BİLGİ DÜNYASI
INFORMATION WORLD

e-ISSN: 2148-354X

# Üniversitelerde İş Süreçlerinin Bir Parçası Olarak Veri Yönetişimi Politikalarının Karşılaştırmalı Değerlendirilmesi

## *Comparative Assessment of Data Governance Policies as Part of Business Processes in Universities*

Burcu TIĞ DEMİR, Özgür KÜLCÜ

**Makale Bilgisi / *Article Information***
**Bu makaleye atıf yapmak için *To cite this article:***
Tığ Demir, B. ve Külcü, Ö. (2025). Üniversitelerde iş süreçlerinin bir parçası olarak veri yönetişimi politikalarının karşılaştırmalı değerlendirilmesi. *Bilgi Dünyası, 26*(2), 636-674. doi: 10.15612/BD.2025.850

**Makale türü / *Paper type:*** Araştırma Makalesi / *Research Article*

**DOI:** 10.15612/BD.2025.850

**Geliş Tarihi / *Received*:** 03.07.2025
**Kabul Tarihi / *Accepted*:** 19.12.2025
**Elektronik Yayınlanma Tarihi / *Online Published*:** 29.12.2025

***İletişim / Communication***
*Üniversite ve Araştırma Kütüphanecileri Derneği / University and Research Librarians Association*
*Posta Adresi / Postal Address: Marmara Sok. No:38/17 06420 Yenişehir, Ankara, Türkiye.*
*Tel: +90 312 430 03 61; Faks / Fax: +90 312 430 03 61; E-posta / E-mail: bilgi@bd.org.tr*
*Web: https://bd.org.tr*

*Araştırma Makalesi*

# Üniversitelerde İş Süreçlerinin Bir Parçası Olarak Veri Yönetişimi Politikalarının Karşılaştırmalı Değerlendirilmesi*

*Burcu TIĞ DEMİR***, *Özgür KÜLCÜ****

## Öz

*Günümüzde verinin stratejik değeri, bireysel yaşamdan kurumsal süreçlere kadar her alanda kendisini göstermektedir. Kurumların veriyi nasıl ve hangi amaçlarla yönettikleri, operasyonel verimlilikten stratejik karar alma mekanizmalarına kadar birçok sorunun çözümüne doğrudan etki etmektedir. Bu bağlamda yükseköğretim kurumlarında da verinin kurumsal bir varlık olarak ele alınması ve etkin bir şekilde yönetilmesi giderek daha önemli hale gelmiştir. Üniversitelerin akademik, idari ve stratejik iş süreçlerinde hızlı, doğru ve kanıta dayalı kararlar alabilme kapasitesi, geliştirdikleri veri yönetişimi yaklaşımlarıyla yakından ilişkilidir. Bu çalışmada, yükseköğretim kurumlarında veri yönetişimi politikalarının mevcut durumunu anlamak ve uluslararası bir karşılaştırma yapabilmek amacıyla Amerika Birleşik Devletleri, Birleşik Krallık ve Avustralya'daki toplam 146 üniversitenin kamuya açık veri yönetişimi politikaları içerik analizi yöntemiyle incelenmiştir. Politika metinlerine tematik kodlamalar yapılmış ve ülkeler arasındaki benzerlikler ile farklılıklar ortaya konulmuştur. Analiz sonuçları, her ülkenin kendi mevzuat yapısı, kurumsal öncelikleri ve yönetişim kültürüne dayalı olarak özgün veri yönetişimi yaklaşımları geliştirdiğini göstermektedir. Bununla birlikte, incelenen üniversitelerin önemli bir bölümünde veri yönetişimi uygulamalarının henüz olgunluk düzeyine ulaşmadığı ve gelişime açık alanlar bulunduğu tespit edilmiştir. Bu çalışma, küresel, ulusal ve bölgesel ölçekteki yükseköğretim kurumları için kavramsal bir çerçeve sunarak, veri yönetişimi politikalarının geliştirilmesi ve bu alandaki standartlaşma çalışmalarına katkı sağlama anlamında yol gösterici olabilir.*

***Anahtar sözcükler:*** *Veri yönetişimi, yükseköğretim kurumları, veri yönetişimi politikaları, üniversitelerin iş süreçleri, üniversitelerde veri yönetişimi.*

* Bu makale Burcu Tığ Demir'in Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümünde yaptığı doktora tezine dayanmaktadır.

** Hacettepe Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, Ankara, burcutig89@gmail.com

*** Hacettepe Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, Ankara, ozgurkulcu@gmail.com

**BİLGİ DÜNYASI, 2025, 26 (2), *636-674*** *DOI: 10.15612/BD.2025.850*

*Research Article*

# Comparative Assessment of Data Governance Policies as Part of Business Processes in Universities*

*Burcu TIĞ DEMİR*** , *Özgür KÜLCÜ****

## Abstract

*The strategic value of data has become evident across all dimensions of modern life, from individual daily activities to complex organizational processes. How institutions manage data and for what purposes they utilize it significantly influences the resolution of various operational and strategic challenges. Similarly, in higher education institutions, recognizing data as an institutional asset and managing it effectively has become increasingly important. The capacity of universities to make fast, accurate, and evidence-based decisions in their academic, administrative, and strategic processes is closely linked to the data governance approaches they adopt. This study aims to examine the current state of data governance policies in higher education institutions and to conduct an international comparison. To this end, publicly available data governance policies from a total of 146 universities in the United States, the United Kingdom, and Australia were analyzed using content analysis. The policy documents were thematically coded, and similarities and differences among countries were identified. The results reveal that each country has developed its own unique data governance approach shaped by national regulations, institutional priorities, and governance culture. However, it was also found that data governance practices in many of the universities reviewed have not yet reached a mature level and that there is significant room for improvement. This study offers a conceptual framework for higher education institutions at global, national, and regional levels, positioning itself as a reference point for the formulation of data governance policies and the advancement of standardization efforts in this domain.*

***Keywords:*** *Data governance, higher education institutions, data governance policies, university business processes, data governance in universities.*

* This article is based on the doctoral dissertation conducted by Burcu Tığ Demir in the Department of Information Management at Hacettepe University.

** Hacettepe University, Department of Information Management, Ankara, burcutig89@gmail.com

*** Hacettepe University, Department of Information Management, Ankara, ozgurkulcu@gmail.com

## Giriş

Yirmi birinci yüzyılda dijitalleşme süreçlerinin kurumsal işleyişe entegre edilmesiyle birlikte, yükseköğretim kurumları giderek daha fazla veri odaklı yapılara dönüşmeye başlamıştır. Özellikle karar alma, kaynak yönetimi[1] ve performans değerlendirme[2] gibi temel süreçlerde veriye dayalı yaklaşım, yükseköğretimin işleyiş mantığını yeniden şekillendirmektedir (Bhansali, 2014, s. 2). Yükseköğretim kurumları veriye yönetsel ve operasyonel[3] düzeyde işlevsellik kazanmak için veriyi stratejik varlık[4] olarak ele almalıdır (Fisher, 2009, s. 20; Ladley, 2020, s. 16). Bu yaklaşım ile hızlı karar alma, risk kontrolü, maliyet azaltma, iş verimliliğini ve entegrasyonunu sağlama, derin içgörüler yakalama gibi rekabet avantajları sağlanmaktadır (Attard ve Brennan, 2018; Otto, 2011). İş süreçlerinin değerini artırmak amacıyla, verilerin tanımlanması, sınıflandırılması, erişimi ve yönetimi için belirli standartlar, politikalar ve süreçlerin geliştirilmesi; buna uygun kurumsal yapı ve altyapının oluşturulması gerekmektedir. Bu noktada, veri yönetişimi disiplini ön plana çıkmaktadır (Panian, 2010). Kurumlar, etkili bir veri yönetişimi yaklaşımı benimseyerek verilerinin değerini en üst düzeye çıkarabilir ve rekabet avantajı elde edebilirler (Jackson ve Carruthers, 2019). Bu nedenle, kurum içindeki verilerin açık bir biçimde tanımlanması, düzenlenmesi ve belirli standartlara uygun şekilde yönetilmesi beklenmektedir (Bhansali, 2014, s. 2).

Kurumsal verinin (institutional data) etkili bir şekilde yönetilebilmesi için, öncelikle kurum içinde veri yönetimi (data management) ve veri yönetişimi (data governance) kavramlarının doğru tanımlanması gerekmektedir (Khatri ve Brown, 2010). İki kavramın birbiri ile doğrudan ilişkili olması kurum içinde karmaşıklığa sebep olabilir (Plotkin, 2013). Veri yönetimi, alınan kararların ve politikaların uygulanmasını sağlayan operasyonel süreçleri kapsarken; veri yönetişimi, bir kurumun verilerinin kullanılabilirliğini, erişilebilirliğini, kalitesini, tutarlılığını, denetlenebilirliğini ve güvenliğini sağlamak için gerekli süreçler, politikalar, standartlar, organizasyon yapıları ve teknolojileri içermektedir (Abed vd., 2014, s. 21-3; Khatri ve Brown, 2010; Panian, 2010, s. 944).

Veri yönetişimi, kurumsal otorite ve kontrol mekanizmalarını güçlendirerek iş süreçlerinin düzenlenmesini sağlamaktadır. Bu kapsamda politika, prosedür, rol tanımları ve standartlar geliştirilmektedir (DAMA International, 2009, s. 37). Aynı zamanda, verinin doğruluğunu, bütünlüğünü, kararlılığını ve güncelliğini güvence altına alan faaliyetleri içermektedir (Wende, 2007). Kurumun hesap verebilirliğini

1 Kurumun sahip olduğu kaynakları (insan, zaman, bütçe, bilgi, malzeme vb.) etkin, verimli ve sürdürülebilir şekilde planlama, organize etme, yönlendirme ve kontrol etme sürecidir.

2 Kurumun belirlenen görev ve sorumluluklara ne ölçüde uygun davrandığını ve hedeflere ne derece ulaştığını değerlendirme sürecidir.

3 Bir kurumunda günlük, pratik işleyişe dair olan; doğrudan uygulamaya, yürütmeye veya üretime yönelik tüm faaliyetleri kapsayan bir terimdir.

4 Bir kurumun uzun vadeli hedeflerine ulaşmasında kritik rol oynayan, rekabet avantajı sağlayan ve kurumun sürdürülebilirliğini doğrudan etkileyen kaynak ya da unsurdur.

artırmak amacıyla veri kalitesini iyileştirmek de veri yönetişiminin temel amaçlarından biridir (Bhansali, 2014, s. 2).

Veri yönetişimi stratejileri, kurumların ihtiyaçları doğrultusunda veri kalitesinin güvence altına alınmasını ve verinin kurumsal amaçlara hizmet edecek biçimde etkin şekilde yönetilmesini hedeflemektedir (Barker, 2016). Günümüzün veri ve bilgi yoğun ekosisteminde yükseköğretim kurumları tarafından geliştirilen veri yönetişimi stratejileri, operasyonel süreçlerle beraber kurumları diğer örgütlerden ayıran temel rekabet avantajlarından birini oluşturmaktadır (Bhansali, 2014, s. 4). Bu stratejiler, kurum içinde kültürel bir dönüşüm yaratmakta ve veri odaklı bir kurum kültürünün oluşmasına katkı sağlamaktadır (Jackson ve Carruthers, 2019).

Veri yönetişimi süreçlerinin kurumsal bir yaklaşım olarak benimsenmesi, kurum kültürünü doğrudan biçimlendiren kritik bir unsur haline gelmektedir. Çoğu zaman teknik bir uygulama alanı[5] olarak değerlendirilen veri yönetişimi, aslında kurum genelinde değerler, davranış kalıpları ve karar alma pratiklerini etkileyen bütüncül bir yönetim anlayışını ifade etmektedir (Nielsen, 2017). Bu doğrultuda üst yönetimin kurum kültürüne ilişkin yaklaşımı, veri yönetişimi süreçlerinin başarısını doğrudan belirleyen temel bir faktör olarak ortaya çıkmaktadır (Putro vd., 2016). Yükseköğretim kurumlarında etkili ve sürdürülebilir bir veri yönetişimi yapısının oluşturulabilmesi için üst yönetimin; işlevsel veri ekiplerinin kurulmasını desteklemesi, iç denetim ve uyumluluk mekanizmalarının geliştirilmesini güvence altına alması, düzenleyici gerekliliklerin sistematik biçimde izlenmesini sağlaması ve veri yönetişimi faaliyetlerinin kurumsal önceliklerini açık şekilde tanımlaması gerekmektedir. Ayrıca tüm çalışanlara yönelik kapsamlı veri yönetişimi eğitimlerinin teşvik edilmesi, uygulama ve izleme standartlarının kurumsal düzeyde belirlenmesi ve veri yönetişimi planları ile politikalarının düzenli aralıklarla gözden geçirilmesi de üst yönetimin liderlik etmesi gereken temel sorumluluk alanları arasında yer almaktadır. Bu kurumsal adımlar, olgun ve sürdürülebilir bir veri yönetişimi programının oluşturulmasına önemli ölçüde katkı sağlamaktadır (Omar ve Almaghthawi, 2020). Oluşturulacak veri yönetişimi programlarının başarıya ulaşabilmesi için kurumların kendi değişim dinamiklerini, yapısal özelliklerini ve karşılaştıkları sorunları bütüncül bir bakış açısıyla ele almaları gerekmektedir (Panian, 2010). Nitekim her kurumun ihtiyaçlarının, süreçlerinin ve veri ekosisteminin[6] farklı olması nedeniyle verilerin etkin biçimde yönetilebilir hale getirilmesi, önemli düzeyde maliyet, sorumluluk ve risk içeren bir dönüşüm süreci olabilir (Smallwood, 2014). Bununla birlikte, veri yönetişimi süreçlerinin doğru ve tutarlı biçimde işletildiği kurumlarda operasyonel verimliliğin arttığı, maliyetlerin azaldığı,

5 Teknik uygulama: Sadece BT'nin yaptığı şey olarak algılandığında veri yönetişiminin kültürel, yönetsel ve stratejik boyutu, kurumsal sorumluluk paylaşımı, karar alma süreçleri gibi daha geniş kapsamlı, insan ve organizasyon merkezli alanları göz ardı edilmektedir.

6 Veri ekosistemi, kurum içinde verinin üretildiği, işlendiği, saklandığı, paylaşıldığı ve kullanıldığı tüm süreçleri; bu süreçlerde rol alan insanları, teknolojileri, kuralları ve ilişkileri kapsayan bütüncül yapıyı ifade eder.

düzenleyici gerekliliklerle uyumun güçlendiği ve tüm bu unsurların kurumun stratejik hedeflerine ulaşmasına doğrudan katkı sağladığı görülmektedir (Bhansali, 2014, s. 3). Literatür, veri yönetişimi alanında öne çıkan başarılı kurumların arka planında genellikle kapsamlı, tutarlı ve etkin biçimde uygulanan veri yönetişimi politikalarının bulunduğunu vurgulamaktadır (Jackson ve Carruthers, 2019).

İş süreçlerinde hızlı, doğru ve stratejik karar alma avantajları sağlayan veri yönetişimi politikalarının genellikle idari yapıların tanımlanmasına yönelik geliştirilmesi temel problemler arasında görülmektedir. Bu bağlamdan hareketle, bu çalışmada üniversitelerin veri yönetişimi yaklaşımlarını analiz edebilmek amacıyla 146 üniversiteye ait veri yönetişimi politika metinleri incelenmiştir. Politikaların incelenmesi sonucunda üniversitelerdeki veri yönetişimi yaklaşımının çeşitliliği ya da benzerliği analiz edilmeye çalışılmıştır. Elde edilen bulguların, küresel, ulusal ve bölgesel düzeydeki yükseköğretim kurumları için kavramsal bir çerçeve sunması ve veri yönetişiminde standartlaşma çalışmalarına katkı sağlaması beklenmektedir.

**Araştırmanın Amacı ve Araştırma Soruları**

Veri yönetişimi politikaları, teknik ve günlük operasyonel süreçlerin ötesinde; karar alma mekanizmalarını, hesap verebilirlik ilişkilerini, roller ile sorumlulukların tanımlanmasını ve genel yönetsel yapıların düzenlenmesini kapsamaktadır. Ancak mevcut uygulamalara bakıldığında, üniversitelerde veri yönetişiminin çoğunlukla yapısal ve yönetsel düzenlemeler çerçevesinde ele alındığı görülmektedir. Bu nedenle araştırma, yükseköğretim kurumlarında geliştirilen veri yönetişimi politikalarının ve yaklaşımlarının durumunu anlamayı amaçlamaktadır. Bu kapsamda çalışmanın temel problemi, üniversitelerde geliştirilen veri yönetişimi politikalarının büyük ölçüde idari yapıların organizasyonu ve işleyişine odaklanmasıdır. Bu politikalar genellikle veri sahipliği, erişim yetkileri, sorumlulukların dağılımı ve idari prosedürlerin düzenlenmesi gibi yapısal konuları merkeze almaktadır. Oysa veri yönetişiminin etkili olabilmesi için teknik, etik, stratejik ve kültürel boyutları da kapsayan bütüncül bir yaklaşım gerekmektedir. Araştırmanın amacı ve temel problemi kapsamında aşağıdaki sorulara yanıtlar aranmıştır:

- Üniversitelerde mevcut veri yönetişimi politikaları hangi temel bileşenleri içermektedir?
- Bu politikalar, teknik, etik, kültürel ve stratejik yönleri ne ölçüde kapsamaktadır?
- Politika metinleri üniversite içindeki veri yönetişimini tanımlama, uygulama ve izleme aşamalarına yönelik mi geliştirilmiştir?
- Üniversitelerin veri yönetişimine yaklaşımları ülkelere göre ne gibi farklılıklar göstermektedir?

**Literatür Değerlendirmesi**

Veri yönetişimi, başlangıçta ağırlıklı olarak teknik altyapı ve bilgi teknolojileriyle (BT) ilişkilendirilerek gelişim göstermiştir. Ancak zamanla bu teknik çerçevenin ötesine geçerek, kurum genelinde stratejik, yönetsel ve kültürel boyutları kapsayan çok katmanlı bir yönetişim alanına dönüşmüştür. Nielsen (2017), veri yönetişimine sistemik bir bakışla yaklaşarak, bu yapının BT yönetişimi üzerine temellendiği görüşünü ortaya koymuştur. Öte yandan, Weber vd. (2009, s. 23) veri yönetişimi ve BT yönetişimi kavramlarının benzer hedefler taşımasına karşın, doğrudan karşılaştırılamayacağını savunmuştur. Panian (2010) ise daha pratik bir yaklaşımla, BT yönetişiminin kurumsal uygulamaları düzenleyen bir çerçeve sunduğunu ifade etmiştir.

Veri yönetişimini çerçevelendirmek amacıyla literatürde önerilen çeşitli modeller bulunmaktadır. Otto'nun (2011, s. 6-7) geliştirdiği morfolojik[7] çerçeve, veri yönetişiminin örgütsel bir tasarım problemi olduğunu ve üç temel boyutta[8] ele alınması gerektiğini ortaya koymaktadır. Khatri ve Brown (2010) tarafından geliştirilen modelde; veri ilkeleri, veri kalitesi, üst veri (metadata), veri erişimi ve veri yaşam döngüsü, yönetişim çerçevesinin temel eksenleri olarak tanımlanmıştır. Bu yapı, verilerin kurumsal bir varlık olarak kabul edilmesi için gerekli olan temel ilkeleri ve politikaları tanımlamayı amaçlamaktadır. Veri Yönetişimi Enstitüsü[9] (Data Governance Institute) çerçevesi, veri yönetişimi alanında en yaygın referans alınan kuramsal modellerden biridir. Veri yönetişimi politikalarını 10 evrensel veri yönetişiminin temel yapı taşlarından biri olarak tanımlamaktadır. Legner vd. (2023) veri yönetişiminin yalnızca kontrol ve uyumluluk süreçleriyle sınırlı kalmaması gerektiğini, aynı zamanda organizasyon içinde veri temelli değer yaratımını desteklemesi gerektiğini vurgulamaktadır. Bu yaklaşım, Weber vd. (2009) ve Abraham vd. (2019) tarafından dile getirilen yönetişim sistemlerinin stratejik değerle bütünleştirilmesi gerekliliği ile uyumludur.

Brous vd. (2016), yönetişim kapsamında politika, standart ve süreçlerin açıklıkla tanımlanmasının kurumsal işbirliğini artıracağını ve sorunların çözümünü kolaylaştıracağını savunmuştur. Yakın tarihli işbirliğine dayalı modelde Leghemo vd. (2025) açık tanımlanmış yönetişim yapıları, birimler arası işbirliği, standart veri politikaları ve güçlü güvenlik önlemlerinin kurumların veri kalitesine ve karar alma süreçlerine katkı sağlayacağı görüşündedir. Panian (2010) da veri yönetişimi uygulamalarının temeline veri politikalarının yerleştirilmesi gerektiğini belirtmektedir. Benzer şekilde Abraham vd. (2019) veri yönetişiminin çerçevesini şekillendiren temel araçlar olarak politika, prosedür ve standartları koymuştur. Otto (2011) ise veri yönetişiminin ilk işlevsel hedefinin veri politikalarının ve veri stratejilerinin oluşturulması olduğunu vurgulamaktadır. Bu yaklaşımı destekleyen Otto ve Reichert (2010), ana veri yönetimi

7 Veri yönetişimini oluşturan tüm yapı taşlarının incelenmesi

8 Hedefler, yapı ve roller

9 https://datagovernance.com/

fonksiyonlarının[10] en temel görevlerinden birinin, veri politikalarının sürekliliğini sağlamak olduğunu ifade etmektedir.

DAMA International (2009) da veri stratejilerinin geliştirilmesini bir üst düzey eylem olarak tanımlamakta ve bu stratejilerin temelini oluşturan ilke, davranış ve kuralların veri politikaları tarafından şekillendirilmesi gerektiğini belirtmektedir. Diğer yandan, Al-Badi vd. (2018), ISO 8000[11] veri kalite standardı ile uyumlu sekiz bileşenli bir veri yönetişimi çerçevesi önererek, veri politikalarını bu çerçevenin merkezine yerleştirmiştir. Bu bağlamda, Wende ve Otto (2007) veri yönetişiminde hesap verebilirliğin sağlanması için veri politikalarının analitik olarak değerlendirilmesi gerektiğini önermektedir. Genel olarak değerlendirildiğinde verilerin politikalarla ve uygulamalarla en iyi şekilde yönetimini veri yönetişimi süreci sağlamaktadır (Ladley, 2020). Veri yönetişimi sürecinde kurumsal kültür engeli, üst yönetimin konuyu önemsememesi, teknik bilgi ve teknik altyapı eksikliği, düşük veri kalitesi, gizlilik ve güvenlik gibi sorunlar ile karşılaşıldığı literatürde belirtilmiştir (Hora vd., 2017; Ladley, 2020; Nielsen, 2017; Omar ve Almaghthawi, 2020; Picciano, 2012; Wende, 2007). Yükseköğretim kurumlarına özel yapılan çalışmada fakülteler ve bölümler arası veri paylaşım eksiliği, veri sahipliği ve veriye dayalı karar alma kültürü eksiklikleri ek sorunlar olarak tespit edilmiştir (Contreras, vd. 2024).

Veri yönetişimi literatürü, son yıllarda verinin kurumsal değer üretimindeki rolünün artmasına paralel olarak önemli bir gelişim göstermiştir. Geleneksel literatür, ağırlıklı olarak veri kalitesi ve düzenleyici uyumluluk gibi kontrol temelli hedeflere odaklanmıştır. Kapsamlı veri yönetişimi çalışmaları değerlendirmesi sonucunda Alhassan, vd. (2016) en çok odaklanılan başlıkların veri rolleri, veri politikaları, prosedürler, standartlar ve veri kalitesi kavramlarının tanımlanması olduğu sonucuna varmıştır. Bu kavramların uygulanması ve izlenmesine yönelik çalışmaların eksik kaldığı ifade edilmektedir. Bu durumun, kurumlardaki veri yönetişimi olgunluk düzeylerinin[12] (maturity levels) düşüklüğünden kaynaklandığı ileri sürülmektedir. Yükseköğretime özgü bir olgunluk modeli geliştirme ihtiyacı vurgulanmıştır (Contreras, vd. 2024).

## Yöntem

Küresel ölçekte çerçeve çizebilmek amacıyla Amerika Birleşik Devletleri (ABD), Avrupa Birliği, Avustralya ve Birleşik Krallık'taki (BK) 1675 üniversitenin web sayfaları ziyaret edilmiştir. Bu çerçevede ilgili üniversitelerin veri yönetişimi yaklaşımları incelenmiş,

10 Ana veri yönetimi (Master Data Management), kurumların veri varlıklarını tanımlayan, sahiplenen ve yöneten, uygulamadan bağımsız bir süreç olarak tanımlanmaktadır.

11 https://www.iso.org/standard/63086.html

12 Bir kurumun belirli bir alandaki süreçlerini ne ölçüde tanımladığı, uyguladığı, ölçtüğü, kontrol ettiği ve sürekli iyileştirdiği hakkında fikir veren aşamalı bir değerlendirme sistemidir.

varsa bu alandaki politika belgeleri PDF formatında indirilmiştir. İndirilen politika belgeleri nitel yöntemlerden olan tematik analiz yöntemiyle değerlendirilmiştir.

Avrupa Birliği üniversitelerinde veri yönetişimi kapsamında özellikle araştırma verilerine yönelik politikalar geliştirilmiş, bu doğrultuda veri sorumluları atanmıştır. AB üniversiteleri çalışma kapsamına alınan kurumsal veri yönetişimine ilişkin politika geliştirmemiştir. Öte yandan, İspanya'daki *Saint Louis Üniversitesi* ve Bulgaristan'daki *Central European Üniversitesi* gibi bazı kurumlarda Kurumsal Araştırma Ofisleri bulunmakta ve bu birimler aracılığıyla kurumsal düzeyde veri toplanmaktadır. Ancak, söz konusu birimlerin faaliyetlerini düzenleyen herhangi bir veri yönetişimi politika belgesine ulaşılamamıştır. Benzer şekilde, *Hamburg Üniversitesi'nde* veri yönetişimi birimi mevcut olmasına karşın, bu birimin yapısı, sorumluluk alanları ve uygulamalarına dair kamuya açık sınırlı bilgi bulunmaktadır.

Bu çalışma, üniversitelerin kurumsal verilerine ilişkin geliştirdikleri veri yönetişimi politikalarının karşılaştırmalı analizini amaçlamıştır. Avrupa Birliği üniversitelerinde ise, veri politikalarının büyük ölçüde araştırma verilerine odaklandığı ve kurumsal verilere yönelik kapsamlı politikaların bulunmadığı görülmüştür. Bu durum, çalışmanın sınırları kapsamı dışında kaldığından, anlamlı ve karşılaştırılabilir analizlerin yapılmasını güçleştirdiğinden, AB üniversiteleri araştırma kapsamı dışında bırakılmıştır.

AB üniversiteleri hariç tutularak veri yönetişimi politikasına sahip 1.174 üniversitenin web sayfası değerlendirmeye alınmıştır. Bu üniversitelerden 146'sında (%12) açıkça tanımlanmış bir veri yönetişimi politikası tespit edilmiştir. Politika bulunan üniversitelerin %90'ı ABD'de yer almaktadır (n=131). Politika geliştirme oranı en yüksek ülke %18 ile Avustralya olmuştur.

**Tablo 1**

*Ülkelere Göre Veri Yönetişimi Politikalarının Dağılımları*

| Ülkeler | Politika Aranan Üniversite Sayısı | | Politika Bulunan Üniversite Sayısı | | Politika Oranı |
|---|---|---|---|---|---|
| | N | % | N | % | % |
| ABD | 971 | 83 | 131 | 90 | 13 |
| Avustralya | 38 | 3 | 7 | 5 | 18 |
| BK | 165 | 14 | 8 | 5 | 5 |
| Toplam | 1174 | 100 | 146 | 100 | 12** |

*Politika: Üniversitelerin "Veri Yönetişimi Politikası" adıyla yayınladıkları belgeler kastedilmektedir.
**Çalışma kapsamına alınan üniversitelerin politika geliştirme oranı

Veri yönetişimi politikalarındaki eğilimleri, kapsamları ve içeriksel öncelikleri ortaya koymak amacıyla aşağıdaki adımlar NVivo 15'in Lumivero AI Assistant[13] adlı nitel veri analizi yazılımı ile değerlendirilmiştir.

**1. Politika Belgesi Toplama:** ABD, Avustralya ve BK'deki üniversitelerin resmî web sayfaları taranarak "veri yönetişimi politikası" adı altında yayımlanan 146 belge toplanmıştır. Politikalara erişimde kurumun türü (vakıf ya da devlet) ayırt edilmeksizin hareket edilmiştir. PDF formatında indirilen belgeler ülkelere göre düzenlenerek veriye aşinalık sağlanması için okunarak analize hazır hale getirilmiştir.

**2. Tematik Kodlama**: Verilerin analizi için hazırlanan ve düzenlenen 146 adet PDF doküman, NVIVO yazılımına aktarılmıştır. Politika belgelerindeki alt başlıklar incelenmiş ve içerikte tekrar eden temalar belirlenerek tematik bir yelpaze oluşturulmuştur. Kodlama geçerliliğini ve güvenirliğini sağlamak amacıyla, politika metinlerinin alt başlıkları anahtar kelime olarak seçilmiş ve toplamda 42 kod belirlenmiştir. Yalnızca Birleşik Krallık üniversitelerine ait politika metinleri, iki bağımsız kodlayıcı tarafından tekrar kodlanmıştır. Kodlama süreci sonunda, *politika metni* kodu altında yer alan *veri kalitesi, roller ve sorumluluklar, veri güvenliği* ve *veri sınıflamaları* alt başlıklarının sınıflandırılmasında farklılıklar gözlenmiştir. Bu durum kodlayıcılar arasında tartışmaya yol açmış, ancak yapılan karşılaştırma ve görüşmeler sonucunda ortak bir uzlaşıya varılmıştır. Örneklem üzerinde gerçekleştirilen tekrar kodlama sonucunda Cohen's Kappa katsayısı 0,82 olarak hesaplanmış ve bu değer kodlamanın yüksek düzeyde güvenirlik gösterdiğini ortaya koymuştur. Kodlama sürecinde, belgelerin hangi yönetişim boyutlarına (örneğin, veri kalitesi, güvenlik, roller ve sorumluluklar, uyumluluk vb.) vurgu yaptığı sistematik biçimde analiz edilmiştir. Kodlama sürecinde, NVivo'nun Nodes (düğümler) özelliğiyle ana temalar ve alt kodlar oluşturulmuş, benzer kavramlar birleştirilerek tematik bütünlük sağlanmıştır.

**3. Sözcük Temelli İçerik Analizi:** Veri yönetişimi politikalarının niteliklerini ve eğilimlerini ortaya koymak amacıyla belgelerde sıklıkla geçen anahtar kavramlar, terimler ve ifadeler tespit edilmiştir. Bu terimler, içeriksel yoğunluklarına (Word Frequency Query) göre sınıflandırılarak ilgili temalarla eşleştirilmiştir. Lumivero AI Assistant, İngilizce metinlerde arka planda tokenleştirme[14] (tokenization) işlemini kullanarak çalışmaktadır. Bu işlem, doğal dil işleme (NLP)[15] sistemlerinin temel yapıtaşıdır. Ancak Lumivero AI bu işlemi otomatik ve kapalı kutu (black-box)[16] biçimde kullanıcı bu adımları görmemektedir. Dil modeli girişi olarak metni token'lara ayırmaktadır. Bu

13 https://help-nv.qsrinternational.com/15/win/Content/ai/ai-assistant.htm

14 Tokenleştirme (tokenization), bir metni anlamlı parçalara (token'lara) ayırma işlemidir. Bu parçalar genellikle kelime, cümle veya alt-kelimeler olabilir.

15 Doğal Dil İşleme (Natural Language Processing – NLP), bilgisayarların insan dilini anlamasını, yorumlamasını, üretmesini ve anlamlı şekilde kullanmasını sağlayan yapay zekâ (AI) ve dilbilim (linguistik) alanıdır.

16 Bir sistemin iç yapısı veya nasıl çalıştığı bilinmeden sadece girdisine ve çıktısına ulaşılabilen durumları tanımlamak için kullanılır.

tokenler, hem anlamsal analiz (yani tema keşfi) hem de özetleme ya da öneri üretme işlemlerine temel olmaktadır. Lumivero AI, metnin bağlamını koruyarak sözcükleri işleyerek *kelime sayımı* yerine *anlam odaklı tokenleştirme*[17] sağlamaktadır. Anlam odaklı tokenleştirme sayesinde sözcükler anlam ilişkileriyle birlikte ele alınmaktadır. Böylece üniversitelerin veri yönetişiminde hangi konu başlıklarına öncelik verdiği, hangi alanlarda daha yüzeysel yaklaşımlar benimsediği ve hangi politika dilinin tercih edildiği analiz edilmiştir.

**4. Karşılaştırmalı Analiz ve Kategorilendirme:** Elde edilen bulgular ülke bazında karşılaştırılarak, veri yönetişimi politikalarının kapsam, içerik ve yapı bakımından benzerlik ve farklılık gösterme durumu değerlendirilmiştir. Bu analiz, ülkeler arasında benimsenen veri yönetişimi kültürlerinin, yasal düzenlemelerin ve kurumsal önceliklerin etkisini ortaya koymayı amaçlamaktadır. Analiz işlemi sonucunda politika metinlerinde kodlanan bazı bölümlerin benzerlik göstermesi sonucu 42 kod, analiz sonuçlarının daha anlamlı çıkabilmesi ve karşılaştırma kolaylığı sağlayabilmesi için 16 kod altında birleştirilmiştir.

**5. Veri Görselleştirme ve Bulguların Sunumu:** Kodlama sürecinden elde edilen bulgular sistematik bir şekilde sunulmak üzere yapılandırılmıştır. İlk aşamada, içerik analizi kapsamında kategorik gruplara ayrılmış 16 kodun veri politikalarında yer alma oranları değerlendirilmiştir. Bu sayede veri yönetişimi politikalarının yapısal dağılımı ve içeriksel yoğunluğu tablolandırılmıştır. Ardından, her bir kodun politika metinlerinde geçme sıklığı dikkate alınarak kurumların veri yönetişimi yaklaşımları arasında benzerlik ve farklılık gösteren örüntüler ortaya konmuştur. Bu aşamada, kodların dağılımı üzerinden ortak veri yönetişimi uygulamaları belirlenmiş, daha sonra üniversite isimleri belirtilerek öne çıkan iyi uygulama örnekleri ayrıntılı biçimde analiz edilmiştir. Son bölümde ise ülkeler düzeyinde karşılaştırmalı bir değerlendirme yapılarak, farklı yükseköğretim sistemlerinde veri yönetişimi uygulamalarının nasıl çeşitlendiği ortaya konmuştur. Bu karşılaştırma hem politikaların olgunluk düzeylerini hem de ülkeler arası yapısal ve yönetsel farklılıkları göstermesi açısından çalışmanın bütüncül analizini tamamlamaktadır.

## Bulgular

Bu bölümde, uluslararası düzeyde 146 üniversitenin kamuya açık veri yönetişimi politikaları bulgularına yer verilmiştir. Analiz sonuçlarının verildiği Tablo 2'ye göre, Tanımlar-Terimler ve Amaç başlıları 98 adet politika metninde geçmektedir (%67,1). Roller ve Sorumluluklar (N=91; %62,3), Arka Plan (N=84; %57,5) ve Kapsam (N=81; %55,5), Politika Metni (N=64; %43,8) gibi başlıkların yaygın biçimde kullanılan politikaların

17 Anlam odaklı tekelleştirme politika metinlerini anlam birimlerine göre, bağlamı dikkate alarak, çok sözcüklü kavramları tek birim olarak, ontolojik veya kavramsal bütünlüğü koruyarak bölmeyi amaçlar. Örneğin "data governance framework" anlam odaklı tokenleştirmede tek bir kavramsal token olabilir.

temel yapı taşlarını oluşturmaktadır. P/B oranlarına[18] bakıldığında özellikle Roller ve Sorumluluklar başlığının öne çıkması politikaların ağırlıklı olarak tanımlayıcı unsurlara ve görev dağılımına odaklandığını ortaya koymaktadır. Bu yönüyle belgelerin büyük ölçüde bilgilendirici ve yapısal nitelikte olduğu söylenebilir.

Destekleyici unsurlar ve güncellenebilirlik vurgusu taşıyan Revizyonlar (N=70; %47,9), Alakalı İçerikler (N=65; %44,5), Politika Hakkında Bilgi (N=46; %31,5) dinamik ve güncellenebilir belgelerin altyapısını oluşturmaktadır. Bu başlıklar yönetişimde sürdürülebilirlik açısından olumlu bir göstergedir. Veri kalitesi, standartlar ve operasyonel bileşenlere yönelik Veri Yönetimi ve Kalitesi (N=68; %41,8), Prosedürler ve Standartlar (N=51; %34,9) ve İş Süreci Unsurları (N=11; %7,5) yer almaktadır. Bu başlıkların P/B oranı değerlendirildiğinde, politikaların uygulama boyutuna işaret etmekte ve günlük iş süreçlerine rehberlik eden unsurlar olarak değerlendirilmektedir.

Paylaşım, erişim ve güvenlik boyutunu temsil eden Veri Erişimi ve Paylaşımı (N=33; %22,6), Veri Güvenliği ve Gizliliği (N=33; %22,6) erişim hakkı ile koruma yükümlülüğü arasında dengeli bir bakış açısı sağlanmaya çalışılmıştır. İlkeler ve Etik (N=24; %16,4) başlıklarının düşük düzeyde temsil edilmesi, kurumsal veri yönetişiminde çerçevenin yetersiz işlendiğine işaret etmektedir. Bu durum, teknik, yönetsel ve değer odaklı bir bakış açısının eksikliğini göstermektedir. Eğitim ve Diğer (N=12; %8,2) bu belgelerin personeli ve paydaşları destekleme yönünde yeterli rehberlik sunamadığını göstermektedir.

**Tablo 2**

*Veri Yönetişimi Politikalarında Geçen Temaların Oranı*

| Kod Kategorisi | N | % | P/B | Kategori Grubu | Açıklama / Not |
|---|---|---|---|---|---|
| Amaç | 98 | 67,1 | 3,0 | Temel Yapı | Politika neden yazılmış, temel hedef nedir? |
| Tanımlar, Terimler | 98 | 67,1 | 9,3 | Temel Yapı | Kavramların netleştirilmesi, standartlaşmayı sağlar |
| Roller ve Sorumluluklar | 91 | 62,3 | 11,0 | Temel Yapı | Kimin ne yapacağı, hangi rolün hangi yetkilere sahip olduğu |
| Arka Plan | 84 | 57,5 | 4,6 | Temel Yapı | Politikanın yazılma geçmişi, gerekçesi |
| Kapsam | 81 | 55,5 | 3,2 | Temel Yapı | Politikanın hangi veri, sistem, kişi ve süreçleri kapsadığı |
| Revizyonlar | 70 | 47,9 | 1,2 | Sürdürülebilirlik | Politikanın güncellenme döngüsü ve sürüm geçmişi |

18 (P/B)*100 P: Tüm politika metindeki toplam kelime sayısı, B: İlgili başlık altındaki kelime

**Tablo 2**

*Devamı*

| Kod Kategorisi | N | % | P/B | Kategori Grubu | Açıklama / Not |
|---|---|---|---|---|---|
| Alakalı İçerikler | 65 | 44,5 | 2,3 | Referanslar/ Ekler | İlgili belgeler, standartlar veya mevzuatlar |
| Politika Metni | 64 | 43,8 | 12,7 | Temel Yapı | Çekirdek politika, asıl metin |
| Veri Yönetimi ve Kalitesi | 61 | 41,8 | 6,6 | İçeriksel Derinlik | Veri kalitesi ölçütleri, kalite güvencesi süreçleri |
| Prosedürler, Standartlar | 51 | 34,9 | 9,3 | Operasyonel Unsurlar | Uygulama adımları, standart iş akışları |
| Politika Hakkında Bilgi | 46 | 31,5 | 1,8 | Üst Bilgi | Politikanın yürürlüğe giriş tarihi, versiyon bilgisi |
| Veri Erişimi ve Paylaşımı | 33 | 22,6 | 4,5 | Paylaşım ve Erişim | Kimin, ne zaman, neye erişebileceği, paylaşım kuralları |
| Veri Güvenliği ve Gizliliği | 33 | 22,6 | 5,3 | Paylaşım ve Erişim | Yetkisiz erişimden korunma, hassas verilerin yönetimi |
| İlkeler ve Etik | 24 | 16,4 | 4,4 | Yönetsel Değerler | Kurumsal etik ilkeler, temel prensipler |
| Eğitim ve Diğer | 12 | 8,2 | 1,7 | Destekleyici Unsurlar | Eğitim faaliyetleri, farkındalık çalışmaları |
| İş Süreci Unsurları | 11 | 7,5 | 4,4 | Operasyonel Unsurlar | Süreç entegrasyonları, iş akış ilişkileri |

## Amaç

Bu bölümde üniversitelerin kurumsal verilerini tanımlama, yönetme, koruma ve erişime sunma amaçları ele alınmıştır. Politikaların amaç bölümündeki ortak noktalar tematik açıdan incelenmiştir. Üniversiteler kurumsal verileri stratejik karar alma, operasyonel verimlilik ve yasal uyumluluk açısından önemli görmektedir. Bu sebeple neredeyse tüm politikalarda kurum verileri kurumsal varlık (institutional asset) olarak tanımlanmaktadır. Doğru, güncel ve tutarlı verinin önemi birçok politikada dikkat çekmektedir. Veri kalitesi ve doğruluğu için sürekli denetim ve kalite kontrol prosedürleri önerilmektedir. Veri erişimi ve güvenliği dengesini sağlayabilmek amacıyla yetkilendirilmiş erişim, rol tabanlı kontroller ve gizlilik politikalarına vurgu yapılmaktadır. Aynı zamanda federal ve eyalet yasalarına, diğer düzenleyici kurumlara ve akreditasyon gereksinimlerine uyum ön planda tutulmaktadır.

Birçok üniversitede veri yönetişimi sürecini yönetebilmek için veri sahiplerine ve komitelere atıfta bulunulmuştur. Üniversite içindeki veri kültürünün ve farkındalığının sağlanması için bilgilendirme ve eğitim gereklilikleri amaçların arasındadır. Her

üniversitenin farklı yapı ve gereksinimleri olsa da veri yönetişimi politikası amaçlarında güvenlik, kalite, şeffaflık ve erişim dengesi ortak tema olarak öne çıkmaktadır.

Kuzey Arizona, Utah, New England Üniversiteleri kurumsal stratejik hedeflerle uyumlu veri yönetişimi dengesini kurmayı temel amaç edinmiştir. Güney Florida, Concord ve Güney Utah gibi üniversitelerde yasal sorumluluk, gizlilik ve mülkiyet temelli politika amacı yapılandırılmıştır. Teksas Christian ve Denver Üniversiteleri veri yönetişimi amaçlarını organizasyonel davranış ve kültürel değişimle ilişkilendirerek kültürel dönüşüm üzerine entegre etmişlerdir. Batı Chester, Kuzey Teksas gibi Üniversiteler ise veri kalitesi ve tutarlılığı amaç edinerek şeffaflığa vurgu yapmaktadırlar.

**Tanımlar, Terimler**

Bu bölümde üniversitelerin veri yönetişimi politikalarında kullanılan terimlerin ne anlamda kullanıldıklarına dair açıklamalar vardır. Birçok politika metninde Veri Sorumlusu (Data Steward), Veri Sahibi (Data Owner), Teknik Veri Sorumlusu (Data Custodian), Veri Kullanıcısı (Data User), Üst Düzey Veri Sorumlusu (Executive Data Steward) gibi terimlerin tanımları bulunmaktadır. Tablo 3'te belirtildiği gibi üniversitelerin politika metinlerinde belirli terimlere ortak tanım ve sorumluluklar yüklenirken bazı üniversitelerde de bu terimler farklı değerlendirilmiştir.

**Tablo 3**

*Tanımlar, Terimler Bölümünün Ortak ve Özgün Yönleri*

| Terimler | Ortak Tanım ve Sorumluluklar | Farklılıklar / Özgünlükler |
|---|---|---|
| Veri Sahibi | Verinin mülkiyetinden sorumlu en üst düzey yönetici. Genellikle Rektör ya da Başkan. | Bazı üniversitelerde Genel Müdür19 olarak tanımlanmış, bazıları ise farklı bilgi alanlarına göre alt dağılım yapmıştır. |
| Üst Düzey Veri Sorumlusu | Politika oluşturma ve veri erişim kurallarını belirleme yetkisine sahip yöneticiler. | Alanlara göre Veri Sorumlusu ve Veri Yöneticisi atama yetkisi |
| Veri Sorumlusu | Belirli veri alanlarında operasyonel sorumluluğa sahip yöneticiler. Genellikle veri kalitesi ve erişim ile ilgilenmektedir. | Bazı üniversitelerde hem iş süreçlerinden hem de teknik altyapıdan sorumlu kişilerdir. |
| Veri Yöneticisi (Data Manager) | Günlük işlemleri ve veri sistemlerinin çalışmasını sağlayan yöneticiler. | Genellikle Uzman Kullanıcı (Power User20) veya Sistem Modülü Yöneticisi olarak tanımlanır. |

19 Chief Executive = CEO (Chief Executive Officer) olarak kabul edilir. Bazı kamu kurumlarında veya BK gibi ülkelerde Chief Executive daha sık kullanılır.

20 Bilgisayar donanımının işletim sistemlerinin programlarının veya web sitelerinin ortalama kullanıcı tarafından kullanılmayan gelişmiş özelliklerini kullanan bilgisayar, yazılım ve diğer elektronik cihazların kullanıcısıdır.

**Tablo 3**

*Devamı*

| Terimler | Ortak Tanım ve Sorumluluklar | Farklılıklar / Özgünlükler |
|---|---|---|
| Data User (Veri Kullanıcısı) | Kurum içi ya da dışı, veriye erişimi olan ve bu veriyi kullanan tüm bireyler. | Öğrenci, akademisyen, danışman, ziyaretçi vb. kapsama dahil |
| Teknik Veri Sorumlusu | Verinin teknik olarak işlenmesi, saklanması, korunması gibi altyapıdan sorumlu kişiler. | BT Koordinatörü (IT Coordinator21) veya Sistem yöneticisi (System Admin22) gibi unvanlar kullanılmaktadır. |
| Bilgi Sistemi (Information System) | Veriyi işleyen ve saklayan tüm sistemler (yazılım, uygulama, veritabanı vb.). | Sistem tanımı çok geniş tutulmuş: fiziksel ya da dijital tüm kaynakları içerebilir. |
| Kurumsal Veri | Kurumun görevlerini yerine getirmesi için gerekli olan tüm veriler. | Risk düzeyine göre sınıflandırma (yüksek, orta, düşük risk gibi) |

Tablo 3'te veri yönetişimi katmanlarını yapılandırabilmek için amacıyla birçok üniversite veri yönetişiminden sorumlu rolleri tanımlamıştır. Bazı üniversiteler ise çok katmanlı olarak Üst Düzey Veri Sorumlusu> Veri Sorumlusu> Veri Yöneticisi> Veri Kullanıcısı şeklinde tanımlamalar bulunmaktadır (örneğin Middle Georgia State Üniversitesi). Minnesota, Rochester, Güney Carolina gibi Üniversiteler rollerin etki alanlarının ve erişim yetkilerinin hiyerarşik şekilde tanımlanması ile öne çıkmaktadır. Minnesota, Tulane, Nevada Las Vegas Üniversitesi, Rochester Teknoloji Enstitüsünde karar alma süreçleri çok paydaşlı bir komite tarafından alınmaktadır. Tulane Üniversitesinde oluşturulan Veri Sorumluluğu Danışma Kurulu (Data Stewardship Advisory) kullanıcılar köprü sağlayan bir yapıdadır. Bazı üniversitelerde rollerin ve terimlerin büyük ölçüde benzer olduğu ve uygulama esnasındaki noktalarına göre değişiklik gösterdiği fark edilmiştir.

Kurumsal veriler için üniversitelerin tanım genişliği dikkat çekmiştir. Bazı üniversiteler tüm verileri kurumsal veri olarak değerlendirirken bazılarında sadece iş süreçlerinde üretilen verileri kurumsal veri olarak tanımlamaktadır. Avustralya'daki James Cook Üniversitesi ABD'deki üniversitelerin aksine araştırma verileriyle kurumsal verilerin ayrımı yapılmıştır. Rochester ve Southern Üniversiteleri veri tanımlarını meta23 düzeyde tutmaktadır. Rochester Teknoloji Enstitüsü ve Güney Carolina Üniversiteleri kurumlar arası rol ayrımı ve veri sınıflandırma konusunda en sistematik olanlardır. Bazı üniversitelerinde kurumsal verilerin sınıflandırılması veri güvenlik politikalarının

21 Bilgi Teknolojileri projelerini denetlemek, kaynakları yönetmek, ekip çalışmalarını koordine etmek, ağ güvenliğini sağlamak, teknik sorunları çözmek ve kurumsal hedeflere ulaşmak için BT stratejilerini uygulamaktan sorumludur.

22 Çok kullanıcılı bir bilgi işlem ortamını destekleyen ve BT hizmetlerinin ve destek sistemlerinin sürekli ve en iyi şekilde çalışmasını sağlayan bir bilgi teknolojileri uzmanıdır.

23 Daha genel, soyut, kavramsal ya da üst düzey bir bakışla ele almak

kapsamını genişletmiştir. Örneğin Oakwood Üniversitesinde kaybı durumunda ciddi zarar doğuracak veri türünü tanımlanmış ve verilerin yönetimi için bütünsel bir süreç dizisi oluşturulmuştur. Snow Koleji veri soybilgisi (verinin nereden geldiği, nasıl dönüştüğü ve kimler tarafından kullanıldığını gösteren) olarak adlandırılan bir süreç benimsenmiştir. Aynı zamanda dikkat çeken başka noktalardan biri üniversitelerin politika metinlerinin birçoğunda Aile Eğitsel Haklar ve Gizlilik Yasası (Family Educational Rights and Privacy Act, FERPA[24]), Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act, HIPAA[25]), GDPR gibi genel yasal düzenlemelere olan uyum vurgulanmıştır.

**Roller ve Sorumluluklar**

Veri yönetişimi politikalarının içerik analizi sonucunda dört ortak organizasyonel yapılanma belirgin hale gelmiştir. Birinci düzey roller olarak görülen Veri Sponsoru[26] (Data Sponsor), Veri Vekili[27] (Data Trustee), Veri Sahibi (Data Owner) gibi yöneticiler tarafından üstlenilen sorumluluklardandır. Kurumsal veri politikalarının oluşturulması, onaylanması, stratejik planlama ve kaynaklarının tahsisi, veri sınıflandırılması ve risk yönetimi konusunda otorite sorumluluklardır. Greensboro'daki Kuzey Carolina Üniversitesi örneğinde, Yürütme Komitesi Veri Sponsoru sorumluluğunda, politika onayı ve bütçe sağlama işleviyle stratejik düzeyde bir yönetişim sağlamaktadır. Benzer şekilde, New Mexico Üniversitesinde Veri Sahibi, veriye ilişkin tanımlama, erişim ve güvenlik gibi konularda nihai yetkiye sahiptir.

İkinci düzey roller veri kalitesi, erişim yönetimi, sistem güvenliği ve günlük işlemlerden sorumlu orta düzey yöneticiler ve teknik personel tarafından yürütülmektedir. Politika metinleri analizine göre Veri Sorumlusu rolü neredeyse tüm üniversitelerde bulunmaktadır. İkinci düzey roller tanım ve standart geliştirme, erişim taleplerinin değerlendirilmesi, eğitim ve farkındalık programlarının yürütülmesi, veri kalitesinin izlenmesi ve raporlanması gibi sorumlulukları gerçekleştirmektedir. Bu sorumluluklardan farklı olarak Northeastern Üniversitesindeki Veri Sorumlusu veri bütünlüğü sağlamanın yanında veri güvenliği süreçlerinde de rol almaktadır. Hudson İlçe Topluluk Koleji ve Little Rock'taki Arkansas Üniversitesinde farklı bir yöntem olan RACI matrisi[28]ne dayalı roller geliştirilmiştir. Matriste dikkat edilen en önemli nokta

24 ABD'de öğrenci eğitsel kayıtlarının gizliliğini güvence altına alan ve öğrencilere/velilere kayıtlarına erişim ile paylaşımını kontrol etme hakları tanıyan temel bir hukuki düzenlemedir.

25 ABD'de, kişisel sağlık bilgilerinin gizliliğini ve güvenliğini korumayı amaçlayan temel federal düzenlemedir.

26 Bir kurum içinde veri yönetişimi çerçevesinde stratejik sorumluluk üstlenen, üst düzey bir yöneticidir. Genellikle veriyle ilgili girişimlerin savunuculuğunu ve kaynak desteğini sağlar.

27 Kurumsal veri yönetişimi yapısı içinde, belirli veri alanlarının işsel sahipliğini ve yönetimini üstlenen kişidir. Genellikle veri kalitesi, güvenliği, gizliliği ve uyumu sağlama konusunda kritik sorumluluklara sahiptir.

28 RACI Matrisi, proje ve süreç yönetiminde kullanılan bir rol ve sorumluluk atama aracıdır. RACI, dört İngilizce terimin baş harflerinden oluşur: Responsible, Accountable, Consulted, Informed (Sorumlu, Hesap veren, Danışılan, Bilgilendirilen)

görevler arasındaki ilişkinin netleştirilmesidir. Matris iş süreçlerine entegre edildiğinde denetlenebilen bir mekanizma geliştirmektedir. Brandeis Üniversitesi örneğinde Teknik Veri Sorumlusu veri kültürü oluşturma konusunda görevlendirilmiştir.

Üçüncü düzey roller veriyle doğrudan çalışan kullanıcılar örneğin Veri Kullanıcısı ve Teknoloji Altyapı Yöneticisi[29] (Technology Custodian) gibi görevlere sahip kişilerdir. Yetkilendirilmiş verileri kullanmak temel görevleridir. Sorunları raporlamak ve güvenlik politikalarına uyum sağlamak gibi rolleri vardır. Greensboro'daki Kuzey Carolina Üniversitesi örneğinde üçüncü düzey rollerde çalışanlar sadece veri kullanmanın yanında sistem bütünlüğüne katkı sağlayan kişiler olarak geçmektedir. Benzer şekilde Oregon Eyalet Üniversitesi ve New Mexico Üniversitesi örneklerinde veri güvenliği ve etik standartlara uyan kullanıcılar arasına üçüncü düzey roller alınmıştır.

Dördüncü düzey rolleri veri yönetişimi süreçlerini kurumsallaştırmak adına çok katmanlı komiteler ve konseyler oluşturmaktadır. Veri politikalarının oluşturulması ve uygulanmasından sorumlu Veri Yönetişimi Kurulu[30] (Data Governance Council), işlevsel koordinasyon ve kalite kontrolünden sorumlu Veri Sorumluluğu Konseyi[31] (Data Stewardship Council) ve stratejik yönlendirme ve onay mekanizmalarından sorumlu Yürütme Yönlendirme Kurulu[32] (Executive Steering Committees) bu düzey roller arasında sayılmıştır. Northeastern Üniversitesinde Veri Sorumluluğu Kurulu farklı birimlerinden temsilcilerin olduğu veri kararlarını yöneten bir sorumluluktur. St. Louis'deki Washington Üniversitesi ise hiyerarşik bir yapı içinde Yürütme BT Yönetişim Kurulu[33] (Executive IT Governance Committee) → Veri Yönetişimi Kurulu → Veri Sorumlulukları dizilimini benimsenmiştir.

Kraliyet Sanat Kolejinde hem kriz senaryoları için hem de yasal uyumluluk süreçlerinde her düzey roller için çok katmanlı yapı tanımlanmıştır. Hiyerarşik veri sahipliği sistemi ile yönetim süreçlerine katkı sağlanmaktadır. Batı Michigan Üniversitesinde veri sözlüğü[34] (data dictionary) oluşturma ve güncelleme ile ilgili

29 Sistemler, uygulamalar, sunucular, veritabanları ve altyapı teknolojileri üzerinde operasyonel düzeyde koruma, bakım ve uygulama standartlarını sağlamakla sorumlu kişidir. Bu rol genellikle Teknik Veri Sorumlusu rolüyle yakından ilişkilidir. Farkı, daha geniş bir teknoloji altyapısı odağına sahip olmasıdır.

30 Bir kurumun veri varlıklarını nasıl yöneteceğine dair kararları alan, veri yönetişimi stratejilerini belirleyen, veri sahipliği, erişim, güvenlik ve kalite gibi konularda politika ve rehber ilkeleri oluşturan üst düzey yürütme kuruludur.

31 Bir kurumda veri sorumluluğu süreçlerini yönlendiren, koordine eden ve geliştiren çok paydaşlı bir danışma ve karar grubudur.

32 Büyük ölçekli projelerde veya kurumsal düzeyde stratejik girişimlerde yönetişim, yönlendirme ve karar alma sorumluluğunu üstlenen en üst düzey rehber kuruldur. Bu komiteler, genellikle üst yönetimden oluşur ve projenin veya programın stratejik hedeflere uygun şekilde ilerlemesini sağlar.

33 Bilgi teknolojileriyle ilgili tüm kararların kurumsal hedeflerle hizalanmasını güvence altına alan, genellikle üst düzey yöneticilerden oluşan stratejik ve denetleyici bir yönetişim yapısıdır.

34 Bir kurumun veri varlıklarına ait tüm temel bilgileri (tanım, format, kaynak, sorumlu kişi, kullanım kuralları vb.) sistematik biçimde belgeleyen ve yöneten resmî referans kaynağıdır. Kurum içinde veriyle ilgili ortak bir dil oluşturur ve veri yönetişiminin temel araçlarından biridir.

sorumluluklar tanımlanmıştır. Üniversite içindeki veri bütünlüğü ve tutarlılığı açısından önemli bir süreçtir. Arlington'daki Teksas Üniversitesi'nde kalıcı olarak oluşturulan Veri Yönetişimi Ofisi[35] (Data Governance Office) veri politikalarını izleme, uygulama, eğitim verme gibi çok yönlü görevleri üstlenmiştir. Veri yönetişiminin sürekliliğine katkı sağlayan bir yaklaşımdır.

**Arka Plan**

Arka plan metinlerinde veri yönetişimi, teknik bir süreçten öte kurumsal stratejilerin ve yönetişim kültürünün parçası olarak ele alınmaktadır. Üniversite içindeki veri varlığının mülkiyet ve sorumluluk tanımlarının altyapısı oluşturulmuştur. Örneğin Montana Üniversitesi, Grand Valley Eyalet Üniversitesi, Baltimore Üniversitesi, Rochester Üniversitesi arka planında varlık olarak kurumsal veri ilkesi vurgulanmaktadır. Grand Valley Eyalet Üniversitesi de veriye varlık olarak yaklaşmanın stratejik avantaj sağlayarak öğrenci başarısı ve dışa açılma süreçlerinde önem taşıdığı açısından bakmaktadır. Aynı zamanda veri erişim ve güvenlik politikalarının yapılandırılması ile ilgili çerçeve çizilmektedir. Seviyesini verinin korunma seviyesini nesnel ölçütlere dayandırarak belirlemesini sağlamaya çalışmaktadır. Örneğin Montana Üniversitesi Federal Bilgi İşleme Standartları[36] (Federal Information Processing Standards, FIPS) 199 tabanlı sınıflandırma sistemi, belgedeki en sistematik güvenlik modellerinden biridir. Verileri risk derecelerine göre sınıflandırarak gerekli önlemlerin alınmasını sağlamaktadır. Verinin yaşam döngüsü boyunca bütünlüğünün ve kalitesinin sağlanması üzerinde de durulmaktadır. Örneğin Baltimore Üniversitesi, verinin kullanım biçimlerini ve iş süreçlerini standartlaştırma odaklı bir veri mimarisi oluşturma çabasındadır. Veri yönetişimi politikaları yalnızca teknik düzenlemelerden ibaret olmayıp kurumsal stratejilerin, yönetişim kültürünün ve karar destek sistemlerinin bir aracı olarak yapılandırılmaktadır. Örneğin Lower Columbia Koleji, veri yönetişimini karar verme kapasitesini doğrudan güçlendiren bir stratejik araç olarak tanımlamaktadır.

Üniversitelerde ortak veri yönetişimi anlayışına sahip olma arka plan kısmında yansıtmaktadır. Arka planda birçok kurumsal roller yapılara da değinilmiştir. Kurumsal rollere yer verilmiş olması, veri yönetişiminin kurumsal liderlik düzeyinde sahiplenilmesini vurgulayan bir yaklaşımdır. Aslında her üniversite kendi yapılanmasına uygun rol-yetki-denetim üçgeni inşa etmektedir.

35 Kurumsal verilerin doğru, güvenli, erişilebilir ve stratejik şekilde yönetilmesini sağlamak amacıyla veri yönetişimi yapısını yürüten, yönlendiren ve sürdüren organizasyon birimidir.

36 ABD federal hükümet kurumları tarafından bilgi sistemlerinin güvenliği, veri işleme ve bilişim teknolojisi alanlarında kullanılmak üzere geliştirilen zorunlu teknik standartlar dizisidir. FIPS standartları, Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST) tarafından yayınlanır.

**Kapsam**

Başlık altında politikanın sınırları ve içeriksel çerçevesi verilmektedir. Bu bölümde neyin veri sayılacağı, kimin hangi verilere erişebileceği ve hangi süreçlerin yönetişime dahil olduğunun yanıtı verilmektedir. Birçok üniversite kapsam bölümünü teknik olarak değerlendirmektedir. California Üniversitesi kapsam tanımını etik, yasal ve sosyolojik boyutlar üzerinden yapılandırarak "veriye erişim" ve "veriyi kullanma" kavramlarını ayrı ayrı analiz etmektedir. Tablo 4'te kapsam bölümünün temaları ve temaya uygun uygulama şekilleri verilmiştir.

**Tablo 4**

*Kapsam Bölümünün Temalara göre Uygulama Türleri*

| Kapsam Bölümünün Temaları | Uygulama Türleri |
|---|---|
| Veri Türleri ve Sınırları | 1) Tüm ortamdaki veriler (elektronik, fiziksel, bulut) dahil<br>2) Kurumsal işleyişi destekleyen veriler (örneğin, öğrenci, mali, insan kaynakları verisi)<br>3) Yönetim sürecinde kullanılan tüm veriler |
| Veri Yaşam Döngüsü | Oluşturma, işleme, erişim, paylaşım, saklama ve imha |
| Kapsam Dışı Veriler | Araştırma, klinik, kişisel notlar ve yasal olarak bağımsız kabul edilen veriler (örneğin akademisyenlerin telif haklarına tabi dokümanları), birçok üniversite tarafından kapsam dışında bırakılmıştır. |
| Örgütsel Yansımaları | 1) Kurumsal çapta veri yönetişimi organları, birimleri ve rolleri<br>2) İzleme, denetim, eğitim ve politika yayılımı süreçlerinin sorumluluğu |
| Uyum ve Etik Çerçeve | Yasalarla birlikte etik, şeffaflık ve hesap verebilirlik vurgulanmaktadır. |

Tablo 4'te farklı anlamdaki uygulamalar kapsamında Batı Chester Üniversitesi, araştırma verilerini politika kapsamı dışında bırakmaktadır. Rochester Teknoloji Enstitüsü ise tüm verilerini Kurumsal Veritabanı (Institutional Database) düzenleyerek kullanıma sunmaktadır. New Mexico Üniversitesi sağlık bilimlerine ait tüm verileri ve araştırma verilerini kapsamı dışında bırakmaktadır. Alabama Üniversitesi ve Olympic Koleji, kapsam başlığını veri yönetişimi programının bir bileşeni olarak sistematikleştirmiştir. Olympic Kolejinde veri yaşam döngüsü ayrıntılı olarak tanımlanmıştır. Erişim ve entegrasyon ilkeleriyle birlikte veri analizi, yedekleme ve felaket kurtarma gibi teknik işlemler de kapsama dâhil edilmiştir.

**Revizyonlar**

Üniversitelerin veri yönetişimi politikalarına ilişkin güncelleme, gözden geçirme, onay ve uygulama tarihlerini içermektedir. Birçok politikanın belirli aralıklar güncelleme yaptığı ve yapılan güncellemelerin kimin tarafından yapıldığı detaylı bir şekilde verilmiştir. Politika metninde güncellenen başlıklar incelendiğinde özellikle veri güvenliği, rol tanımları, organizasyon yapıları başlıkları yoğunluktadır. Belirli aralıklarla güncellenen politikalar, yönetsel süreçlere uyum ve güncellik sunmaktadır. Aynı zamanda politika yaşam döngüsünden ve yönetişim olgunluğundan bahsedilebilir. Örneğin St. Andrews Üniversitesi ve Andrews Üniversitesi gibi üniversitelerde, politika belgelerinin her versiyonu için tarih, içerik değişikliği ve katkıda bulunan makamları şeffaf biçimde listelemiştir. Bu durum hem iç denetim hem de dış değerlendirme açısından üst düzey izlenilebilirlik sağlamaktadır.

Chapel Hill'deki Kuzey Carolina Üniversitesi, veri yönetişimi modelini üç düzeyli yapıdan dört düzeye çıkararak rollerin tanımını ve teknik sorumlulukları yeniden şekillendirmiştir. Güney Carolina Üniversitesi, yönetim sorumluluğunu farklı birimlere devretmiş, program adlarını ve şematik yapısını değiştirmiştir. Bu örnekler üniversitelerin dijital dönüşüm süreçlerine hızlı tepki verdiğini göstermektedir.

Revizyonlarda içerik güncellemesinin yanında kurumsal hiyerarşiyi yansıtan bir yapıdan söz edilebilir. Politika metinlerinde Başkanlık Kabinesi / Konseyi (President's Cabinet / Council), Baş Bilgi Yöneticisi (Chief Information Officer, CIO), Üniversite Sekreteri (University Secretary), Mütevelli Heyeti (Board of Trustees) başlıklarının onay makamı olarak geçtiği fark edilmiştir. Bu durum üst düzey yöneticilerin politikaları sahiplendiği ve stratejik karar alma aşamasında kullanabileceği anlamına gelmektedir. Üst belge hiyerarşisi kuran Güney Methodist Üniversitesi, tüm iç politika belgeleriyle çelişki durumunda Üniversite Politika Kılavuzu'nu (University Policy Manual) esas alınacağını belirtmiştir.

Bazı üniversiteler ise revizyon nedenleri ile açıklamıştır. Revizyon nedenlerinin iç politikaların uyumu ve mevzuat bütünlüğü için yapılması mümkün görülmektedir. Güney Carolina Üniversitesinde program adı değişikliği, erişim yetkilerinin yeniden dağıtılması, politika şablonuna uygunluk gibi nedenlerle revizyon yapılmıştır. Australian Catholic Üniversitesi'nde ACU Veri Stratejisi (ACU Data Strategy) kapsamındaki araştırma ve tartışmalar sonucunda revizyona gerek görülmüştür. Utah Üniversitesinde hem düzenleyici güncellemeler hem de dilin sadeleştirilmesi (editorial revisions) gibi iki ayrı revizyondan söz edilmiştir.

**Alakalı İçerikler**

1. Yasal Düzenlemeler

    - ABD'deki örnekler: HIPAA, FERPA, Federal Bilgi Güvenliği Yönetim Yasası[37] (Federal Information Security Management Act, FISMA), Gramm-Leach-Bliley Yasası[38] (Gramm-Leach-Bliley Act, GLBA), Engelli Amerikalılar Yasası[39] (Americans with Disabilities Act, ADA), Kimlik Hırsızlığına Karşı Kırmızı Bayraklar Kuralı[40] (Identity Theft Red Flags Rule) gibi federal yasa ve yönetmelikler veri güvenliği, sağlık, eğitim ve tüketici haklarına ilişkin çerçeve sağlamaktadır.
    - Avustralya ve BK örnekleri: Gizlilik Yasası[41] (Privacy Act), GDPR, Bilgi Edinme Özgürlüğü Yasası[42] (Freedom of Information Act) gibi düzenlemeler daha çok veri koruma, şeffaflık ve kamuya erişim konularıyla ilişkilidir.

2. Kurumsal Politika ve Standartlar

    - Bilgi Güvenliği Politikası (Information Security Policy)
    - Veri Sınıflandırma Politikası (Data Classification Policy)
    - Teknoloji Kaynaklarının Kabul Edilebilir Kullanımı Politikası (Acceptable Use of Technology Resources)
    - Kayıt Yönetimi Politikası (Records Management Policy)

3. Kurumsal Yönetişim Belgeleri

    - Veri Yönetişimi Komitesi Yönergesi (Data Governance Committee Charters)
    - Veri Sorumluluğu Çerçeveleri (Stewardship Frameworks)
    - Risk Yönetim Protokolleri (Risk Management Protocols)

37 Kamu kurumlarının bilgi sistemleri için bilgi güvenliği politikaları, standartları ve rehberlerinin uygulanmasını zorunlu hâle getiren bir federal yasadır.

38 Finansal kurumların, müşterilerinin kişisel finansal verilerini toplama, kullanma, paylaşma ve koruma süreçlerini düzenlemek ve veri gizliliğini güvence altına almaktır.

39 Fiziksel, zihinsel veya duyusal engeli olan bireylerin yaşamın her alanında ayrımcılığa uğramadan eşit fırsatlara sahip olmalarını sağlamak ve erişilebilirliği güvence altına almaktır.

40 Finansal işlemlerde veya müşteri hesaplarında kimlik hırsızlığına işaret eden uyarı sinyallerini ("kırmızı bayraklar") tespit etmek, bunlara karşı önlem almak ve olayları yönetmek için kurumların bir kimlik hırsızlığı önleme programı oluşturmasını zorunlu kılar.

41 Federal kurumların topladığı bireysel verilerin kötüye kullanımını önlemek, veri sahiplerinin verileri üzerinde bilgi edinme, düzeltme ve itiraz hakkını güvence altına almak.

42 Federal kurumlarının faaliyetlerini şeffaflaştırmak, vatandaşların hükümet hakkında bilgi edinme hakkını yasal güvence altına almak ve kamu yönetiminde hesap verebilirlik sağlamaktır.

4. Eğitim, Farkındalık ve Davranış Belgeleri

   - Eğitim Kılavuzları (Training Manuals), Personel/Öğrenci Davranış Kuralları (Staff/Student Code of Conduct), Gizlilik Beyanları (Confidentiality Attestations) gibi belgeler, politika metinlerinin normatif altyapısını oluşturmaktadır.
   - Kurum içi veri okuryazarlığını ve etik davranışı hedefler.

5. Ulusal ve Kurumsal Veri Stratejileri

   - Veri Yönetimi Planları (Data Management Plans, DMP) veya Veri Stratejileri gibi belgelere yapılan atıflar, politikanın yalnızca koruma amacı taşımadığını, veriyi etkin ve stratejik kullanma amacını ortaya koymaktadır.

Veri yönetişimi politika metinlerinin yasal düzenlemelerle bağlantılı şekilde sunulması, uyum, hesap verebilirlik, dış denetim gibi konulara katkı sağlamaktadır. Aynı zamanda birden fazla belge türü ile ilişkilendirilmesi çok boyutlu bakış açısı sağlamaktadır. Örneğin James Cook Üniversitesi 20'den fazla belge ve yasa ile bağ kurmuştur. Alaska Üniversitesinin politikası, tüm ABD federal kurumlarının DMP yönergelerine link vererek çok kaynaklı regülasyon takibi[43] sağlamaktadır. Montana Eyalet Üniversitesi Olay Raporlama Standartları (Incident Reporting Standards) gibi prosedürleri de dahil etmiştir.

**Politika Metni**

Politikaların bu bölümü, özellikle veri sınıflandırması, sorumluluk dağılımı, veri güvenliği, erişim ilkeleri, yaşam döngüsü yönetimi ve hukuki uyum gibi temel eksenlerde yapılandırılmıştır.

Üniversitelerin büyük bir bölümü verilerini Genel (Public), Korunan (Protected), Gizli (Confidential), Özel (Private) olmak üzere sınıflandırmıştır. Aynı zamanda veri sınıflandırma işlemleri verilerin erişim, depolama ve imha süreçlerini belirlemektedir. Güney Utah Üniversitesi verileri üç düzeye ayırarak sınıflandırmıştır. Veri tipine özgü protokoller tanımlayarak yasal, etik ve kurumsal sınırları belirlemiştir.

Veri sahipliği ve yönetişim rolleri, Veri Sorumlusu, Teknik Veri Sorumlusu, Veri Sahibi, Veri Kullanıcısı olarak tanımlanarak teknik, yönetsel ve operasyonel sorumlulukları belirtilmiştir. Örneğin, Montana Eyalet Üniversitesi farklı kampüslerindeki yönetsel pozisyonlar için Veri Sorumlusu tanımlamış ve görevleri merkezden atamıştır.

43 Bir kurumun, farklı kurumlar, ülkeler, sektörler ve konular düzeyinde yayınlanan birden fazla düzenleyici kaynağı sistemli bir şekilde izleme, analiz etme ve uygulama sürecidir.

Tüm üniversitelerde erişim yetkilendirmesi, şifreleme, iki faktörlü kimlik doğrulama, uzaktan bağlantı güvenliği gibi teknik önlemler yer almaktadır. Central Arkansas Üniversitesi, bireysel cihazlarda hassas verilerin depolanmasını yasaklamakta ve veri envanteri yapılmasını zorunlu tutmaktadır.

Politikalarda CIO, Bilgi Güvenliği Sorumlusu (Chief Information Security Officer, CISO), Veri Yönetişimi Kurulu ve Risk Yönetim Komiteleri (Risk Management Committee) gibi karar mekanizmalarına sıkça yer verilmiştir. Güney Utah Üniversitesi, yönetişim rollerini kapsamlı bir yapı içinde tanımlamış, Veri Konseyi (Data Council) ve Risk Yönetim Komitesi gibi kurullar aracılığıyla koordinasyon modeli kurmuştur.

Metinde şeffaflık, hesap verebilirlik, veri bütünlüğü, karar alma süreçlerinde veri temelli yaklaşım ve sürdürülebilirlik ilkeleri öne çıkmaktadır. Wisconsin Üniversitesi, yönetişim ilkelerini ISO standartlarına benzer bir çerçevede (örneğin, şeffaflık, tutarlılık, erişilebilirlik) yapılandırmıştır.

Ödeme Kartı Endüstrisi[44] (Payment Card Industry, PCI), FERPA, HIPAA gibi yasal düzenlemelere uyum vurgulanmakta, güvenlik açıklarının bildirilmesi zorunlu tutulmakta ve veri ihlallerine yönelik tepki planları yapılandırılmıştır. Utah Üniversitesi, veriye erişimde gereklilik ilkesi [45] (need-to-know) ilkesini esas alarak hem gizliliği hem de kaynak verimliliğini önceleyen bir yaklaşım sergilemektedir.

Politika metni olarak adlandırılan bölümde kurumsal sorumluluk alanlarının tanımlanması, yönetimsel süreçlerin düzenlenmesi yasal ve etik uyumluluğun sağlanması gibi konular başka bölümlerde de yer almaktadır. Bazı politika metinlerinde ayrı bir başlık açmak yerine tek bir başlık altında birden fazla başlık toplanmıştır. Bu durumda olan politikaların bazı başlıkları daha genel anlamda aldığını söylemek yanlış olmaz. Tablo 5'te politika metni başlığı altında geçen üniversitelere özgün uygulamalar sunulmuştur. Aslında Tablo 5'e göre veri güvenliğini sağlayan farklı durumlar için uygulanan önlemleri görülmektedir.

44 Ödeme kartı endüstrisi banka kartı, kredi kartı, ön ödemeli kart, e-cüzdan, ATM ve POS kartlarını ve ilgili işletmeleri ifade eder.

45 Bir kişinin ya da birim çalışanının yalnızca görevini yerine getirebilmesi için zorunlu olan minimum bilgiye erişebilmesini öngören bilgi erişim ilkesidir. Yani, herhangi bir veri ya da bilgiye erişim, kişinin iş tanımı gereği bu bilgiye gerçekten ihtiyaç duyması durumunda verilir.

**Tablo 5**

*Politika Metninde Geçen Özgün Uygulamalar*

| Üniversite | Özgün Uygulama |
|---|---|
| **Chicago Üniversitesi** | Kredi kartı verileri için özel politika ve bağımsız denetim süreci |
| **Wesleyan Koleji** | Google Apps[46] entegrasyonu ve FERPA uyumu üzerinden yapılandırılmış şifreleme kuralları |
| **Güney Florida Üniversitesi** | Üst veri (metadata) yönetimi ve kurumsal veri modelleme zorunluluğu |
| **Concord Üniversitesi** | Harici veri talep süreçleri için yazılı onay ve yasal risk değerlendirme prosedürü |
| **Arkansas Üniversitesi** | Hassas veriyle ilgili cihaz düzeyinde şifreleme, transfer ve imha zorunluluğu |

## Veri Yönetimi ve Kalitesi

Politikaların bu bölümünde veri yönetimindeki roller, komiteler ve ofisler ile yatay ve dikey yapı kurulmaya çalışılmıştır. Roller arası ayrımlar sayesinde hem teknik hem yönetsel sorumluluklar netleştirilmiştir. Aynı zamanda veri mülkiyeti ve sorumluluk alanı tanımlanmaya çalışılmıştır. Örneğin, New York Üniversitesi, tüm idari verilerin üniversiteye ait olduğunu belirtmiştir. Bu varlık üzerindeki sorumluluğu Veri Vekili ve Veri Sorumlusu gibi rollere dağıtmıştır.

Verilerin sınıflandırması ve erişim ile ilgili düzenlemelere yer verilmiştir. Veriler genellikle düşük, orta ve yüksek risk kategorilerine ayrılmakta ve her seviyeye uygun güvenlik önlemleri tanımlanmaktadır. Hertfordshire Üniversitesi, veri türlerini gizlilik derecesine göre sınıflandırmakta ve erişim yetkilerini bu sınıflamaya göre düzenlemektedir.

Veri kalitesi; doğruluk (accuracy), tutarlılık (consistency), güncellik (timeliness) ve güvenilirlik (reliability) gibi ölçütlerle somutlaştırılmıştır. Texas Christian ve St Andrews Üniversiteleri, veri kalitesi için özel kurul oluşturarak metrik yapılandırmalar geliştirmiştir.

Lamar Üniversitesi bünyesinde dikkat çekici bir uygulama vardır. Veriler, kullanım amacına göre "Resmi Raporlama İçin Sertifikalı", "İç Kullanım İçin Sertifikalı" ve "Taslak/Değerlendirme Aşamasında" göre sınıflandırılmaktadır. Bu yaklaşım ile veri güvenilirliğini kullanım bağlamına göre ayrıştırmakta ve yanlış veri kullanımının önüne geçmeye çalışmaktadır.

46 https://workspace.google.com/

**Prosedürler ve Standartlar**

Diğer başlıklarla benzer şekilde veri sınıflandırması, erişim kontrolleri, güvenlik uygulamaları, rol dağılımı ve sistem yönetimi gibi başlıklarda kurumsal veri yönetişiminin bütüncül bir çerçevesini sunmaktadır. Aslında politika metinleri içinde başlıklar farklı adlandırılmış olsa da içeriğin ana hatları benzer şekilde geliştirilmiştir. Aşağıda bu başlık altındaki özgün uygulamalara yer verilmiştir.

Indiana Üniversitesi, veri sınıflandırmasını üç düzeyde (Kamu, Üniversite-İç, Kritik) yapılandırmakta ve her sınıfa özgü erişim kontrolü uygulamaktadır. Kurum, veri görünürlüğü (data view) ile sınıflandırma arasında ayrım yaparak, bazı durumlarda kullanıcıya veri erişimi yetkisi verirken veri değiştirme izni vermemektedir. Uzaktan erişim sadece VPN[47] aracılığıyla sağlanmakta, kritik veriler için şifreleme ve loglama zorunlu tutulmaktadır.

Drake Üniversitesi, veri yönetişimi rollerini ayrıntılı biçimde tanımlayarak fakülte üyelerini kendi akademik verilerinin Veri Sorumlusu olarak konumlandırmaktadır. Kurum, veri sahibi, koruyucu ve kullanıcı rollerini iş birimi düzeyinde belirlemekte ve her rol için görev tanımı, yetki düzeyi ve sorumluluk alanını açık biçimde ilişkilendirmektedir. Böylece, yönetişim uygulamalarını yerinde ve katılımcı biçimde yürütmektedir.

Oregon Eyalet Üniversitesi, veri erişimini gereklilik ilkesi temelinde yapılandırmakta, tüm erişim izinlerini işleve dayalı olarak belirlemektedir. Üç katmanlı veri sınıflandırması (Gizli, Hassas, Kamu) uygulanmakta ve her düzeye göre farklı şifreleme, depolama ve erişim protokolleri tanımlanmaktadır. Kurum aynı zamanda erişim talepleri için form tabanlı onay süreci işletmektedir.

Delaware Üniversitesi, veri yönetişimi uygulamalarını işlevsel alanlara göre sınıflandırarak her alan için ayrı bir yönetişim modeli geliştirmiştir. Örneğin, öğrenci işleri, insan kaynakları ve mali işler gibi fonksiyonlar için bağımsız veri sorumluları atanmıştır. Kurum, stratejik (policy-level), operasyonel (management-level) ve teknik (implementation-level) düzeylerde ayrıştırılmış roller üzerinden çok katmanlı bir yönetişim yapısı kurgulamaktadır.

William Paterson Üniversitesi, veri kalitesini sürdürülebilir kılmak amacıyla veri görünürlüğü ilkesini sistemleştirmiştir. Kurum, her veri kümesinin kimler tarafından görüntülenebileceğini ve bu görünümün hangi versiyona dayandığını belgelemektedir. Ayrıca, hatalı veri tespiti durumunda düzeltme, yeniden dağıtım ve kullanıcı bilgilendirme gibi adımları içeren prosedürel süreçler uygulanmaktadır.

47 Virtual Private Network (Sanal Özel Ağ): Uzaktan erişim yoluyla farklı ağlara bağlanmayı sağlayan bir internet teknolojisidir.

Appalachian Eyalet Üniversitesi, veri yönetişimini iki düzeyli bir kurumsal yapı (Veri Mütevelli Heyeti ve Veri Sorumluluğu Konseyi) ile organize etmektedir. Bu yapı, yönetişimde hem karar alma hem uygulama süreçlerini işlevsel olarak ayrıştırmakta, aynı zamanda birimler arası koordinasyonu artırmaktadır. Kurum, standart işletim prosedürleri[48] (Standard Operating Procedures, SOP) ile her rol için belirli görev dizileri tanımlamıştır.

Üniversitelerin bu uygulamaları, veri yönetişiminin yalnızca güvenlik odaklı bir sistem olmaktan kurumsal sorumluluğun, etik kullanımın ve süreç standardizasyonunun sağlanmasına yönelik olduğunu göstermektedir.

**Politika Hakkında Bilgi**

Bu başlık politika metinlerine dair kısa özetler, uygulama tarihleri, sorumlu makamlar ve kurumsal yapı bilgilerini içermektedir. Bu yapı, veri yönetişimi belgelerinin hangi biçimsel ve içeriksel standartlar altında şekillendiğini göstermektedir.

Özellikle Austin'deki Teksas Üniversitesi örneğinde, veri yönetişiminin üniversite genelinde bir stratejiye dayanmadığı ve bu durumun veri kalitesi ve kurumsal hedeflerle uyumda sorunlara yol açtığı raporlanmıştır. Bu durum, stratejik uyumsuzlukların kurumsal veri yönetiminde sistemsel kalite sorunlarına yol açabileceğini ortaya koymaktadır.

Birçok üniversite bu bölümde Veri Sahibi, Veri Sorumlusu, Veri Kullanıcısı, Politika Onaylayıcı Kurullar gibi rollerin açık tanımını yapmaktadır. Örneğin, Columbia International Üniversitesinde bilgiye erişim, e-posta listeleri ve rapor yönetimi ayrı ayrı düzenlenmiş ve veriyle temas eden tüm personelin sorumluluk alanı net şekilde tanımlanmıştır.

Bazı üniversiteler (örneğin, Cardiff Metropolitan Üniversitesi, Suffolk Üniversitesi) politika belgelerinin düzenli olarak güncellendiğini, ilgili kurul ve onay organlarının devreye girdiğini bu bölümde belirtmektedir (bkz. Tablo 6).

48 Bir kurumda belirli bir işi veya süreci her seferinde tutarlı, verimli ve hatasız şekilde gerçekleştirmek için izlenmesi gereken adım adım talimatları içeren resmî dokümanlardır.

**Tablo 6**

*Politika Hakkında Bilgi Bölümünde Geçen Uygulamalar*

| Politika Özellikleri | Uygulama Biçimi |
|---|---|
| Onay Makamı | Rektörlük, akademik kurul, BT ofisi veya kalite komitesi |
| Sorumlu Birim | CIO, Veri Yönetişimi Ofisi, Kalite Ofisi |
| Gözden Geçirme Takvimi | Genellikle 2-4 yılda bir; bazı durumlarda yasa değişikliği sonrası olağanüstü gözden geçirme |
| Kapsam Tanımı | Kişisel veriler, idari veriler, öğrenci verileri, sistem kayıtları vb. |
| İhlal Durumları | Uyarı, disiplin süreci, işten çıkarma gibi yaptırımlarla açıkça ilişkilendirilmiş |

**Veri Erişimi ve Paylaşımı**

Bu başlık altında üniversiteler veri erişimini gereklilik ilkesi doğrultusunda sınırlandırmakta ve yalnızca görev tanımına uygun yetkiler tanımaktadır. Vincennes Üniversitesi örneğinde, hassas verilere erişim Veri Sorumluları tarafından onaylanmaktadır. SSN[49] gibi özel veriler için ise üst düzey yöneticilerden onay gerekmektedir. North Georgia Üniversitesi, altı ayda bir erişim kontrollerinin gözden geçirilmesini zorunlu tutmakta ve işten ayrılma gibi durumlarda beş iş günü içinde erişim iptali talep etmektedir. Güney Methodist Üniversitesi, veriye erişim için önce ilgili eğitimi almayı şart koşmakta ve Veri Sorumlusu onayı aramaktadır. Kuzey Iowa Üniversitesi, erişim yetkisinin yalnızca verilme amacıyla sınırlı olduğunu ve ikincil kullanımın yasaklandığını açıkça belirtmiştir.

Üniversite mensubu dışı kişi ya da kuruluşlarla veri paylaşımı, genellikle sözleşme veya uzlaşı belgesi (Memorandum Of Understanding[50], MOU) çerçevesinde yürütülmektedir. Montana Eyalet Üniversitesi, hassas veri paylaşımını yalnızca şifreli dosya transferi veya güvenli web hizmetleri aracılığıyla gerçekleştirmektedir. E-posta ile veri gönderimi yasaktır. Saint Thomas Üniversitesi, ülke dışına veri paylaşma ve yabancı uyruklu bireylerle paylaşım gibi durumlarda ihracat kontrol yasalarına dikkat çekmekte ve ön onay talep etmektedir. Vincennes Üniversitesi, güvenlik riski düşükse ya da akademik/iş gerekliliği varsa istisnai erişim izinlerinin üst yönetim tarafından verilebileceğini belirtmektedir.

49 Social Security Number (Sosyal Güvenlik Numarası): ABD vatandaşlarına ve yasal ikamet eden bireylere verilen, bireylerin kimliğini tanımlamak ve sosyal güvenlik işlemlerini yürütmek için kullanılan benzersiz 9 haneli bir numaradır.

50 "University of X" ile "University of Y" arasında yapılan MOU, ortak veri paylaşımı, lisansüstü araştırma desteği ve akademik yayın iş birliklerini kapsayan genel bir çerçeve sunmaktadır.

**Veri Güvenliği ve Gizliliği**

Üniversitelerin veri güvenliği ve gizliliğine yönelik politika uygulamalarını örnekleyen bir içerik sunmaktadır. Üniversiteler, veri türlerine göre sınıflandırma yaparak kamuya açık, hassas, gizli ve özel veri türlerine farklı koruma önlemleri getirmektedir. Bucknell Üniversitesi kamuya açık, hassas ve gizli veriler için çok katmanlı güvenlik düzeyleri oluşturmuştur. Her kategori, bulut depolama, basılı materyal, şifreleme ve fiziksel erişim gibi kriterlere göre korunmaktadır. Wollongong Üniversitesi veri sınıflamasını hassas (sensitive), sınırlı (restricted), korunan (protected), kontrollü (controlled) ve kamu (public) olmak üzere beş seviyede tanımlamıştır. Her seviyeye özgü teknik ve etik koruma standartları belirlenmiştir.

Maryland Üniversitesi, sistemler arası erişim izolasyonu[51], görev ayrılığı ilkesi[52], çevresel güvenlik tedbirleri ve yedekleme sistemleri gibi kapsamlı teknik önlemlerini öne çıkarmaktadır. Cleveland Eyalet Üniversitesi dış hizmet sağlayıcılarla yapılan sözleşmelerde veri gizliliği ve denetlenebilirliğe yönelik ayrıntılı hükümler sunmaktadır (örneğin veri ihlalinde yaptırımlar, veri imha taahhütleri ve sözleşme iptal hakları).

Kuzey Kentucky Üniversitesi ve Suffolk Üniversitesi, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü'ne (GDPR) tam uyum politikası geliştirmiştir. Bu kapsamda şeffaflık, veri öznesinin hakları (erişim, silme, düzeltme), otomatik karar verme süreçlerinde etki analizi yapılması gibi düzenlemeler vurgulanmaktadır.

Indiana Eyalet Üniversitesi ve Oregon Eyalet Üniversitesi, veri ihlali durumlarında izlenecek adımları ayrıntılı olarak tanımlamıştır. Bu adımlar olay tespiti, ilgili makamlara bildirim, teknik müdahale ve kriz yönetimi, ihlal sonrası denetim süreçlerini kapsamaktadır. Bu, kurumsal itibarın korunması ve yasal yaptırımlardan kaçınılması açısından önleyici ve tepkisel güvenlik anlayışının benimsendiğini göstermektedir.

**İlkeler ve Etik**

Bu bölümde veriyle etkileşimde bulunan tüm aktörlerin (veri sahibi, veri sorumlusu, kullanıcı) etik yükümlülükleri, kurumsal ilkeler ve ihlal durumlarıyla ilgili düzenlemeler yer almaktadır. Kavramsal yapı; sorumluluk, şeffaflık, gizlilik, hesap verebilirlik ve etik kullanımı temel alan bir yönetişim anlayışına dayanmaktadır.

51 Bir bilgi sisteminde kullanıcıların yalnızca yetkili oldukları verilere veya kaynaklara erişebilmesini, yetkili olmadıkları bölümlere ise erişememesini sağlayan bir güvenlik ilkesidir.

52 Bir işlemin tüm adımlarının tek bir kişi veya birim tarafından yapılmasını engelleyen, bunun yerine yetki, sorumluluk ve kontrollerin birden fazla kişiye dağıtılmasını öngören temel bir bilgi güvenliği ve iç kontrol ilkesidir.

Cornell Üniversitesi, yönetimsel gözetleme[53] (administrative voyeurism), yetkisiz veri paylaşımı, çıkar çatışması ve veri manipülasyonu gibi etik dışı davranışları açıkça yasaklamaktadır. Her veri kullanıcısının, yalnızca göreviyle doğrudan ilgili ve yetkilendirildiği veriye erişebileceği belirtilmiştir. Politika, veri sorumlularının ve yöneticilerinin kararlarının itiraz süreçlerini de düzenlemekte, kurumsal denge ve itiraz mekanizması tanımlamaktadır. Bu örnekten politikanın bireysel davranışları düzenleyen bir etik sistem olarak yapılandırıldığı düşünülebilir.

Connecticut Koleji, verinin kötüye kullanımını sadece kurumsal bir ihlal olarak görmemektedir. Aynı zamanda hukuki bir risk alanı olarak değerlendirerek her kullanıcıyı doğrudan bireysel sorumluluğa dahil etmektedir. Güvenlik ihlallerinin, farklı paydaşlar (öğrenci, çalışan, dış kullanıcı) için ayrı ayrı soruşturulması ve sonuçlarının disiplin süreçleriyle ilişkilendirilmesi dikkat çekicidir.

Arcadia Üniversitesi, veri kullanımında kurumsal risk dereceleri tanımlamıştır (örneğin Seviye 1 – Ciddi Risk → Seviye 4 – Düşük/Hiçbir Risk). Bu sınıflandırmaya göre erişim ve şifreleme gereklilikleri belirlenmiştir. Örneğin yüksek riskli verilerin paylaşımı sadece yetkili ve şifreli ağlar[54] (encrypted networks) üzerinden yapılabilmektedir.

Fullerto'daki California Eyalet Üniversitesi, politikasını misyonla uyum, şeffaflık, meşru amaç, güvenlik, mahremiyet, doğrulama, eğitim ilkeleri ile arasında köprü kurarak yapılandırmıştır.

**Eğitim ve Diğer**

Üniversiteler tüm çalışanlara yönelik zorunlu veri koruma ve gizlilik eğitimi sunmakta, bu eğitimlerin genellikle 2 ila 3 yılda bir güncellenmesi gerektiğini belirtmektedir. Örneğin, Suffolk Üniversitesi ve Royal Sanat Koleji, tüm personelin her üç yılda bir veri koruma eğitimini şart koşmaktadır.

Eğitim programları genellikle veri sahibi, veri sorumlusu, veri kullanıcısı gibi rollerin ihtiyaçlarına göre farklılaştırılmaktadır. Oklahoma Üniversitesi, veri yönetişimi rollerine atanmış personel için ayrıntılı bir eğitim takvimi uygulamaktadır. İlk atamadan itibaren 30–365 gün içinde çeşitli modüller tamamlaması beklenmektedir.

53 Kamu veya özel sektör kurumlarının, bireylerin kişisel yaşamlarına dair gereksiz veya aşırı detaylı bilgilere erişme ve bu bilgileri izleme eğilimi anlamına gelmektedir.

54 Veri iletimini güvenli hale getirmek için verilerin şifrelenerek (kriptolanarak) gönderildiği ağlardır. Bu tür ağlarda veriler, yalnızca doğru anahtara sahip alıcı tarafından çözülebilir.

Eğitimler verilirken çevrimiçi platformlar (ör. Moodle[55], MyReview[56]) üzerinden verilmesi benimsemiştir. St Andrews Üniversitesi ve Andrews Üniversitesi, eğitimleri hem işe giriş sürecinde hem de düzenli mesleki gelişim kapsamında döngüsel olarak sunmaktadır.

Kurumlar, çalışanların eğitimlere katılımını kurumsal sistemlerde kayıt altına almakta ve zamanında tamamlanmayan eğitimleri üst yönetime bildirmektedir. Kuzey Georgia Üniversitesi, eğitim katılımlarını periyodik olarak denetlemekte ve eğitim materyallerinin güncel tutulmasını zorunlu kılmaktadır.

Hassas veriyle çalışan personel (ör. sağlık verisi, öğrenci kayıtları) için ek eğitimler düzenlenmektedir. Tennessee Wesleyan Üniversitesi ve George Mason Üniversitesi, yüksek riskli verilere erişimden önce özel güvenlik eğitimi zorunluluğu getirmiştir.

**İş Süreci Unsurları**

Üniversitelerin politika metinlerinde çok az geçen operasyonel unsurlar olarak adlandırılan ve günlük işleyişini sağlayan uygulama, süreç ve araçların bir araya toplandığı bölümdür. Veri yönetişimi politikalarında roller net biçimde tanımlanmış olsa da bu rollerin operasyonel düzeyde nasıl etkileşim kurduğu, ortak süreçlerde nasıl iş birliği yaptığı çoğu zaman açıklanmamaktadır. Üst veri, veri bağlantısı[57] (data linkage), veri çıkarımı[58] (data inference) ve arşivleme, üst veri araçları, kayıt yönetimi, karar alma süreçleri ve veri kalite yönetimi gibi alanlara odaklanmaktadır.

Üst veri, veri yaşam döngüsünün her aşamadaki verinin izlenebilir, yorumlanabilir ve denetlenebilir hale getirilmesini sağlamaktadır. Wichita Eyalet Üniversitesi ve Austin'deki Teksas Üniversitesi veri yönetişimi politikalarında üst veriyi ayrı bir başlık altında ele almıştır. Wichita Eyalet Üniversitesi, iş birimleri arasında ortak anlayış yaratma, veri uyumluluğu ve entegrasyonu sağlama, düzenleyici gerekliliklere uyumu kolaylaştırma amacıyla üsveriyi yönetimsel bir araç olarak kullanmaktadır.

Austin'deki Teksas Üniversitesi, üst veri paydaş rolleri ve sorumluluklarının tanımlanması, üst veri bileşenlerinin ve kategorilerinin belirlenmesi, ortak bir üst veri deposu kurulması, yaşam döngüsü yönetimi (oluşturma, güncelleme, silme), sorgulama, raporlama ve analiz kabiliyeti geliştirme gibi için stratejik çerçevede kullanılabileceğini önermiştir. Bu sayede de karar verme süreçlerine destek olacağı öngörülmektedir. Aynı

55 https://moodle.org/

56 https://my.reviewr.com/

57 Farklı kaynaklardan elde edilen veri kümelerinin, aynı birey, kuruluş, nesne ya da olayla ilgili bilgileri birleştirmek üzere eşleştirilmesi sürecidir.

58 Doğrudan gözlemlenmeyen veya açıkça belirtilmemiş bilgilerin, mevcut verilerden istatistiksel, analitik ya da algoritmik yöntemlerle tahmin edilmesi ya da türetilmesi sürecidir. Bu süreç, özellikle büyük veri analitiği, yapay zekâ, makine öğrenmesi ve veri madenciliğinde önemli bir yer tutar.

zamanda Austin'deki Teksas Üniversitesi, üst veri yönetiminde dağınık bir yapıya sahip olduğunu, bu durumun kurumsal verilerin tanımlanması ve yeniden kullanımı önünde ciddi engeller oluşturduğunu belirtmektedir. Data Cookbook[59] (Veri Pişirme Kitabı) adlı bir üst veri aracı projeye dahil edilmiştir. Ama uygulaması sürdürülememiştir.

Griffith Üniversitesi veri bağlantısı yöntemlerini belirli şartlara bağlamıştır. Deterministik[60] (doğrudan eşleşme), olasılıklı eşleşme[61] (probabilistik), ortak tanımlayıcılar[62] (common identifier), veri kimliksizleştirme[63] (de-identification) yöntemlerinin her biri, veri hassasiyetine ve yasal sınıflandırmalarına göre değişmektedir. Üniversite, kişisel verilerin mahremiyetini korurken aynı zamanda araştırma ve analiz süreçlerine katkı sunacak güvenli veri birleştirme yöntemleri geliştirmiştir.

Teksas Tech Üniversitesi, veri rollerinin içinde bulunduğu kayıt yönetim politikaları ile kurumsal hafıza ve yasal uyumu sistematikleştirilmiştir.

Kuzeybatı Purdue Üniversitesi ortak veri dili inşa edebilmek amacıyla üst veri yönetimi aracılığıyla kurumda veri anlam birliği ve kalite standardizasyonu sağlanmaktadır. Data Cookbook isimli yazılım aracı, veri tanımları, veri sözlüğü, rapor talepleri, süreç şemaları ve iş birliği panelleri gibi çok yönlü bir üst veri yönetim altyapısı sunmaktadır.

Doğu Stroudsburg Üniversitesi karar süreçlerinde çoğulcu veri yönetimi anlayışına örnek olmuştur. Veri yönetişimi komiteleri bünyesinde kararlar oy birliği ya da 2/3 çoğunlukla alınmaktadır. Bu yaklaşım ile katılımcı yönetişim kültürünü sağlamaktadır.

Montana Eyalet Üniversitesi raporlama sürecinde veri bütünlüğü ve güvenlik ilkeleri ile bütünleşmiştir. Örneğin hassas veriler özel izin olmadan raporlara dahil edilmemektedir. Verileri tekrar kullanımı izne tabidir ve sistem dışı paylaşım yasaktır.

59 Veri yönetişimi, veri kalite yönetimi ve veri tanımı yönetimi alanlarında kullanılan, kurumsal düzeyde bir veri sözlüğü (data glossary) ve iş tanımı (business definitions) platformudur.

60 Tam ve kesin bir eşleşme şeklidir. Genellikle iki veya daha fazla veritabanındaki kayıtlar, benzersiz tanımlayıcılar (örneğin T.C. Kimlik No, öğrenci numarası, sigorta numarası) veya belirli bir dizi değişkenin birebir eşleşmesiyle bağlanır.

61 Kayıtların aynı kişi ya da varlıkla ilişkili olma olasılığını hesaplayan istatistiksel yöntemleri kullanır. Tam eşleşme olmasa bile, benzerlik skorları üzerinden karar verilir.

62 Farklı veri setleri ya da sistemlerde bulunan kayıtların aynı birey, nesne ya da olayla ilişkili olduğunu belirlemek amacıyla kullanılan ortak veri alanlarıdır.

63 Kişisel verilerin bireylerle ilişkilendirilemeyecek hâle getirilmesi işlemidir. Amaç, verinin analitik, istatistiksel veya araştırma amacıyla kullanılabilirliğini sürdürürken, veri sahibinin kimliğinin korunmasıdır.

## Sonuç ve Öneriler

Veri yönetişimi, sadece bilgi teknolojileri birimlerinin yürüteceği bir süreç olmaktan çıkmıştır. Tüm akademik, idari ve stratejik birimlerin ortak sorumluluğuna dayalı çok katmanlı bir yönetişim sistemi haline gelmiştir. Veri, karar alma süreçlerini belirleyen, kurumsal sürdürülebilirliği besleyen ve hukuki/etik sorumluluk doğuran stratejik bir varlık olarak tanımlanmaya başlamıştır.

Bu bağlamda, üniversitelere ait veri yönetişimi politika metinlerinde en dikkat çeken unsur, kurumsal rollerin, sorumlulukların ve yapısal bileşenlerin açık biçimde tanımlanmış olmasıdır. Literatürde veri yönetişiminin en güçlü katmanı "tanımlama" aşamasıdır. Üniversitelerdeki politika belgelerinin aynı özelliği göstermesi şaşırtıcı bir sonuç değildir. Veri Yönetişimi Enstitüsü Çerçevesi ve DAMA-DMBOK[64] Olgunluk Modeli ile karşılaştırıldığında bazı güçlü yönler ve eksiklikler dikkat çekmektedir. Veri Yönetişimi Enstitüsü Çerçevesi modelinde vurgulanan temel bileşenler (roller, politikalar, standartlar, süreçler ve ölçümleme) ile DAMA-DMBOK'un olgunluk boyutları (strateji, kalite, güvenlik, metadata, yaşam döngüsü yönetimi, organizasyon) incelendiğinde, üniversite politikalarının özellikle roller ve sorumlulukların tanımlanması, politika metinleri ve prosedürlerin oluşturulması ve veri güvenliği/saklama konularının düzenlenmesi bakımından güçlü olduğu görülmektedir. Ancak bu olumlu görünüme rağmen, belgelerde ortak bir terminoloji ve standart kavramsal çerçevenin bulunmadığı göze çarpmaktadır. Aynı role farklı isimler verilmesi (ör. veri sahibi, bilgi yöneticisi, veri yöneticisi) veya benzer isimlerle farklı işlevlerin tanımlanması, kurumsal karşılaştırmaları ve yatay entegrasyonu zorlaştırmaktadır.

Daha da önemlisi, tanımlanan rollerin birbirleriyle nasıl etkileşime gireceği, ortak karar alma mekanizmaları içinde nasıl yer alacağı ve yetki-sorumluluk sınırlarının olası çakışmalarda nasıl yönetileceği çoğu belgede açıkça belirtilmemiştir. Bu durum, özellikle veri kalitesi yönetimi, üst veri tanımlama, raporlama ve veri erişimi gibi çok aktörlü süreçlerde yetki bulanıklığı, işlem tekrarları ya da sorumluluk devri belirsizliği gibi sorunlara neden olma potansiyeli taşımaktadır.

Yine de mevcut politika metinleri "rolleri tanımlama" açısından olgunluk gösterdiği söylenebilir. Ancak bu roller arası yatay entegrasyonu, işbirliği senaryolarını ve sorumluluk paylaşım modellerini yapılandırma açısından önemli eksiklikler barındırmaktadır.

Veri yönetişiminin uygulama aşamasında, kurumlar veri kalitesi ve güvenliğini sağlamak amacıyla prosedürler ve teknik standartlar geliştirmiştir. Bu çerçevede, veri üst verileri yalnızca teknik bir kayıt unsuru olarak ele alınmamıştır. Aynı zamanda işlevsel,

64 https://dama.org/learning-resources/dama-data-management-body-of-knowledge-dmbok/

analitik ve yapısal boyutlarda sınıflandırılarak yönetişim süreçlerine entegre edilmiştir. Uygulamalarda şifreleme protokolleri, VPN erişimi ve erişim kontrol mekanizmaları yaygın olarak kullanılarak veri gizliliği ve güvenliği teknik önlemlerle desteklenmektedir.

Ancak bu sistematik altyapıya rağmen, yeni nesil veri türleri çoğunlukla yönetişim kapsamı dışında kalmaktadır. Özellikle yapay zekâ (artificial intelligence, AI) ile üretilen veriler, öğrenci analitiği çıktıları ve büyük veri kaynaklı türetilmiş bilgiler, mevcut politika metinlerinde sınırlı biçimde yer almakta ya da tamamen atlanmaktadır. Bu durum, veri yönetişiminin gelişen teknolojik ortamlarla uyum kapasitesinin henüz kurumsallaşmadığını ve yönetişim kapsamının klasik veri yapılarıyla sınırlı kaldığını göstermektedir.

Veri yönetişimi belgelerinde eğitim ve farkındalık uygulamalarının rol bazlı, çevrimiçi ve zorunlu biçimde tasarlanması, katılım oranlarını artırmakta ve kurumsal işleyişe bütünleşmeyi kolaylaştırmaktadır. Bu tür yapılandırılmış yaklaşımlar, veriyle etkileşime giren tüm rollerin sorumluluklarının farkında olmasını ve kurumsal politikaları içselleştirmesini desteklemektedir. İncelenen üniversitelerin önemli bir kısmında veri eğitimi ve farkındalık faaliyetlerine ilişkin sistematik bir düzenleme bulunmamaktadır. Bu eksiklik, veriyi kullanan bireylerin etik davranışları, veri güvenliğine ilişkin duyarlılığı ve sorumluluk bilincini olumsuz yönde etkilemektedir. Benzer şekilde üst veri yönetimi, veri kalitesi, stratejik planlama ve etik kullanıma ilişkin başlıkların düşük oranda temsil edilmesi, hem Veri Yönetişimi Enstitüsünün *ölçümleme ve olgunluk* boyutunun hem de DAMA-DMBOK'un *strateji ve kalite* bileşenlerinin yeterince kurumsallaşmadığını ortaya koymaktadır. Bu durum, üniversitelerin veri yönetişimi politikalarında olgunluk düzeyinin sınırlı kaldığını ve daha çok uyum ve operasyonel süreçlerin düzenlenmesine yoğunlaşıldığını göstermektedir.

Üniversite içinde veri eğitimi ve farkındalığına ilişkin kurumsal yatırımın yetersizliği, veri yönetişimini teknik bir sistem olarak algılayan dar bir perspektife yol açmaktadır. Kültürel dönüşüm, veri okuryazarlığı, hesap verebilirlik ve etik kullanıma yönelik farkındalık gibi kritik boyutları geri plana itmektedir. Bu durum, veri yönetişiminin kültür ve davranış biçimleriyle desteklenmesi gerektiği gerçeğini ortaya koymaktadır.

Politika belgelerinde revizyon ve onay mekanizmalarının açık biçimde tanımlanmış olması, kurumların politika yaşam döngüsünü sürdürme konusunda belirli bir kurumsal olgunluk düzeyine ulaştığını göstermektedir. Bu durum, veri yönetişimi belgelerinin dönemsel olarak gözden geçirilen ve gerektiğinde güncellenen dinamik metinler olduğunu göstermektedir.

Ancak buna rağmen, veri yönetişimi uygulamalarının başarısını ölçmeye yönelik anahtar performans göstergeleri[65] (Key Performance Indicators, KPI), periyodik denetim takvimleri ve geribildirim mekanizmaları, çoğu politika belgesinde ya hiç yer almamakta ya da yüzeysel biçimde geçmektedir. Bu eksiklik, politika belgelerinin revize edilmesi sürecinde kanıta dayalı izleme, etki değerlendirme ve sürekli iyileştirme döngüsü kurma açısından önemli bir zafiyet yaratmaktadır. Aynı zamanda veri yönetişimi süreçlerinden "izleme" aşamasının doğru çalışmadığını göstermektedir.

Veri yönetişimi, yalnızca belirli sorumlulukların ve teknik düzenlemelerin tanımlanmasıyla yapılandırılmamalıdır. Aynı zamanda bu düzenlemelerin uygulama sonuçlarının sistematik olarak izlenmesi ve geri bildirim yoluyla iyileştirilmesi ile kurumsallaşabilir. Dolayısıyla KPI'ların, kullanıcı memnuniyeti ölçütlerinin, iç denetim raporlarının ve uygulama raporlarının politika döngüsüne entegre edilmemesi, yönetişim yapısının sürdürülebilirliğini ve hesap verebilirliğini zayıflatmaktadır.

**Tablo 7**

*Ülkelerin Veri Yönetişimi Yaklaşımı Farkları*

| Boyut | ABD | BK | Avustralya |
|---|---|---|---|
| Yönetişim Yapısı | Dağıtık, güçlü rol tanımlamaları | Merkezî yapılar daha yaygın, komite temelli karar alma süreci | Hibrit model: Yerel özerklik + üst düzey yönetişim kurulları |
| Yasal Çerçeve Etkisi | FERPA, HIPAA, GLBA gibi düzenlemeler belgelere yön vermekte | GDPR eksenli, güçlü kişisel veri hakları | Privacy Act ve OAIC66 rehberleri ile ulusal uyum ön planda |
| Veri Kalitesi | Sertifikasyon ve metrikler geliştirilmiş | Kalite denetimi vurgulanmakta ama genelde teknik değil süreç odaklı | Veri yönetişimi ile entegre, eğitim ve süreç tasarımı güçlü |
| Eğitim ve Farkındalık | Zorunlu eğitimler yaygın, rol bazlı içerik geliştirme dikkat çekmekte | Eğitim genel olarak bilgi güvenliğiyle entegre, detaylı yapıda değil | Eğitim modülleri düzenli ve kullanıcı dostu, izlenebilirlik vurgulanmakta |
| Etik ve Stratejik Vizyon | Teknik süreçten kopuk etik ilkeler açıkça tanımlanmış | Belgelerde etik, şeffaflık ve hesap verebilirlik ilkeleri | Etik, karar alma ve dış paylaşım politikalarıyla örtüşmekte |
| Üst veri ve Veri Envanteri | "Data Cookbook" gibi araçlarla desteklenen teknik üst veri yapıları | Veri kataloglar ile entegre kullanıcı dostu yapı | Hem stratejik hem operasyonel kararları destekleyen yapı |

65 Bir organizasyonun hedeflerine ne ölçüde ulaştığını değerlendirmek için kullanılan ölçülebilir metriklerdir. KPI'lar, stratejik, taktiksel ya da operasyonel düzeyde olabilir ve genellikle performansı izlemek, karar vermeyi desteklemek ve iyileştirmeleri teşvik etmek amacıyla kullanılır.

66 https://www.oaic.gov.au/

Tablo 7'den anlaşılabileceği üzere, üniversiteler yapı ve bağlamlarına göre kendi kurumsal ihtiyaçlarına uygun özgün veri yönetişimi yaklaşımları geliştirmiştir (Brous vd., 2016). Ülke bazında değerlendirildiğinde, veri yönetişimi politikalarının içeriksel öncelikleri ve yönetsel derinliği önemli farklılıklar göstermektedir.

ABD'ye ait politika belgelerinde, bilişim teknolojileri temelli uygulamaların, gelişmiş veri güvenliği önlemlerinin, sınıflandırma sistemlerinin ve risk temelli yaklaşımların belirgin biçimde öne çıktığı görülmektedir. Bu bağlamda, veriyi korumaya ve erişimi düzenlemeye yönelik teknik uygulamalar oldukça güçlüdür. Kurumsal düzeyde ise bağımsızlık ön plandadır. Her üniversite, kendi iç ihtiyaç ve önceliklerine göre özelleştirilmiş veri yönetişimi modelleri geliştirmektedir.

Öte yandan, BK'deki üniversitelerin veri yönetişimi politikaları, daha çok kişisel veri haklarına, şeffaflık, açık rıza ve kurumsal sorumluluk ilkelerine dayanmaktadır. Belgelerde, veri yalnızca teknik bir unsur ele alınmamıştır. Aynı zamanda etik, toplumsal sorumluluk ve kamu yararı çerçevesinde de ele alınmaktadır. Bu yönüyle veri yönetişimi değer temelli bir yaklaşımla yapılandırılmaktadır. Politika belgelerinde kurumsal olgunluk hedeflenirken daha standartlaştırılmış yapılar geliştirilmiştir.

Avustralya üniversitelerine ait politika belgelerinde ise, veri yönetişimi uygulamalarının kurumsal süreçlerle yüksek düzeyde uyumlu olduğu ve politikaların bütünsel bir yapı içinde geliştirildiği görülmektedir. Belgeler, ulusal yasal düzenlemelere (ör. Privacy Act) açıkça referans verirken, aynı zamanda kurumsal farklılıkları da gözeten esnek ve uyarlanabilir bir yönetişim yaklaşımı benimsemektedir. Bu yönüyle hem standartlaştırma eğilimi hem de kurum bazlı ihtiyaçlara yanıt verme kapasitesi dengeli biçimde yapılandırılmıştır.

Sonuç olarak, üniversitelerin veri yönetişimi politika metinleri kurumsallaşma yolunda önemli adımlar atmıştır. Özellikle tanımlama, güvenlik ve kurumsal rol dağılımı gibi alanlarda belirgin bir olgunluk düzeyine ulaşılmıştır. Buna karşın, izleme, değerlendirme, olgunluk ölçümü (maturity assessment), yeni veri türleri ve etik sorumluluk, stratejik yönler, kurum kültürü gibi konularda gelişime açık önemli boşluklar mevcuttur. Bu bağlamda aşağıda veri yönetişimi politikası geliştirecek üniversitelere bazı öneriler sunulmuştur:

- Kurumsal rollerin yalnızca tanımlanmasıyla yetinilmemelidir. Roller arası etkileşim senaryoları, karar alma zincirleri ve çatışma çözüm mekanizmaları politika metinlerine açık biçimde entegre edilmelidir.

- Veri yönetişimi bilgi teknolojileri bölümünün yanı sıra strateji, hukuk, etik ve akademik birimlerle çok paydaşlı komiteler aracılığıyla yürütülmelidir.

- Kurumlar, veri doğruluk, bütünlük, tutarlılık ve zamanlılık gibi kalite ölçütlerini içeren standart kalite tanımları geliştirmelidir.
- KPI'lar belirlenmeli ve bu göstergeler üzerinden veri kalitesi düzenli olarak izlenmelidir.
- Veri kalitesi sorunlarının raporlanmasına yönelik geribildirim mekanizmaları oluşturulmalıdır.
- Üst veri, teknik, işlevsel, analitik ve yönetsel boyutlarda da tanımlanmalı ve kurumsal karar destek sistemleriyle ilişkilendirilmelidir.
- Tüm kullanıcılar için erişilebilir bir veri sözlüğü (ör. *Data Cookbook*) oluşturulmalı ve düzenli güncellenmelidir.
- Veri erişim izinleri, rol temelli erişim kontrolü (role-based access control, RBAC[67]) olarak yapılandırılmalıdır. Hassas verilere erişim, veri sınıfına göre şifreleme ve log kayıtları ile denetlenmelidir.
- Gizlilik seviyeleri ve yasal sınıflandırmalar açıkça belirtilmelidir. Ulusal düzenlemelerle uyumluluğu sağlanmalıdır.
- Üniversitenin tüm sistemleri arasında veri akışı, dönüşümü ve saklanması sürecini gösteren veri mimarisi haritaları oluşturulmalı ve paydaşlarla paylaşılmalıdır.
- Farklı kaynaklardan gelen verilerin entegrasyonu için veri bağlantısı stratejileri ve veri gölleri (data lakes) yapılandırılmalıdır.
- Verilerin oluşturulmasından imhasına kadar tüm aşamalar için kapsamlı bir veri yaşam döngüsü politikası tanımlanmalıdır.
- Arşivleme, anonimleştirme ve imha süreçleri açık prosedürlerle desteklenmelidir.
- Üniversiteler, veri yönetimi olgunluk değerlendirmesi araçlarını kullanarak mevcut durumlarını haritalandırmalı ve gelişim planları oluşturmalıdır.
- Olgunluk seviyesi (ör. başlangıç, tanımlı, kurumsallaşmış, yönetilen, optimize edilmiş) yılda en az bir kez değerlendirilmelidir.
- Veri yönetişimi politikalarının tüm çalışanlar için zorunlu ve rol bazlı eğitim modülleriyle desteklenmesi gereklidir.
- Eğitim içerikleri veri etiği, kişisel veri koruma, veri kalitesi, sorumluluk ve risk bilinci gibi konuları da kapsamalıdır.
- Veriyle çalışan tüm birimlerin uyması gereken etik ilkeler bildirgesi hazırlanmalı, politika metinlerine eklenmelidir.

67 RBAC, kullanıcıların bir sistemde hangi kaynaklara erişebileceğini ve ne tür işlemler yapabileceğini rollerine göre sınırlandırmaktadır.

- Özellikle AI, öğrenci analitiği ve davranışsal veri gibi hassas alanlarda etik izleme ve veri koruma etki analizleri (data protection impact assessment, DPIA[68]) yapılmalıdır.
- Veri yönetişimi, kurumun stratejik hedefleriyle hizalanmalıdır. Stratejik planlarda veri kalitesi, analitik kapasite ve dijital dönüşüm yer bulmalıdır.
- Her yönetişim politikası, ölçülebilir hedefler ve belirlenmiş sorumlularla birlikte yapılandırılmalıdır.

**Çıkar Çatışması**

Çalışma esnasında kişisel ve finansal herhangi bir çıkar bulunmamaktadır.

**Yazarlık Katkısı**

Burcu Tığ Demir: Kavramsallaştırma, yöntem, veri toplama, veri analizi, görselleştirme, özgün ve gözden geçirilmiş taslakların yazılması ve düzenlenmesi.

Özgür Külcü: Kavramsallaştırma, yöntem, veri analizi, görselleştirme, denetleme, taslakları gözden geçirme ve düzeltme.

## Kaynakça

Abed, W. E., Brillant, P. ve Njonko, P. B. (2014). Governance of organizational data and information. Topi, H. ve Tucker, A. (Edt.), *Computing handbook* içinde (3. baskı). Chapman and Hall/CRC. https://doi.org/10.1201/b16768

Abraham, R., Schneider, J. ve vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Alhassan, I., Sammon, D. ve Daly, M. (2016). Data governance activities: An analysis of the literature. *Journal of Decision Systems*, *25*(sup1), 64–75. https://doi.org/10.1080/12460125.2016.1187397

Al-Badi, A., Tarhini, A. ve Khan, A. I. (2018). Exploring big data governance frameworks. *Procedia Computer Science, 141*, 271–277. https://doi.org/10.1016/j.procs.2018.10.181

Attard, J. ve Brennan, R. (2018). Challenges in value-driven data governance. H. Panetto, C. Debruyne, H. Proper, C. Ardagna, D. Roman ve R. Meersman (Edt.), *On the Move to Meaningful Internet Systems. OTM 2018 Conferences* içinde (ss. 546-554*)*. Springer International Publishing. https://doi.org/10.1007/978-3-030-02671-4_33

68 DPIA, özellikle yüksek risk içeren kişisel veri işleme faaliyetleri için kullanılan, önleyici ve hesap verebilirliğe dayalı bir veri koruma aracıdır. Avrupa Birliği'nin GDPR (Genel Veri Koruma Tüzüğü) kapsamında zorunlu hale getirilmiştir (Madde 35). Ayr. bkz. https://gdpr.eu/data-protection-impact-assessment-template/

Barker, J. M. (2016). *Data governance: The missing approach to improving data quality* [Doktora tezi]. ProQuest Dissertations ve Theses Global. https://www.proquest.com/dissertations-theses/data-governance-missing-approach-improving/docview/1862110139/se-2

Bhansali, N. (2014). The role of data governance in an organization. N. Bhansali (Edt.), *Data governance: Creating value from information assets* içinde (ss. 1–19). Taylor & Francis.

Brous, P., Janssen, M. ve Vilminko-Heikkinen, R. (2016). Coordinating decision-making in data management activities: A systematic review of data governance principles. H. J. Scholl, O. Glassey, M. Janssen, B. Klievink, I. Lindgren, P. Parycek, E. Tambouris, M. A. Wimmer, T. Janowski ve D. Sá Soares (Edt.), *Electronic Government* içinde (ss. 115-125). Springer International Publishing. https://doi.org/10.1007/978-3-319-44421-5_9

Contreras, I. A., Leal, A. C. ve Vergara, A. F. (2024). Proposal for a data governance framework in higher education. *43rd International Conference of the Chilean Computer Science Society (SCCC)*, 1-9. https://doi.org/10.1109/SCCC63879.2024.10767672

DAMA International. (2009). *DAMA-DMBOK: Data management body of knowledge*. Technics Publications

Fisher, T. (2009). *The data asset: How smart companies govern their data for business success*. John Wiley & Sons.

Hora, M. T., Bouwma-Gearhart, J. ve Park, H. J. (2017). Data driven decision-making in the era of accountability: Fostering faculty data cultures for learning. *The Review of Higher Education, 40*(3), 391–426. https://doi.org/10.1353/rhe.2017.0013

Jackson, P. ve Carruthers, C. (2019). *Data driven business transformation: How to disrupt, innovate and stay ahead of the competition*. Wiley.

Khatri, V. ve Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

Ladley, J. (2020). *Data governance: How to design, deploy, and sustain an effective data governance program*. Elsevier.

Leghemo, I. M., Segun-Falade, O. D., Odionu, C. S. ve Azubuike, C. (2025). A collaborative model for data governance: Enhancing integration across multi-line businesses. *Gulf Journal of Advance Business Research, 3*(1), 47-63. https://doi.org/10.51594/gjabr.v3i1.66

Legner, C., Fadler, M. ve Pentek, T. (2023). Data governance methodologies: The CC CDQ reference model for data and analytics governance. I. Caballero ve M. Piattini (Edt.), *Data Governance* içinde (ss. 99-119). Springer. https://doi.org/10.1007/978-3-031-43773-1_5

Nielsen, O. B. (2017). A comprehensive review of data governance literature. *Selected Papers of the IRIS, 8*(3), 120–133. https://aisel.aisnet.org/iris2017/3

Omar, A. ve Almaghthawi, A. (2020). Towards an integrated model of data governance and integration for the implementation of digital transformation processes in the Saudi universities. *International Journal of Advanced Computer Science and Applications, 11*(8), 588–593. https://doi.org/10.14569/IJACSA.2020.0110873

Otto, B. (2011). A morphology of the organisation of data governance. *ECIS 2011 Proceedings*, 272. https://aisel.aisnet.org/ecis2011/272

Otto, B. ve Reichert, A. (2010). Organizing master data management: Findings from an expert survey. *Proceedings of the 25th ACM Symposium on Applied Computing* içinde (ss. 106–110). Sierre, Switzerland.

Panian, Z. (2010). Some practical experiences in data governance. *World Academy of Science, Engineering and Technology, 38*, 150–157.

Picciano, A. G. (2012). The evolution of big data and learning analytics in American higher education. *Journal of Asynchronous Learning Networks, 16*(3), 9–20.

Plotkin, D. (2013). *Data stewardship: An actionable guide to effective data management and data governance*. Newnes.

Putro, B. L., Surendro, K. ve Herbert. (2016). Leadership and culture of data governance for the achievement of higher education goals (Case study: Indonesia University of Education). *Proceedings of International Seminar on Mathematics, Science and Computer Science Education (MSCEIS 2015)* içinde (ss. 1–12). Melville, NY: American Institute of Physics (AIP) Publishing.

Smallwood, R. F. (2014). *Information governance: Concept strategies and best practices*. John Wiley & Sons.

Weber, K., Otto, B. ve Oesterle, H. (2009). One size does not fit all---a contingency approach to data governance. *ACM Journal of Data and Information Quality, 1*(1), 4:1-4:27. https://ssrn.com/abstract=1728505

Wende, K. (2007). A model for data governance: Organising accountabilities for data quality management. *Proceedings of the 18th Australasian Conference on Information Systems* içinde (ss. 417-425). Toowoomba, Avustralya.

Wende, K. ve Otto, B. (2007). A contingency approach to data governance. M.A. Robert, R. O'Hare, M.L.Markus, ve B. Klein (Edt.) *Proceedings of 12th International Conference on Information Quality* içinde (ss. 163-176). Cambridge, USA. https://www.alexandria.unisg.ch/handle/20.500.14171/79975