veri setini dış bilgiyle birleştirerek bireyleri yeniden tanımladığı saldırı kategorisidir. Bu saldırıların iki temel

biçimi bulunmaktadır: Kayıt bağlantısı (record linkage) — iki farklı veri setindeki kayıtların aynı bireye ait olduğunun saptanması. Nitelik bağlantısı (attribute linkage) — kayıt düzeyinde tanımlama yapmaksızın bir bireye ait hassas niteliği çıkarsama.

Yapay zeka ve büyük veri teknolojilerinin bu alandaki etkisi, geleneksel re-identification tehditini niteliksel olarak dönüştürmektedir. APPA'nın (2025) uyarısına göre: 'ISO/IEC 27559, birinci nesil gizlilik yasalarının katı ikili ayrımıyla çalışmaktadır; ancak modern gizlilik yasaları daha esnek üçlü bir ayrım eğilimindedir. Bu farklılık, ISO 27559 kapsamında anonimleştirilmiş sayılan verinin yerel mevzuat altında hâlâ pseudonymized sayılabileceği anlamına gelmektedir.'

Büyük dil modellerinin (LLM) eğitim verisi bağlamında bu risk özellikle kritik hale gelmektedir: Nesil Teknoloji'nin (2026) tespitine göre 'yapay zeka promptlarına girilen veriler, anonimleştirilmediyse veri ihlali sayılabilir.' Bu uyarı, yapay zeka platformlarının kuruluşlarda yaygınlaşmasıyla birlikte BGYS kapsamındaki veri maskeleme ve anonimleştirme kontrollerinin neden stratejik öncelik taşıdığını somutlaştırmaktadır.

7. ISO 27001:2022 BGYS'ye Entegrasyon: Pratik Uygulama

7.1 A.8.11 Kontrolünün Uygulanması

A.8.11 Veri Maskeleme kontrolünün BGYS çerçevesinde etkin biçimde uygulanması için Polymer HQ'nun (2024) önerisi şöyledir: 'Veri maskeleme kurallarını ve erişim haklarını Bilgi Sınıflandırma Politikası, Erişim Kontrol Politikası ve Güvenli Geliştirme Politikasında belgelemeniz tavsiye edilir.' Bu belgeleme yükümlülüğü, anonimleştirme kararlarının sistematik ve denetlenebilir biçimde alınmasını güvence altına almaktadır.

Pratik uygulama adımları şöyle sıralanabilir: Varlık envanterindeki bilgi varlıklarının kişisel veri içerip içermediğinin sınıflandırılması. Her varlık için re-identification risk düzeyinin belirlenmesi. Risk düzeyine göre uygun anonimleştirme veya pseudonymization tekniğinin seçilmesi. Seçilen tekniğin uygulanması ve etkinliğinin doğrulanması. Anonimleştirme kararlarının Uygulanabilirlik Bildirgesi (SoA) ile ilişkilendirilmesi.

7.2 A.8.12 Veri Sızıntısı Önleme (DLP) ile Sinerjisi

A.8.11 Veri Maskeleme ve A.8.12 Veri Sızıntısı Önleme (DLP) kontrolleri, birbirini tamamlayan savunma katmanları oluşturmaktadır. Anonimleştirme, verinin kişisel veri statüsünden çıkmasını sağlarken DLP, bu kararı geçersiz kılabilecek yetkisiz veri ifşasını engeller. Bu iki kontrolün entegre tasarımı; anonimleştirme öncesi veri sızdırılmasının önlenmesini ve anonimleştirme sonrası yeniden kişisel veriye dönüşebilecek ham veriye erişimin kısıtlanmasını sağlar.

7.3 Risk Değerlendirmesi ve SoA'ya Yansıtma

Anonimleştirme kararlarının BGYS risk değerlendirmesi ve Uygulanabilirlik Bildirgesi'ne entegrasyonu için önerilen yaklaşım şöyledir: Varlık envanterinde kişisel veri içeren tüm varlıklar için ayrı risk girdisi oluşturulmalıdır. Her giriş için re-identification riski, ISO/IEC 27559'un beş faktörlü değerlendirme çerçevesi kullanılarak puanlanmalıdır. Risk işleme

planında seçilen anonimleştirme tekniği ve bu tekniğin riski nasıl azalttığı belgelenmelidir. SoA'da A.8.11 kontrolünün uygulanabilir olup olmadığı ve uygulanıyorsa hangi varlıklar ve teknikler için geçerli olduğu açıklanmalıdır.

Tablo 2. *BGYS Risk Değerlendirmesinde Anonimleştirme Karar Matrisi*

Veri Türü	Re-ID Risk	Önerilen Teknik	İzleme Sıklığı	Standart Referans
Sağlık verisi	**KRİTİK**	k-anon (k≥5) + DP + Bastırma	Her yayımda yeniden değerlendir	ISO 27559 + HIPAA
Lokasyon verisi	YÜKSEK	Genelleştirme + gürültü ekleme	3 ayda bir	ISO 27559:2022
Finansal veri	**YÜKSEK**	Pseudonymization + DLP	Sürekli (otomasyon)	ISO 27001 A.8.11
Davranışsal veri	ORTA	k-anonymity (k≥3) + maskeleme	6 ayda bir	ISO 20889:2018
Demografik istatistik	DÜŞÜK	Genelleştirme + bastırma	Yıllık	KVKK Rehberi (2018)
AI eğitim verisi	**YÜKSEK**	Differential Privacy veya Sentetik	Sürekli	ISO 27559 + GDPR

Not. Kaynak: ISO/IEC 27559:2022; Censinet (2026); Polymer HQ (2024); KVKK (tarihsiz) temel alınarak derlenmiştir.

8. Türk Hukuku ve GDPR Bağlamında Anonimleştirme

8.1 KVKK'nın Anonimleştirme Tanımı ve Gereksinimleri

6698 sayılı Kişisel Verilerin Korunması Kanunu, anonimleştirmeyi şöyle tanımlamaktadır: 'Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir' (KVKK, tarihsiz). Bu tanım, GDPR ile örtüşmekle birlikte 'başka verilerle eşleştirilse dahi' ifadesi, bağlantı saldırılarının da dikkate alınmasını açıkça gerektirmekte; dolayısıyla salt doğrudan tanımlayıcı kaldırma yöntemlerinin yetersiz olduğunu ortaya koymaktadır.

KVKK'nın Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, kuruluşların anonimleştirme sürecinde uygulaması gereken teknik ve idari tedbirleri kapsamlı biçimde ele almaktadır. Ersan Çetin'in (2025) aktarımına göre bu rehber kapsamındaki başlıca anonimleştirme teknikleri şunlardır: Değer genelleştirme, maskeleme, toplulaştırma (aggregation) ve k-anonymity. Rehberin önemi, bu teknikler arasında hiyerarşik bir sıralama yerine duruma göre uygun tekniğin seçilmesini zorunlu kılan risk bazlı yaklaşımı benimsemesinden kaynaklanmaktadır.

Anonimleştirmenin hukuki sonucu belirgindir: Veri anonim hale geldiği anda, artık kişisel veri vasfını yitirir ve KVKK hükümleri — aydınlatma yükümlülüğü, açık rıza, saklama süresi — uygulanmaz hale gelir (Nesil Teknoloji, 2026). TÜİK'in yayımladığı istatistikler bu uygulamanın en doğal örneğidir. Bu hukuki geçiş, verinin yeniden kullanılabilmesi ve

paylaşılabilmesi açısından son derece değerli; ancak bu geçişin teknik geçerliliğinin hukuki belirlilikle çelişmeyen bir sağlamlıkta kurgulanması zorunludur.

8.2 GDPR ve AB Hukukundaki Gelişmeler

GDPR'ın Recital 26'sı, anonim bilginin GDPR kapsamı dışında kaldığını açıkça belirtmektedir. Bununla birlikte AB 29. Madde Çalışma Grubu (WP29) ve halefi EDPB, anonimlik standardını son derece yüksek tutmaktadır. WP29'un 05/2014 Opinyonu, k-anonymity'nin tek başına GDPR anlamında anonimlik güvencesi için yeterli olmayabileceğini; çünkü bağlantı saldırıları karşısında kırılgan kaldığını vurgulamaktadır.

AB Yapay Zeka Yönetmeliği (AI Act), anonimleştirme standardını yapay zeka sistemleri bağlamında yeni bir boyuta taşımaktadır. Yüksek riskli AI sistemlerinde kullanılan eğitim veri setlerinin kişisel veri içermemesi ya da kişisel verinin yeterince anonimleştirilmiş olması zorunluluğu, ISO 27559'un A.8.11 BGYS kontrolüyle entegre uygulanmasını kaçınılmaz kılmaktadır. 1Password'ün (2024) aktardığına göre ISO 27000 serisi 'GDPR yürürlüğe girmeden önce hazırlanmış olmakla birlikte, kapsamlı mevzuatın bilgi güvenliği yönetim sistemleri için uluslararası standartlara yeni değer biçmesine neden olmuştur.'

8.3 Pseudonymization'ın KVKK ve GDPR'daki Yeri

Her iki mevzuatta da pseudonymization, anonimleştirmeden keskin biçimde ayrılmaktadır. GDPR Madde 4(5), pseudonymize verinin 'ek bilgi kullanılarak belirli bir gerçek kişiye atfedilebileceği' için kişisel veri olmaya devam ettiğini hükme bağlamaktadır. Türk hukukunda da KVKK kapsamındaki anonim hale getirme tanımının geri döndürülemezlik koşulunu içermesi, pseudonymization'ı bu koşulu karşılayamaz kılmaktadır.

Bununla birlikte pseudonymization, her iki mevzuatta da güvenlik tedbiri olarak tanınmaktadır. GDPR Madde 32, uygun güvenlik seviyesini sağlamak için alınabilecek teknik tedbirler arasında pseudonymization'ı açıkça saymaktadır. Bu düzenleme, pseudonymization'ı anonimleştirmenin alternatifi değil; anonimleştirme yapılmayan durumlarda veri güvenliğini artıran tamamlayıcı bir koruma katmanı olarak konumlandırmaktadır.

9. Sektörel Uygulamalar ve Örnek Senaryolar

9.1 Sağlık Sektörü

Sağlık verisi, anonimleştirmenin hem en kritik hem de en zorlu uygulama alanını oluşturmaktadır. Hasta kayıtları; demografik bilgiler, tanı kodları, ilaç reçeteleri ve genetik verinin kesişiminde son derece yüksek re-identification riski barındırmaktadır. Naef ve diğerlerinin (2024) dijital sağlık uygulamaları için geliştirdiği pratik anonimleştirme çerçevesi, literatürdeki en kapsamlı sektörel rehberlerden birini sunmaktadır.

Sağlık verisi anonimleştirmesinde öne çıkan yaklaşım, doğrudan tanımlayıcı bastırma (ad, TC kimlik numarası, sigorta numarası kaldırma) ile k-anonymity genelleştirmesinin (yaş aralıklarına dönüştürme, posta kodu kısaltma) kombinasyonudur. Özellikle nadir hastalıklar söz konusu olduğunda bu kombinasyon yeterli olmayabilmekte; ek bastırma ya da differential privacy gürültüsü gerekebilmektedir. Censinet'in (2026) aktarımına göre bu teknikler 'HIPAA

de-identification standartları ve GDPR odaklı anonimleştirme kurallarıyla uyumlu' biçimde uygulanabilmektedir.

9.2 Finans Sektörü

Finans sektöründe anonimleştirme ihtiyacı birkaç temel kullanım senaryosundan kaynaklanmaktadır: Akademik araştırma amaçlı işlem verisi paylaşımı, dolandırıcılık tespiti algoritmaları geliştirmek için anonimleştirilmiş işlem geçmişinin üçüncü taraflarla paylaşılması ve düzenleyici raporlamada bireyleri gizleme zorunluluğu.

Finansal verinin re-identification riski, işlem tutarlarının ve zaman damgalarının quasi-identifier işlevi görmesinden kaynaklanmaktadır. ODYA'nın (2026) aktarımına göre: 'Anonimleştirme; KVKK, GDPR ve benzeri düzenlemelerle uyumlu veri süreçleri oluşturmak kritik. Veri anonimleştirme aracı bu uyumu kolaylaştırır.' Finans kuruluşları için önerilen yaklaşım, kural tabanlı pseudonymization (müşteri ID tokenizasyonu) ile istatistiksel aggregation'ın birleşimidir.

9.3 Yapay Zeka ve Büyük Veri Bağlamı

Makine öğrenmesi modellerinin eğitimi, anonimleştirmenin yeni ve kritik bir kullanım alanını oluşturmaktadır. Geleneksel anonimleştirme yaklaşımları, büyük veri kümelerinden model eğitirken ortaya çıkan gizlilik tehditlerini tam olarak ele alamamaktadır. Özellikle derin öğrenme modelleri, eğitim verilerini 'ezberleyebilmekte' ve bu ezber, modele sorgulama yoluyla erişildiğinde bireysel verilerin kısmen yeniden elde edilmesine olanak tanıyabilmektedir — bu saldırı türü 'model inversion attack' olarak bilinmektedir.

Differential Privacy, bu tehdidin matematiksel karşı tedbiri olarak öne çıkmaktadır. DP ile eğitilen modeller, bireysel eğitim örüntüleri yerine genel dağılımı öğrenmekte; bu sayede model inversion saldırılarının bilgi kazanımı ε parametresiyle sınırlandırılmaktadır. Apple, Google ve Meta'nın DP'yi prodüksiyon sistemlerinde benimsemesi, bu yaklaşımın yalnızca akademik değil kurumsal ölçekte de uygulanabilir olduğunu kanıtlamaktadır.

10. Zorluklar, Açık Sorunlar ve Öneriler

10.1 Fayda-Gizlilik Ödünleşimi

Anonimleştirmenin en temel gerilimi, gizlilik koruması ile verinin analitik faydasının ters orantılı ilişkisidir. Daha güçlü anonimleştirme, daha fazla bilgi kaybı anlamına gelir; bu ise verinin istatistiksel geçerlilik ve model doğruluğunu tehlikeye atabilir. Bu ödünleşimi optimize etmek, hem teknik hem de kurumsal yönetim kararları gerektirmektedir.

ISO/IEC 27559'un yaklaşımı bu ödünleşimi kullanım senaryosu odaklı çözmektedir: Hangi kullanım amacı için hangi gizlilik düzeyi yeterlidir? Genel istatistiksel yayın için k=3 yeterli olabilirken, genetik araştırma için k≥100 ya da differential privacy zorunlu olabilir. Bu sorunun yanıtı, teknik değil etik ve kurumsal politika düzeyinde verilmek zorundadır.

10.2 Metodolojik Standartlaşma Eksikliği

Mevcut anonimleştirme uygulamalarının en kritik sorunu, metodoloji standartlaşmasının yetersizliğidir. PubMed literatür araştırmasına dayanan Naef ve diğerlerinin (2024) tespitine göre, anonimleştirme üzerine yayımlanan çalışmalar son derece heterojen metodolojiler kullanmakta ve çoğu çalışma ISO 27000'in tanımladığı temel güvenlik özelliklerinden bir ya da birkaçını açıklamamaktadır. Bu tutarsızlık, yöntemlerin karşılaştırılmasını ve düzenleyici denetimini zorlaştırmaktadır.

10.3 Politika Önerileri

Uluslararası uygulamalar ve literatür ışığında aşağıdaki politika önerileri sunulmaktadır:

- **ISO 27559 benimseyin:** Tüm veri de-kimlik belirleme kararları, ISO/IEC 27559:2022'nin beş faktörlü risk değerlendirme çerçevesi esas alınarak belgelenmelidir.
- **Tek teknik yeterli değil:** Anonimleştirme politikası, birden fazla tekniğin katmanlı uygulanmasını öngörmelidir; yalnızca doğrudan tanımlayıcı kaldırma kesinlikle yetersizdir.
- **Yeniden değerlendirme döngüsü:** Veri yayım koşullarındaki değişiklikler ve yeni saldırı teknikleri gözetilerek re-identification riski düzenli aralıklarla yeniden değerlendirilmelidir.
- **AI eğitim verisi için DP:** Makine öğrenmesi modeli eğitiminde kişisel veri kullanılması kaçınılmazsa, differential privacy tekniği uygulanmalı ya da sentetik veri üretimi tercih edilmelidir.
- **BGYS kapsamına dahil edin:** Anonimleştirme süreçleri, ISO 27001 A.8.11 çerçevesinde BGYS risk değerlendirmesine ve SoA'ya sistematik olarak yansıtılmalıdır.
- **Pseudonymization ≠ Anonimleştirme:** Pseudonymization'ı anonimleştirme ile eşdeğer tutan hatalı uygulamalar, kurumsal KVKK/GDPR uyum politikaları aracılığıyla giderilmelidir.

11. Sonuç

Anonimleştirme, veri ekonomisinin en kritik kavşaklarından birinde konumlanmaktadır: Kişisel verilerin korunması ile bu verilerin bilimsel ve ticari değerinin gerçekleştirilmesi arasındaki gerilimin en teknik çözüm noktasında. ISO/IEC 27001:2022'nin A.8.11 kontrolü, bu teknik çözümü bilgi güvenliği yönetiminin resmi kontrollerine ekleyerek anonimleştirmeyi BGYS'nin ayrılmaz bir bileşeni haline getirmiştir.

ISO/IEC 27559:2022 ve ISO/IEC 20889:2018, bu alandaki metodoloji boşluğunu doldurmayı hedefleyen kapsamlı standartları temsil etmektedir. Bununla birlikte APPA'nın (2025) uyarısı önemini korumaktadır: Bu standartlar, katı ikili ayrım (kişisel / anonim) varsayımıyla yazılmıştır; oysa modern gizlilik hukukları üçlü bir kategorizasyona yönelmektedir. Bu yapısal boşluk, ISO standartlarına uyumun yerel mevzuat uyumunu otomatik olarak sağladığı yanılgısının yaratılmamasını zorunlu kılmaktadır.

Teknik cephede ise k-anonymity'den differential privacy'ye uzanan model çeşitliliği, farklı kullanım senaryoları için farklı güvenlik garantileri sunmaktadır. Yapay zekanın model inversion saldırıları ve büyük dil modellerinin veri ezberleme kapasitesi, geleneksel

anonimleştirme çerçevelerini zorlamaktadır. Differential privacy'nin matematiksel güvencesi ve sentetik verinin yükselen uygulanabilirliği, bu zorluğa en umut verici teknik yanıtları oluşturmaktadır.

Türkiye bağlamında KVKK'nın anonimleştirme tanımı, 'başka verilerle eşleştirilse dahi' ifadesiyle bağlantı saldırılarına karşı güçlü bir standart belirlemiştir. Bu standardın pratikte karşılanabilmesi için ISO/IEC 27559 risk değerlendirme çerçevesinin KVKK Rehberi ile entegre uygulanması ve BGYS A.8.11 kontrolünün kurum politikalarına sistematik biçimde yansıtılması gereklidir. Veri ekonomisinde Türkiye'nin rekabetçi konumunu sürdürmesi açısından bu teknik-hukuki uyum kapasitesinin geliştirilmesi, hem özel sektör hem de kamu kurumları için öncelikli bir gündem maddesi olmaya devam etmektedir.

Kaynakça

1Password. (2024, August 30). What you need to know about ISO 27000 standards. https://blog.1password.com/what-you-need-to-know-about-iso-27000-standards

ANSI Blog. (2025, November 6). ISO/IEC 27701:2025 — Privacy information management systems. https://blog.ansi.org/ansi/iso-iec-27701-2025-privacy-management-systems/

APPA Technology Working Group. (2025). Guide to getting started with anonymisation. Office of the Australian Information Commissioner. https://www.pcpd.org.hk/english/resources_centre/publications/files/appa_anonymisation_guide072025.pdf

Censinet. (2026, January 1). Top frameworks for GDPR data de-identification. https://censinet.com/perspectives/top-frameworks-gdpr-data-de-identification

Domingo-Ferrer, J., & Soria-Comas, J. (2015). From t-closeness to differential privacy and vice versa in data anonymization. Knowledge-Based Systems, 74, 151–158. https://arxiv.org/pdf/1512.05110

Ersan Çetin, A. (2025, March 15). KVKK: Veri silme ve anonimleştirme. https://ersancetin.av.tr/makaleler/kvkk-silme-anonimlestime/

IAPP. (2026, February 17). A new standard for anonymization. International Association of Privacy Professionals. https://iapp.org/news/a/a-new-standard-for-anonymization

ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques. International Organization for Standardization.

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

ISO/IEC 27559:2022. Information security, cybersecurity and privacy protection — Privacy enhancing data de-identification framework. International Organization for Standardization.

ISO/IEC 29100:2024. Information technology — Security techniques — Privacy framework. International Organization for Standardization.

k2view. (2025, April 24). Complying with today's data anonymization standards. https://www.k2view.com/blog/data-anonymization-standards/

KVKK. (tarihsiz). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi. Kişisel Verileri Koruma Kurumu. https://www.kvkk.gov.tr/Icerik/2038

KVKK. (2018). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi. Kişisel Verileri Koruma Kurumu.

Naef, A., Coduti, E., & Windisch, P. Y. (2024). The anonymous data warehouse: A hands-on framework for anonymizing data from digital health applications. Cureus, 16(4), e57519. https://doi.org/10.7759/cureus.57519

Nesil Teknoloji. (2026, February 6). Kişisel veri nedir? KVKK'ya göre tanım, örnekler ve sınırlar. https://www.nesilteknoloji.com/kisisel-veri-nedir-kvkk-tanim-ornekler-sinirlar/

ODYA. (2026, February 3). Veri anonimleştirme aracı: Hassas verileri gizleyin! https://odya.com.tr/blog/veri-anonimlestirme-araci-kvkk-gdpr-uyumlu-hassas-veri-koruma/

PECB. (2025, July 8). The future of privacy with ISO/IEC 27701. https://pecb.com/en/whitepaper/the-future-of-privacy-with-isoiec-27701

Polymer HQ. (2024, September 6). What is changing in ISO 27001 with 2022 updates? https://www.polymerhq.io/blog/iso-27001/what-is-changing-in-iso-27001-with-2022-updates/

Reisman, D., & Nissim, K. (2019). Towards formalizing the GDPR's notion of singling out. arXiv preprint arXiv:1904.06009. https://arxiv.org/pdf/1904.06009

SPIDYA. (2026). Veri anonimleştirme aracı. https://odya.com.tr/blog/veri-anonimlestirme-araci-kvkk-gdpr-uyumlu-hassas-veri-koruma/

Sweeney, L. (1997). Guaranteeing anonymity when sharing medical data: The Datafly system. Proceedings of the AMIA Annual Fall Symposium, 51–55.

Vries, M. de, & Oprescu, A. (2023). Energy cost and machine learning accuracy impact of k-anonymisation and synthetic data techniques. arXiv preprint arXiv:2305.07116. https://arxiv.org/pdf/2305.07116

Wagner, I., & Eckhoff, D. (2019). Technical privacy metrics: A systematic survey. ACM Computing Surveys, 51(3), Article 57. https://doi.org/10.1145/3168389

Wikipedia. (2026). ISO/IEC 27000. https://en.wikipedia.org/wiki/ISO/IEC_27000