



Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Anabilim Dalı

ÜNİVERSİTELERDE KURUMSAL VERİ YÖNETİŞİMİ MODELİNİN GELİŞTİRİLMESİ

Burcu TIĞ DEMİR

Doktora Tezi

Ankara, 2026

ÜNİVERSİTELERDE KURUMSAL VERİ YÖNETİŞİMİ MODELİNİN GELİŞTİRİLMESİ

Burcu TİĞ DEMİR

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Anabilim Dalı

Doktora Tezi

Ankara, 2026

KABUL VE ONAY

Burcu TIĞ DEMİR tarafından hazırlanan “Üniversitelerde Kurumsal Veri Yönetiřimi Modelinin Geliřtirilmesi” bařlıklı bu alıřma, 02/07/2026 tarihinde yapılan savunma sınavı sonucunda bařarılı bulunarak jürimiz tarafından bařarılı olarak kabul edilmiřtir.

Prof. Dr. Uğur ÖMÜRGÖNÜLŐEN (Bařkan)

Prof. Dr. Arif ALTUN (Üye)

Prof. Dr. Cořkun Polat (Üye)

Dr. Öğr. Üyesi Zafer KADIRHAN (Üye)

Prof. Dr. Özgür KÜLCÜ (Danıřman)

Yukarıdaki imzaların adı geen öğretim üyelerine ait olduėunu onaylım.

Prof. Dr. Uğur ÖMÜRGÖNÜLŐEN

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan “**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge**” kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. ⁽¹⁾
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ... ay ertelenmiştir. ⁽²⁾
- Tezimle ilgili gizlilik kararı verilmiştir. ⁽³⁾

28/08/2026

Burcu TIĞ DEMİR

¹ “Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge”

- (1) Madde 6. 1. Lisansüstü teze ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.
- (2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.
- (3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir

* Tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu tarafından karar verilir.

ETİK BEYAN

Bu alıřmadaki bütn bilgi ve belgeleri akademik kurallar erevesinde elde ettiđimi, grsel, iřitsel ve yazılı tm bilgi ve sonuları bilimsel ahlak kurallarına uygun olarak sunduđumu, kullandıđım verilerde herhangi bir tahrifat yapmadıđımı, yararlandıđım kaynaklara bilimsel normlara uygun olarak atıfta bulunduđumu, tezimin kaynak gsterilen durumlar dıřında zgn olduđunu, **Prof. Dr. zgr KLC** danıřmanlıđında tarafımdan retildiđini ve Hacettepe niversitesi Sosyal Bilimler Enstits Tez Yazım Ynergesine gre yazıldıđını beyan ederim.

Burcu TİĐ DEMİR

TEŞEKKÜR

Bazı yolculuklar çocukluğun sessiz bir odasında başlar.

Benim yolculuğum da öyle başladı. Babamın benim için yaptığı kara tahtanın önünde, karşıma dizdiğim boş sandalyelere ansiklopedilerden öğrendiğim bilgileri anlatırken... O günlerde dinleyicilerim yoktu. Ama bitmek bilmeyen bir merakım vardı. Şimdi geriye dönüp baktığımda görüyorum ki aslında o boş sandalyeler, yıllar sonra karşıma çıkacak bütün öğrencilerin, meslektaşların, dostların ve beni anlayacak insanların sessiz habercileriydi.

Sonra okul hayatı başladı.

Çocuk aklımla bilginin özgürce dolaştığı bir dünya hayal ederken, çoğu zaman tek bir doğru cevabın peşinden koşulan bir dünyanın içine girdim. Sonucu en başından belli matematik problemleri, satırların arasına sıkıştırılmış tek bir ana düşünce, ezberlenmesi beklenen bilgiler... Merakın bazen yavaşça sustuğunu, hayal kurmanın ise her zaman ödüllendirilmediğini öğrendim. Oysa ben, cevaplardan çok sorulara aşıktım.

Yine de merakın ilginç bir huyu vardı, susturulabilir ama asla yok edilemezdi.

Yıllar boyunca bu merak, beni bazen çıkmaz sokaklara, bazen de hiç hayal etmediğim kapılara götürdü. Yorulduğum, düştüğüm, vazgeçmeyi düşündüğüm zamanlar oldu. Ama her seferinde yeniden ayağa kalkmamı sağlayan şey, çocukluğumda o kara tahtanın başında hissettiğim öğrenme heyecanıydı. Bugün elimde tuttuğum bu tez, yalnızca akademik bir çalışmanın ürünü değil, çocukluğumdan bugüne uzanan merakın, emeğin, sabrın ve umudun somut bir karşılığıdır.

Bir zamanlar boş sandalyelere anlattığım hikayelerin, sorduğum soruların ve kurduğum hayallerin ulaştığı ilk durak belki de burasıdır. Ancak bu yolculuk hiçbir zaman tek başıma yürüdüğüm bir yol olmadı. Merakıma yön veren, bana inanan, bilgi ve deneyimleriyle yolumu aydınlatan, en zor anlarımda yanımda duran pek çok insan bu yolculuğun ayrılmaz bir parçası oldu.

Bu nedenle, bu tez çalışmasının hazırlanması ve tamamlanması sürecinde emeği geçen, bilgi ve deneyimleriyle bana yol gösteren, destek veren ve sabırla yanımda olan herkese içtenlikle teşekkür ederim.

Öncelikle, tez danışmanım Sayın Prof. Dr. Özgür KÜLCÜ'ye akademik rehberliği, bilimsel yaklaşımı, değerli katkıları ve bana duyduğu güven için en içten teşekkürlerimi sunarım. Araştırmanın her aşamasında sağladığı yönlendirme, önerileri ve teşvik edici desteği bu çalışmanın şekillenmesinde büyük rol oynamıştır.

Tez izleme komitemde yer alan değerli hocalarım Sayın Prof. Dr. Uğur ÖMÜRGÖNÜLŞEN ve Sayın Prof. Dr. Arif ALTUN'a çalışmaya yönelik yapıcı değerlendirmeleri ve akademik katkıları için teşekkür ederim. Görüş ve önerileri araştırmanın geliştirilmesine önemli katkılar sağlamıştır.

Tez jüri üyelerim Sayın Prof. Dr. Coşkun POLAT ve Sayın Dr. Öğr. Üyesi Zafer KADIRHAN'a, tezime kazandırdıkları farklı bakış açıları, yapıcı değerlendirmeleri ve değerli katkıları için içten teşekkürlerimi sunarım. Görüş ve önerileri, bu çalışmanın daha da gelişmesine önemli katkılar sağlamıştır.

Araştırma sürecinde görüşme taleplerimi kabul eden, bilgi ve deneyimlerini paylaşan üniversite temsilcilerine ve veri yönetişimi alanında çalışan tüm katılımcılara katkılarından dolayı teşekkür ederim.

Doktora eğitimim boyunca bilgi ve deneyimlerinden yararlandığım Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğretim üyelerine ve akademik süreçte desteklerini hissettiğim tüm arkadaşlarıma teşekkür ederim.

Hayatım boyunca her koşulda yanımda olan, desteklerini ve sevgilerini daima hissettiğim eşim ve aileme ise ayrı bir teşekkür borçluyum. Varlıkları, sabırları ve güvenleri bu sürecin en büyük motivasyon kaynağı olmuştur.

Son olarak bana kimi zaman zorluklarla, kimi zaman umutla yol gösteren, her düşüşte yeniden ayağa kalkmayı, vazgeçmemeyi ve merak etmeye devam etmeyi öğreten hayat sana da teşekkür ederim.

Dilerim bu çalışma, veri yönetiřimi alanına mütevazı da olsa bir katkı sunmanın ötesinde, merakın, sorgulamanın ve bilimin insanı dönüřtüren gücüne olan inancın da küçük bir yansıması olur.

ÖZET

TIĞ DEMİR, Burcu. *Üniversitelerde Kurumsal Veri Yönetişimi Modelinin Geliştirilmesi*,
Doktora Tezi, Ankara, 2026.

Çalışmanın çıkış noktası, verinin stratejik bir kurumsal varlık olarak ele alınması gerektiği yaklaşımıdır. Bu kapsamda veri yönetişimi stratejik, yönetsel, teknik, kültürel ve yasal boyutlarıyla incelenmiştir. Bu araştırmanın temel amacı, Türkiye’deki üniversitelerde kurumsal veri yönetişiminin mevcut durumunu ortaya koymak, veri yönetişimi süreçlerinde karşılaşılan sorunları belirlemek ve yükseköğretim kurumları için uygulanabilir bir veri yönetişimi modeli geliştirmektir.

Araştırma, tematik analiz ve yarı yapılandırılmış görüşmelere dayalı nitel araştırma yöntemiyle yürütülmüştür. Çalışma kapsamında uluslararası üniversitelerin veri yönetişimi politika belgeleri tematik analiz yöntemiyle incelenmiştir. Türkiye’de veri yönetişimi birimine sahip üniversitelerin web siteleri, politika belgeleri ve kurumsal yapıları değerlendirilmiştir. Ayrıca veri yönetiminden sorumlu üniversite temsilcileriyle yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Elde edilen veriler MAXQDA yazılımından yararlanılarak tematik olarak analiz edilmiştir.

Araştırma bulguları, Türkiye’deki üniversitelerde veri yönetişimi süreçlerinin büyük ölçüde dağınık yapılar üzerinden yürütüldüğünü göstermektedir. Veri standartları, rol ve sorumluluk tanımları ile veri paylaşım mekanizmaları yeterince kurumsallaşmamıştır. Veri yönetişimi süreçlerinde teknik altyapı eksiklikleri, organizasyonel koordinasyon sorunları, veri kültürü eksikliği ve politika yetersizlikleri dikkat çeken temel sorun alanları arasında yer almaktadır. Buna karşılık uluslararası üniversitelerde veri yönetişimi süreçlerinin daha sistematik yapılar, açık politika belgeleri ve belirlenmiş yönetim mekanizmaları çerçevesinde yürütüldüğü görülmektedir.

Araştırma sonucunda, üniversiteler için stratejik, yönetim, süreç, teknik, kültür ve yasal/etik katmanlardan oluşan bir veri yönetişimi modeli önerilmiştir. Geliştirilen modelin, üniversitelerde veri temelli karar alma süreçlerinin güçlendirilmesine, veri kalitesinin artırılmasına ve sürdürülebilir kurumsal veri yönetişimi yapılarının oluşturulmasına katkı sağlayacağı düşünülmektedir.

Anahtar Sözcükler

Veri yönetişimi, veri yönetimi, yükseköğretim kurumları, üniversiteler, veri politikaları, kurumsal veri yönetişimi, veri yönetişimi modeli

ABSTRACT

TİĞ DEMİR, Burcu. *Development of Institutional Data Governance Model in Universities*, Ph.D. Dissertation, Ankara, 2026.

The point of departure for this study is the premise that data should be regarded as a strategic institutional asset. Within this framework, data governance is examined through its strategic, managerial, technical, cultural, and legal dimensions. The primary objective of the research is to investigate the current state of institutional data governance practices in Turkish universities, identify the challenges encountered in data governance processes, and develop an applicable data governance model for higher education institutions.

The study was designed using a qualitative research approach. As part of the research, data governance policy documents from international universities were examined through thematic analysis. In addition, the websites, policy documents, and organizational structures of Turkish universities with established data governance units were evaluated. Semi-structured interviews were also conducted with university representatives responsible for data governance. The collected data were analyzed using content analysis, supported by the MAXQDA software package.

The findings reveal that data governance processes in Turkish universities are largely carried out through fragmented organizational structures. Data standards, role and responsibility definitions, and data-sharing mechanisms have not yet been sufficiently institutionalized. Key challenges identified include deficiencies in technical infrastructure, organizational coordination issues, a lack of data culture, and inadequacies in policy frameworks. In contrast, international universities appear to manage data governance through more systematic structures, clearly defined policy documents, and established governance mechanisms.

Based on the findings, a data governance model consisting of strategic, governance, process, technical, cultural, and legal/ethical layers is proposed for higher education institutions. The model is expected to contribute to strengthening data-driven decision-making processes, improving data quality, and establishing sustainable institutional data governance structures within universities.

Keywords

Data governance, data management, higher education institutions, universities, data policies, institutional data governance, data governance model

İÇİNDEKİLER

KABUL VE ONAY	i
YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI.....	ii
ETİK BEYAN.....	iii
TEŞEKKÜR	iv
ÖZET.....	vii
ABSTRACT	viii
İÇİNDEKİLER.....	ix
KISALTMALAR DİZİNİ	xiv
TABLolar DİZİNİ	xvii
ŞEKİLLER DİZİNİ	xviii
GRAFİKLER DİZİNİ	xix
1. BÖLÜM: GİRİŞ.....	1
1.1. KONUNUN ÖNEMİ.....	1
1.2. AMAÇ, PROBLEM VE ARAŞTIRMA SORULARI	2
1.3. ARAŞTIRMANIN YAPILANDIRILMASI	4
1.4. ARAŞTIRMANIN SINIRLILIKLARI.....	5
1.5. ARAŞTIRMANIN YÖNTEMİ, VERİ TOPLAMA VE DEĞERLENDİRME TEKNİKLERİ	9
1.5.1. Araştırma Yaklaşımı ve Veri Toplama Süreci	9
1.5.2. Verilerin Analizi.....	11
1.5.3. Geçerlik ve Güvenirlik	14
1.6. ARAŞTIRMANIN DÜZENİ.....	15
2. BÖLÜM: VERİ YÖNETİŞİMİ KAVRAMSAL ÇERÇEVE.....	17
2.1. KURUMSAL VARLIK OLARAK VERİLER	17
2.2. VERİ YÖNETİŞİMİ	18

2.2.1. Stratejik Boyut.....	21
2.2.2. Örgütsel (Yönetmel) Boyut	22
2.2.3. Teknik Boyut.....	23
2.2.4. Kültürel ve Davranışsal Boyut	26
2.2.5. Yasal ve Etik Boyut.....	27
2.3. VERİ YÖNETİŞİMİ İLE İLGİLİ ÇALIŞMALAR	29
2.4. VERİ YÖNETİŞİMİ MODELLERİ.....	32
2.4.1. Merkezi Veri Yönetişimi Modeli	34
2.4.2. Dağınık (Merkezi Olmayan) Veri Yönetişimi Modeli	35
2.4.3. Federatif (Hibrit) Veri Yönetişimi Modeli	36
2.4.4. Veri Yönetişimi Olgunluk Modelleri	37
3. BÖLÜM: VERİ YÖNETİŞİMİ STANDARTLARI, ÇERÇEVELERİ, YASAL DÜZENLEMELERİ VE POLİTİKALARI.....	41
3.1. ULUSLARARASI STANDARTLAR	42
3.1.1. ISO/IEC 38505 Serisi: Veri Yönetişimi Standartları	42
3.1.2. ISO/IEC 25642:2025 Veri İş Birliği Çerçevesi.....	46
3.1.3. ISO/IEC 11179 Serisi: Üst Veri Kayıtları Standardı.....	48
3.1.4. ISO/IEC 27001 ve 27701 Standartları: Bilgi Güvenliği ve Gizlilik Bilgi Yönetim Sistemi.....	50
3.1.5. ISO/IEC ISO 8000-51:2023 Veri Kalitesi: Bölüm 51: Veri Yönetişimi: Veri Politikası Bildirimlerinin Paylaşımı	53
3.1.6. ISO/IEC 5259-5:2025 Veri Kalitesi Yönetişim Çerçevesi.....	55
3.2. ULUSLARARASI KURUM TEMELLİ ÇERÇEVELER.....	57
3.2.1. DAMA-DMBOK2 Çerçevesi.....	57
3.2.2. Veri Yönetişimi Enstitüsü Çerçevesi	68
3.2.3. OECD Veri Yönetişimi Çerçevesi	70
3.2.4. UNDP Dijital Strateji 2022–2025	72

3.2.5. Dünya Bankası Veri Yönetişimi Tanı Aracı	74
3.2.6. DCAM Çerçevesi	76
3.2.7. PwC Kurumsal Veri Yönetişimi Çerçevesi.....	78
3.3. ÜLKELERİN VERİ YÖNETİŞİMİ ÇERÇEVELERİ	79
3.3.1. ABD Yaklaşımı	81
3.3.2. AB Yaklaşımı.....	87
3.3.3. Avustralya	89
3.3.4. Birleşik Krallık.....	93
3.3.5. Türkiye	95
3.4. YÜKSEKÖĞRETİM KURUMLARININ ÇERÇEVELERİ.....	98
4. BÖLÜM: BULGULAR VE DEĞERLENDİRME	103
4.1. ULUSLARARASI ÜNİVERSİTELERİN MEVCUT DURUMLARI	104
4.1.1. Veri Yönetişimi Birimleri ve Personeli.....	107
4.1.2. Veri Standartları	112
4.1.3. Veri Erişimi ve Paylaşımı	116
4.1.4. Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	119
4.1.5. Veri Kültürü	122
4.2. ULUSAL ÜNİVERSİTELERİN MEVCUT DURUMLARI.....	124
4.2.1. Veri Yönetişimi Birimleri ve Personeli.....	125
4.2.2. Veri Standartları	134
4.2.3. Veri Erişimi ve Paylaşımı	138
4.2.4. Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	141
4.2.5. Veri Kültürü	143
5. BÖLÜM: ÜNİVERSİTELERE YÖNELİK VERİ YÖNETİŞİMİ MODEL ÖNERİSİ.....	146
5.1. ÜNİVERSİTELER İÇİN VERİ YÖNETİŞİMİ MODELİ.....	146
5.2. MODELİN KATMANLARI.....	152

5.2.1. Stratejik Katman.....	152
5.2.2. Yönetişim Katmanı	156
5.2.3. Süreç Katmanı.....	160
5.2.4. Teknik Katman.....	164
5.2.5. Kültür Katmanı.....	169
5.2.6. Yasal ve Etik Katman.....	173
5.3. MODELİN UYGULANMASINA YÖNELİK EYLEM PLANI	176
5.3.1. Eylem Planının Amacı ve Kapsamı.....	176
5.3.2. Aşamalı Veri Yönetişimi Eylem Planı	177
5.3.2.1. Aşama 1: Kurumsal Hazırlık ve Üst Yönetim Sahipliği.....	177
5.3.2.2. Aşama 2: Mevcut Durum Analizi ve Veri Envanteri.....	179
5.3.2.3. Aşama 3: Politika, Organizasyon ve Standartların Oluşturulması.....	181
5.3.2.4. Aşama 4: Pilot Uygulama ve Hızlı Kazanımlar.....	183
5.3.2.5. Aşama 5: Değerlendirme ve Kurum Geneline Yaygınlaştırma.....	185
5.3.2.6. Aşama 6: Kurumsallaştırma, Ölçme ve Sürekli İyileştirme.....	186
5.4. TARTIŞMA.....	188
6. BÖLÜM: SONUÇ VE ÖNERİLER	194
6.1. SONUÇ	194
6.2. ÖNERİLER.....	200
KAYNAKÇA	203
EK1. ORJİNALLİK FORMU	215
EK 2. ETİK KURUL İZNİ.....	217
EK 3. ÜNİVERSİTELERDE KURUMSAL VERİ YÖNETİMİ POLİTİKALARININ GELİŞTİRİLMESİ GÖNÜLLÜ KATILIM FORMU VE GÖRÜŞME SORULARI.....	218

EK 4. VERİ YÖNETİŞİMİ DÜZENLEMESİ OLAN ULUSAL ÜNİVERSİTELER	224
EK 5. ULUSLARARASI ÜNİVERSİTELERİN VERİ YÖNETİŞİMİ POLİTİKALARINA DAİR BİLGİLER.....	225
EK 6. ULUSLARARASI VE ULUSAL ÜNİVERSİTELERİN TEMATİK KODLAMALARI	229
EK 7. GÖRÜŞME BULGULARI İLE MODEL BİLEŞENLERİNİN KARŞILIKLARI.....	230
EK 8. ULUSLARARASI VERİ YÖNETİŞİMİ POLİTİKALARI VERİLERİNİN MODEL BİLEŞENLERİ KARŞILIĞI.....	235

KISALTMALAR DİZİNİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
BAP	Bilimsel Araştırma Projeleri
BK	Birleşik Krallık
BT	Bilgi Teknolojileri
CDO	Chief Data Officer
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
COPPA	Children's Online Privacy Protection Act
DAMA	Data Management Association
DAMA-DMBOK	Data Management Body of Knowledge
DAMA-DMBOK2	Data Management Body of Knowledge 2
DCAM	Data Management Capability Assessment Model
DGA	Data Governance Act
DGI	Data Governance Institute
DGO	Data Governance Office
DMBOK	Data Management Body of Knowledge
DOL	Department of Labor
DTO	Dijital Dönüşüm Ofisi
EDM	Evaluate Direct Monitor
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
FERPA	Family Educational Rights and Privacy Act
FIPP	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act (Bilgi Edinme Özgürlüğü Yasası)
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act

HIPAA	Health Insurance Portability and Accountability Act
IBM	International Business Machines
ID	Identifier
IFLA	International Federation of Library Associations
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KHK	Kanun Hükmünde Kararname
KVKK	Kişisel Verilerin Korunması Kanunu
MAXQDA	Max Qualitative Data Analysis
MDR	Metadata Registry
OECD	Organisation for Economic Co-operation and Development
PDF	Portable Document Format
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMS	Privacy Information Management System
PwC	PricewaterhouseCoopers
QS	Quacquarelli Symonds
RACI	Responsible, Accountable, Consulted, Informed
SAS	Statistical Analysis System
THE	Times Higher Education
TUCBS	Türkiye Ulusal Coğrafi Bilgi Sistemi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜİK	Türkiye İstatistik Kurumu
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICC	United Nations International Computing Centre
URAP	University Ranking by Academic Performance

VPN	Virtual Private Network
YÖK	Yükseköğretim Kurulu
YÖKAK	Yükseköğretim Kalite Kurulu
YÖKSİS	Yükseköğretim Bilgi Sistemi

TABLÖLAR DİZİNİ

Tablo 1. Veri yönetiřimi birimi olan kurumlar	8
Tablo 2. Görüşme yapılan yükseköğretim kurumları	11
Tablo 3. Veri yönetiřimi modellerinin karşılaştırılması (Lifebit, 2025).	34
Tablo 4. Veri yönetiřimi birimlerinin yapılanması	108
Tablo 5. Veri standardı uygulamaları	113
Tablo 6. Veri erişimi ve paylaşımı uygulamaları.....	117
Tablo 7. Veri kültürü uygulamaları.....	123

ŞEKİLLER DİZİNİ

Şekil 1. Araştırmanın yapılandırılması.	4
Şekil 2. MaxQDA kodlama örneği	13
Şekil 3. Veri yönetişimi ve veri yönetimi (World Bank, 2021).	19
Şekil 4. Veri yönetişimi modelleri (Alation, 2025).....	33
Şekil 5. DAMA veri yönetimi olgunluk modeli (DAMA, 2017, s. 514)	38
Şekil 6. DAMA-DMBOK2 veri yönetimi çerçevesi (DAMA Çarkı) (DAMA, 2017, s. 36).....	58
Şekil 7. DAMA çevresel faktörler altıgeni (DAMA, 2017, s. 36).	59
Şekil 8. Bilgi alanı bağlam şeması (DAMA, 2017, s. 37).....	61
Şekil 9. DMBOK piramidi (Aiken) (DAMA, 2017, s. 40).	63
Şekil 10. DAMA fonksiyonel alan bağımlılıkları (DAMA, 2017, s. 41).....	64
Şekil 11. DAMA veri yönetimi fonksiyon çerçevesi (DAMA, 2017, s. 42).....	66
Şekil 12. Gelişmiş DAMA çarkı (DAMA, 2017, s. 44).....	68
Şekil 13. Veri yönetişimi enstitüsü çerçevesi (DGI, t.y.).....	70
Şekil 14. Kamu sektöründe veri yönetişimi (OECD, 2019, s. 164).....	71
Şekil 15. UNDP veri stratejisi yönetişimi (UNICC, 2021).....	73
Şekil 16. Veri yönetişimi tanı aracı (World Bank, 2020, s. 10).....	75
Şekil 17. DCAM v3 çerçevesi (EDM Association, 2025)	77
Şekil 18. PwC veri yönetişimi çerçevesi.....	79
Şekil 19. DOL veri stratejisi (U.S. Departman of Labor, t.y).	84
Şekil 20. Veri yönetişimi birim personelinin yapılanması.....	110
Şekil 21. Üniversiteler için katmanlı veri yönetişimi modeli	149
Şekil 22. Stratejik katman iş akışı.....	153
Şekil 23. Yönetişim katmanı iş akışı.....	157
Şekil 24. Süreç katman iş akışı	161
Şekil 25. Teknik katman iş akışı	165
Şekil 26. Kültür katman iş akışı.....	170
Şekil 27. Yasal ve etik katman iş akışı.....	173

GRAFİKLER DİZİNİ

Grafik 1. Veri yönetiřimi politikalarının lkelere gre daėılımları	6
Grafik 2. Veri yönetiřimi politikalarının lkelere gre daėılımı	104
Grafik 3. Veri yönetiřimi politikalarının yıllara gre daėılımı	105
Grafik 4. Veri yönetiřimi politikalarının başlıklara gre daėılımı.....	106
Grafik 5. Veri yönetiřimi birimlerinin yapılanma tr	126
Grafik 6. Veri yönetiřimi birim adında geen kelime daėılımı	127
Grafik 7. Veri yönetiřimi birimlerinin kuruluř yılları daėılımı	128
Grafik 8. Veri yönetiřimi birimi yönetici ve personel daėılımı	129
Grafik 9. Veri yönetiřimi birimlerinin idari dzenlemeleri	132

1. BÖLÜM

GİRİŞ

1.1. KONUNUN ÖNEMİ

Üniversiteler eğitim, araştırma, toplumsal katkı ve yönetim süreçleri kapsamında yoğun veri üreten kurumlardır. Öğrenci verileri, araştırma verileri, akademik veriler, yönetim verileri ve dijital öğrenme verileri gibi çok sayıda veri kaynağı, verinin stratejik bir kurumsal varlık olarak ele alınmasını gerekli kılmaktadır (Fisher, 2009). Verinin hacmi, çeşitliliği ve üretim hızı arttıkça veri yönetimi süreçleri de daha karmaşık hale gelmektedir (British Academy ve Royal Society, 2017).

Üniversitelerde birimlerin veriyi çoğu zaman bağımsız biçimde yönetmesi standart eksiklikleri, veri sahipliği belirsizlikleri ve koordinasyon sorunları gibi önemli yönetim problemlerine yol açmaktadır. Veri yönetiminden kimlerin sorumlu olacağına dair (veri sahibi, veri sorumlusu, veri yöneticisi, veri yönetimi kurulu vb.) açık tanımlamaların bulunmaması, uygulamada yönetim boşlukları oluşturmaktadır (Dismute, 2009). Ayrıca veri paylaşımı, veri sahipliği ve fikrî mülkiyet haklarına ilişkin düzenlemelerin yetersizliği kurumsal belirsizlikleri artırmaktadır (World Economic Forum, 2021). Bu durum, verinin karar alma süreçlerinde etkin kullanımını sınırlandırmaktadır (Brous vd., 2016b).

Buna karşın, verinin sistematik biçimde yönetim süreçlerine entegre edilmesi kurumsal performansını artırmaktadır. Araştırmalar, veriye dayalı karar alma yaklaşımını benimseyen kurumların performans ve verimlilik açısından önemli kazanımlar elde ettiğini göstermektedir (Bak, 2023; NewVantage Partners, 2022). Ancak birçok üniversite halen veriyi üreten kurum konumunda kalmakta, veriyi yönetsel ve stratejik bir kaynak olarak yeterince değerlendirememektedir (Fisher, 2009).

Literatürde, verinin değer üretebilmesi için kurumsal bir varlık olarak yönetilmesi gerektiği vurgulanmaktadır (Aisyah ve Ruldeviyani, 2018; Bhansali, 2014). Bu noktada veri yönetimi politika, standart, rol, sorumluluk ve karar mekanizmalarını düzenleyen stratejik bir çerçeve sunmaktadır. Veri kullanımını, paylaşımını ve korunmasını

düzenleyen sürdürülebilir politikaların geliştirilmesi, üniversitelerde veri odaklı yönetim anlayışının temelini oluşturmaktadır (Chen, 2021).

1.2. AMAÇ, PROBLEM VE ARAŞTIRMA SORULARI

Bu araştırmanın temel amacı, Türkiye’deki üniversitelerin kurumsal veri yönetişimi konusundaki mevcut durumlarını ortaya koymak, bu süreçte karşılaştıkları sorunları ve engelleri belirlemek, söz konusu problemlerin çözümüne yönelik öneriler geliştirmek ve üniversitelerde uygulanabilir bir veri yönetişimi modeli tasarlamaktır.

Çalışma, yükseköğretim kurumlarının veriyi bir kurumsal varlık olarak ele alabilmesi, veri yönetimi süreçlerini kurumsal stratejiyle ilişkilendirebilmesi ve sürdürülebilir bir veri yönetişimi yapısı oluşturabilmesi açısından yol gösterici olmayı da amaçlamaktadır.

Bilgi çağının en belirleyici unsurlarından biri olan veri, günümüzde kurumların stratejik karar alma süreçlerinin merkezinde yer almaktadır. Kurumlarda üretilen ve toplanan verinin hacmi hızla artarken, bu verinin nasıl yönetileceği, kimler tarafından kullanılacağı ve hangi ilkelere göre paylaşılacağı soruları giderek daha karmaşık bir hal almaktadır. Üniversiteler eğitim, araştırma ve idari faaliyetler sonucunda çok büyük miktarda veri üretmektedir. Bu verinin kurumsal düzeyde yönetimi ve yönetişimi çoğu zaman sistematik bir çerçeveye oturtulamamaktadır.

Bu durum, üniversitelerde veri yönetişiminin stratejik bir alan olarak kurumsallaşmamasına neden olmaktadır. Sonuç olarak, veri yönetişiminde karşılaşılan organizasyonel, süreçsel ve teknik sorunlar, kurumların veriye dayalı karar alma yetkinliğini zayıflatmakta ve ulusal düzeyde yükseköğretim sisteminin dijital dönüşüm kapasitesini sınırlandırmaktadır.

Bu araştırmanın temel problemi, Türkiye’deki üniversitelerde veri yönetişimi süreçlerinin bir çerçevede yapılandırılmaması, kurumsal rollerin, standartların ve politikaların belirlenememesi nedeniyle veri yönetişimi olgunluk düzeyinin düşük kalması ve sürdürülebilir bir veri yönetişimi modelinin henüz oluşturulamamış olmasıdır.

Araştırmanın temel problemine bağlı olarak aşağıdaki araştırma soruları oluşturulmuştur. Bu sorular, üniversitelerde veri yönetişimi süreçlerinin mevcut durumunu analiz etmeyi,

kurumların karşılaştıkları temel sorunları tanımlamayı ve çözüm yolları geliştirmeyi hedeflemektedir.

Organizasyonel Yapı

1. Üniversitelerde veri yönetiřimi süreçleri nasıl yapılandırılmıştır?
2. Veri yönetiřiminden kimler sorumludur ve bu sorumluluklar hangi kurumsal yapılar üzerinden yürütölmektedir?

Kurumsal Kültür ve Farkındalık

3. Üniversitelerde veri yönetiřimi kültürü hangi faktörlerden etkilenmektedir?
4. Veri yönetiřimi farkındalıęı, kurumların karar alma ve yönetsel süreçlerine nasıl yansımaktadır?

Süreç ve Teknik Boyut

5. Üniversitelerde veri toplama, saklama, erişim, paylaşım ve imha süreçleri nasıl yürütölmektedir?
6. Veri standardizasyonu, kalite güvencesi ve bütönlük sağlama konularında hangi zorluklar yaşanmaktadır?
7. Üniversitelerdeki bilgi sistemleri arasında veri entegrasyonu ne düzeydedir?

Politika, Standartlar ve Yönetişim

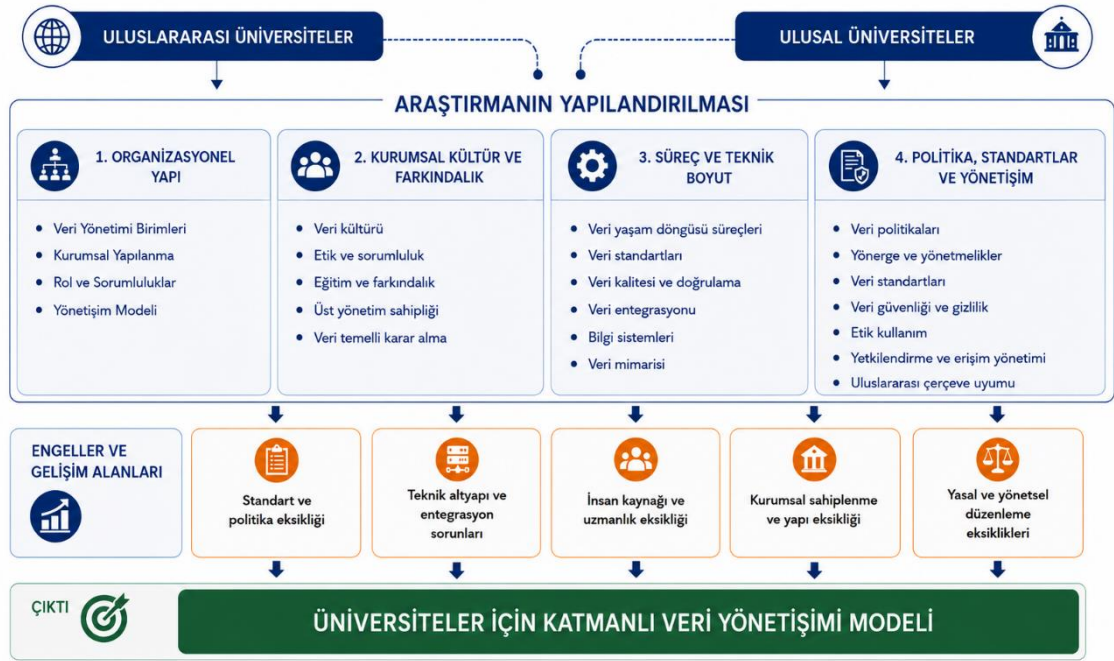
8. Üniversitelerde veri yönetiřimine ilişkin tanımlı politika, standart veya yönergeler mevcut mudur?
9. Mevcut politikalar, uluslararası veri yönetiřimi çerçeveleri (örneğin DGI, DAMA-DMBOK) ile hangi açılardan benzerlik ya da farklılık göstermektedir?
10. Üniversitelerde veri güvenlięi, gizlilik, etik kullanım ve paylaşım konularında hangi uygulamalar yürütölmektedir?

Engeller, Gereksinimler ve Çözüm Önerileri

11. Üniversitelerde etkili bir veri yönetiřimi sisteminin oluřturulmasının önündeki bařlıca engeller nelerdir?
12. Veri yönetiřimi süreçlerinin geliřtirilmesi için kurumların hangi alanlarda kapasite geliřtirmeye ihtiya duyduėu düşünölmektedir?
13. Türkiye'deki üniversiteler için nasıl bir veri yönetiřimi modeli geliřtirilebilir?

1.3. ARAřTIRMANIN YAPILANDIRILMASI

Arařtırmanın yapılandırılması önceki bölümde sunulan amalar ve arařtırma problemleri kapsamında řekil 1'deki gibi geliřtirilmiřtir.



řekil 1. Arařtırmanın yapılandırılması

Arařtırma, Türkiye'deki üniversitelerde veri yönetiřimi süreçlerinin mevcut durumunu deėerlendirebilmek amacıyla uluslararası üniversiteler ile ulusal üniversitelerin veri yönetiřimi yaklařımlarını karřılařtırmalı inceleyen bir yapı üzerine kurulmuřtur. Karřılařtırmalı analiz kapsamında uluslararası üniversitelerin veri yönetiřimi yaklařımları ve politika belgeleri incelenmiřtir. Ulusal üniversitelerdeki veri yönetiřimi birimlerinin temsilcileriyle yarı yapılandırılmıř görüřmeler gerekleřtirilmiřtir. Yine

ulusal üniversitelerin veri yönetişimi birimlerinin web sayfalarından teşkilatlanma şekilleri, yönerge, yönetmelik, politika belgeleri incelemiştir.

Şekil 1’de görüleceği gibi araştırma dört yapıda ele alınmıştır. Organizasyonel yapı, veri yönetişiminin kurumsal düzeyde ne ölçüde yapılandırıldığını ve yönetsel sahipliğin nasıl organize edildiğini değerlendirmeyi amaçlamaktadır. Kurumsal kültür ve farkındalık, üniversitelerde veri yönetişiminin kurumsal kültürle ilişkili bir dönüşüm alanı olduğunu vurgulamaktadır. Süreç ve teknik, üniversitelerin teknik altyapıları, sistemler arası entegrasyon düzeyleri ve veri yönetişimi süreçlerinin işleyişi değerlendirilmektedir. Politika, standartlar ve yönetim ise üniversitelerde veri yönetişiminin kurumsal politika ve düzenlemeler çerçevesinde nasıl yapılandırıldığını incelemektedir.

Araştırmanın literatür taraması yapılırken veri yönetişimi süreçlerini sınırlayan temel engel ve gelişim alanları da belirlenmiştir. Bunlar standart ve politika eksikliği, teknik altyapı ve entegrasyon sorunları, insan kaynağı ve uzmanlık eksikliği, kurumsal sahiplenme yetersizliği ile yasal ve yönetsel düzenleme eksiklikleri olarak sınıflandırılmıştır. Bu alanlar, üniversitelerde veri yönetişimi olgunluğunu etkileyen temel yapısal sorunları temsil etmektedir.

Şeklin en alt bölümünde ise araştırmanın nihai çıktısı olarak geliştirilecek olan Üniversiteler İçin Katmanlı Veri Yönetişimi Modeli yer almaktadır. Modelin, araştırma kapsamında elde edilen bulgular doğrultusunda stratejik, organizasyonel, teknik, kültürel ve yönetsel katmanları ele alan sürdürülebilir bir veri yönetişimi yapısı sunması amaçlanmaktadır.

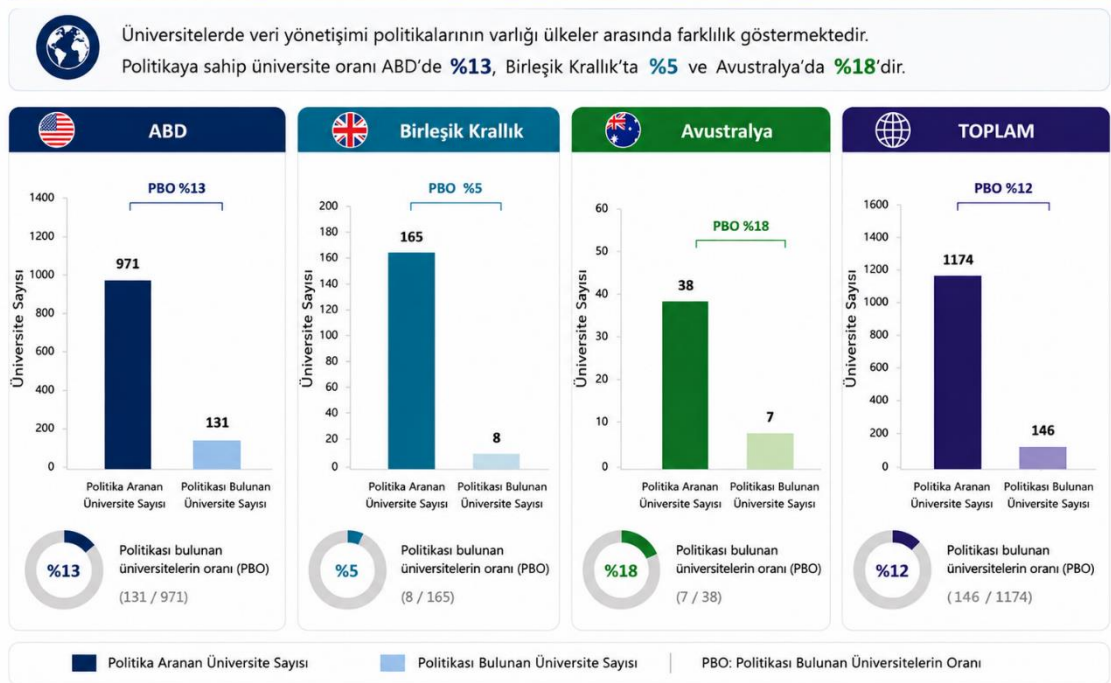
1.4. ARAŞTIRMANIN SINIRLILIKLARI

Araştırmanın literatür değerlendirmesi veri yönetişimi alanında ulusal ve uluslararası ölçekte gerçekleştirilen çalışmalarla sınırlandırılmıştır. Bu doğrultuda veri yönetişiminin kavramsal gelişimi, kurumsal veri yönetişimi yaklaşımları, veri yönetişimi çerçeveleri, politika ve standartlar ile yükseköğretim kurumlarında veri yönetişimi uygulamalarına ilişkin akademik çalışmalar değerlendirilmiştir. Ayrıca küresel veri yönetişimi çerçeveleri, veri yönetişimi standartları, veri yönetişimi ile ilişkili yasal düzenlemeler, uluslararası üniversitelerin veri yönetişimi modelleri ve çalışma kapsamına alınan

ülkelerin veri yönetişimi yaklaşımları analiz edilerek alanın kuramsal ve uygulamalı gelişimine ilişkin temel eğilimler ortaya konulmuştur.

Veri yönetişiminin uluslararası yaklaşımı için, literatür taraması sonucu elde edilen kaynaklarda Amerika Birleşik Devletleri (ABD), Avrupa Birliği (AB), Avustralya ve Birleşik Krallık'ın (BK) çalışmaları veri yönetişimi kapasitesi yüksek ülkeler arasında yer almakta ve birçok uygulama örneği sunmaktadır. Bu doğrultuda araştırma kapsamına söz konusu ülkelerdeki üniversiteler kurumun türü (vakıf ya da devlet) fark etmeksizin dahil edilmiştir. Üniversitelerin belirlenmesinde 2024 yılı QS (World University Rankings) ve THE (Times Higher Education) esas alınmış, bu sıralamalarda yer alan toplam 1675 üniversitenin resmî web sayfaları incelenmiştir. İnceleme sonucunda ülkelerindeki üniversitelerde yayımlanan politika belgelerinin büyük ölçüde kurumsal veri yönetişiminden ziyade araştırma verilerinin yönetimine odaklandığı görülmüştür. Bu sebeple uluslararası yaklaşım ABD, Avustralya ve BK üniversiteleri üzerinden yürütülmüştür.

Veri Yönetişimi Politikalarının Ükelere Göre Dağılımları



Grafik 1. Veri yönetişimi politikalarının ülkelere göre dağılımları

AB üniversiteleri hariç tutulduktan sonra veri yönetiřimi politikaları 1174 üniversitenin web sayfasında aranmıřtır. Veri yönetiřimi birimi olan uluslararası üniversitelerin veri yönetiřimi yaklařımları ve varsa politika belgeleri PDF formatında indirilmiřtir. İndirilen veri yönetiřimi politika belgeleri tematik analiz yöntemiyle analiz edilmiřtir. Yapılan analiz sonucunda, bu üniversitelerin 146'sında (%12) açık biçimde tanımlanmıř veri yönetiřimi politikalarının bulunduđu belirlenmiřtir. Veri yönetiřimi politikası tespit edilen üniversitelerin büyük çoğunluğunun ABD'de bulunduđu görölmüřtür. Bu oran yaklařık %90'dır (n=131). Politika geliřtirme oranı bakımından ise en yüksek düzeyin %18 ile Avustralya'daki üniversitelerde olduđu saptanmıřtır (Bkz. Grafik 1). Türkiye'deki üniversitelerin mevcut durumunun uluslararası yaklařımlar çerçevesinde deđerlendirilmesine yönelik bir analiz zemini bu yolla hazırlanmıřtır.

Arařtırmanın ulusal yaklařımı için Türkiye'de 2024 yılındaki 208 üniversitenin web sayfalarında kurumun türü (vakıf ya da devlet) fark etmeksizin veri yönetiřimi alanında kurumsal bir yapılanma oluřturmuř olan 24 yükseköğretim kurumu ile sınırlandırılmıřtır (Bkz. Tablo 1). Arařtırma kapsamında ilgili üniversitelerin web siteleri, kurumsal organizasyon yapıları, resmî politika belgeleri, yönergeleri, yönetmelikleri ve veri yönetiřimine iliřkin dokümanları incelenmiřtir. Ayrıca veri yönetiřiminden sorumlu birim yöneticileri veya temsilcileriyle yarı yapılandırılmıř görüřmeler gerçekteřirilmıřtir. Bu kapsamda arařtırmada organizasyonel yapı, kurumsal kültür ve farkındalık, süreç ve teknik boyut ile politika, standartlar ve yönetiřim alanlarına iliřkin incelemeler yapılmıřtır. Üniversitelerin veri yönetiřimi birimleri, kurumsal yapılanmaları, politika belgeleri, teknik altyapıları ve yönetiřim uygulamaları deđerlendirilmiřtir.

Tablo 1. Veri yönetiřimi birimi olan kurumlar

N o	Üniversite Adı	Birim Adı
1	Yükseköğretim Kurulu	Veri Yönetimi İzleme ve Değerlendirme Daire Başkanlığı
2	Ankara Üniversitesi	Kurumsal Veri Yönetimi Koordinatörlüğü
3	Atatürk Üniversitesi	Büyük Veri Yönetim Ofisi
4	Bilkent Üniversitesi	Kurumsal Veri Analizi ve Kalite Yönetimi Birimi
5	Dokuz Eylül Üniversitesi	Kurumsal Veri Yönetim Koordinatörlüğü
6	Erciyes Üniversitesi	Kurumsal Veri Yönetimi ve Analitiğı Koordinatörlüğü
7	Fatih Sultan Mehmet Vakıf Üniversitesi	Veri Bilimi Uygulama ve Arařtırma Merkezi
8	Gazi Üniversitesi	Kurumsal Veri Yönetimi Koordinatörlüğü
9	Hacettepe Üniversitesi	Kurumsal Veri Yönetimi Koordinatörlüğü
10	Hitit Üniversitesi	Veri Analiz Ofisi
11	Isparta Uygulamalı Bilimler Üniversitesi	Veri Yönetimi Uygulama ve Arařtırma Merkezi
12	İstanbul Üniversitesi-Cerrahpařa	Kurumsal Veri Yönetim Ofisi
13	İzmir Kâtip Çelebi Üniversitesi	Yapay Zeka ve Veri Bilimi Uygulama ve Arařtırma Merkezi
14	Lokman Hekim Üniversitesi	Akademik Veri Yönetim Birimi
15	Necmettin Erbakan Üniversitesi	Büyük Veri Koordinatörlüğü
16	ODTÜ	Kurumsal Büyük Veri Yönetimi Koordinatörlüğü
17	Osmaniye Korkut Ata Üniversitesi	Veri Analizi Uygulama ve Arařtırma Merkezi
18	Pamukkale Üniversitesi	Kalite Yönetimi ve Veri Değerlendirme Uygulama ve Arařtırma Merkezi
19	Sabancı Üniversitesi	Veri Analitiğı Arařtırma ve Uygulama Merkezi
20	Sakarya Uygulamalı Bilimler Üniversitesi	Yapay Zeka ve Veri Bilimi Uygulama ve Arařtırma Merkezi
21	Sivas Cumhuriyet Üniversitesi	Yapay Zeka ve Veri Bilimi Arařtırma ve Uygulama Merkezi
22	Trabzon Üniversitesi	Büyük Veri ve Yapay Zeka Koordinatörlüğü
23	Üsküdar Üniversitesi	Veri Uygulama ve Arařtırma Merkezi
24	Zonguldak Bülent Ecevit Üniversitesi	Veri Merkezi Koordinatörlüğü

Tablo 1’de listelenen üniversiteler, Türkiye’de veri yönetiřimi alanında kurumsal yapı oluřtırmaya yönelik örnek uygulamalar sunmaktadır. Bu arařtırmanın sonuçları doğrudan Türkiye’deki tüm yükseköğretim kurumlarına genellenememektedir. Bunun temel nedeni, Türkiye’deki üniversitelerin kurumsal kapasite, dijital dönüşüm düzeyi, teknik altyapı, insan kaynağı ve yönetsel yapı bakımından farklılık göstermesidir. Dolayısıyla arařtırma bulguları, özellikle veri yönetiřimi konusunda belirli düzeyde kurumsal yapılanmaya sahip üniversiteler çerçevesinde değerlendirilmelidir.

Araştırma, veri yönetişimi süreçlerini ağırlıklı olarak kurumsal belgeler, politika metinleri ve yönetici görüşleri üzerinden incelemektedir. Bu nedenle akademik personel, idari personel ve öğrencilerin veri yönetişimine ilişkin bireysel deneyim ve algıları araştırma kapsamı dışında bırakılmıştır. Ayrıca araştırmada incelenen politika ve uygulamalar, üniversitelerin kamuya açık olarak paylaştıkları bilgiler ile görüşmeler sırasında elde edilen verilerle sınırlıdır.

1.5. ARAŞTIRMANIN YÖNTEMİ, VERİ TOPLAMA VE DEĞERLENDİRME TEKNİKLERİ

1.5.1. Araştırma Yaklaşımı ve Veri Toplama Süreci

Bu araştırma, yükseköğretim kurumlarında kurumsal veri yönetişimi yaklaşımlarının mevcut durumunu ortaya koymak ve Türkiye’deki üniversiteler için uygulanabilir bir veri yönetişimi modeli geliştirmek amacıyla gerçekleştirilmiştir. Araştırmanın doğası gereği, veri yönetişimi olgusunun kurumsal yapı, politika, süreç, kültür ve teknik altyapı boyutlarıyla incelenebilmesi için çalışma, nitel araştırma yaklaşımı temelinde tasarlanmıştır.

Nitel araştırmanın temel amaçlarından birinin toplumsal gerçekliği ayrıntılı biçimde betimlemektir (Kvale, 1996; Leavy, 2014). Nitel yöntem, belirli bir olguyu anlamlandırmak, katılımcıların deneyim ve algılarını derinlemesine incelemek için uygun bir yaklaşımdır (Hennink vd., 2020, s. 11). Nitel araştırmalarda ölçüm tekniği yerine bireylerin yaşadıkları dünyayı nasıl anlamlandırdıkları önemlidir (Kvale, 1996).

Kvale’a (1996) göre nitel araştırmalarda araştırma süreci katı hipotezlerle başlamaktan çok, araştırma konusu hakkında anlam üretmeye ve olguları derinlemesine anlamaya yönelmektedir. Bu sebeple araştırmada hipotez üretilmeden hem ulusal hem de uluslararası üniversitelerin veri yönetişimi yaklaşımları araştırma sorularıyla derinlemesine anlamlandırılmaya çalışılmıştır.

Araştırmanın kuramsal temelini oluşturmak ve veri toplama sürecini yapılandırmak amacıyla veri yönetişimi, veri yönetimi, veri kalitesi, veri politikaları, veri kültürü ve yükseköğretimde veri yönetişimi konularında kapsamlı bir literatür incelemesi gerçekleştirilmiştir. Araştırma alanı ile ilgili daha önceden neler yapılmış, hangi

yöntemler uygulanmış ve hangi sonuçlara ulaşılmış olduğunu ortaya koymaktır (Bryman, 2016, s. 6). Bu kapsamda Web of Science, Scopus, ScienceDirect, Emerald, SpringerLink, Google Scholar, ProQuest Dissertations and Theses ve TR Dizin veri tabanlarında taramalar yapılmıştır.

Araştırmada veri toplama süreci, 1174 uluslararası üniversitelerin 146 adet veri yönetişimi politika belgeleri, Türkiye’de veri yönetişimi alanında kurumsal yapılanmaya sahip 24 adet yükseköğretim kurumunun kamuya açık belgeleri ve web sayfaları ile bu kurumların 10 tanesinin temsilcileriyle gerçekleştirilen yarı yapılandırılmış görüşmelerden oluşmaktadır. Bu araştırmada görüşme ve belge incelemesi yoluyla elde edilen veriler tematik analiz yöntemiyle çözümlenmiştir.

ABD, Avustralya ve BK’deki 1174 üniversitenin web sayfası değerlendirmeye alınmıştır. 146 üniversitenin veri yönetişimi politikasına erişim sağlanmıştır (Bkz. Ek 5). Uluslararası veri yönetişimi politikaları PDF formatında indirilmiş ve veriler temizlendikten sonra 984 sayfa metin MaxQDA nitel veri analizi yazılımına aktarılmıştır.

Türkiye’deki veri yönetişimi alanında kurumsal yapılanmaya sahip olan yükseköğretim kurumlarının web siteleri, organizasyon şemaları, politika belgeleri, yönergeleri ve yönetmelikleri incelenmiştir. Tablo 1’de sunulan 24 adet üniversitenin veri yönetişimi yaklaşımlarını anlayabilmek amacıyla veri yönetişimi biriminin web sayfaları tarihçe, amaç, hedefler, misyon, vizyon ve görevler başlıkları altında incelenmiştir. İncelemeler sonucunda veri yönetişimi ile ilgili yedi adet üniversitenin yönergesi, yedi adet üniversitenin yönetmeliği, bir adet üniversitenin veri yönetişimi politikası bulunmuştur. Geri kalan dokuz üniversitenin konu ile ilgili hiçbir belgesi bulunmamaktadır. Toplamda 15 adet kamuya açık yönerge, yönetmelik, politika ve ayrıca hazırlanan web sitelerinde geçen ifadeler tematik analiz yöntemi ile yine MaxQDA nitel veri analizi yazılımına aktararak 85 sayfa metin değerlendirilmiştir (Bkz. Ek 4).

Yine Tablo 1’de sunulan 24 adet üniversite ile veri yönetişimi yaklaşımlarını anlayabilmek amacıyla yarı yapılandırılmış görüşme yapılması planlanmıştır. Görüşme, belirli bir amaç doğrultusunda katılımcılardan veri elde etmeye yönelik, etkileşimli ve sistematik bir iletişim süreci olarak tanımlanmaktadır (Stewart ve Cash, 2017, s. 7). Bu doğrultuda, araştırma için yarı yapılandırılmış görüşme formu hazırlanmıştır (Bkz. Ek 3).

Yarı yapılandırılmış görüşmeler, önceden hazırlanmış sorulara dayansa da görüşme sırasında ortaya çıkan yeni düşünceler doğrultusunda esnek biçimde derinleştirilebilen nitel veri toplama aracıdır (Yıldırım ve Şimşek, 2021, s. 130).

Hazırlanan görüşme formu için Sosyal ve Beşerî Bilimler Araştırma Etik Kurulu'na başvuruda bulunulmuştur. Etik kurul izni geldikten sonra pilot bir görüşmede bulunulmuştur (Bkz. Ek 2). Bu görüşmelerden elde edilen veriler analize dahil edilmiştir. Sonrasında Tablo 1'de sunulan üniversiteler veri yönetişimi birimlerinin ve temsilcilerinin iletişim adresleri bulunmuştur. Her birine Etik Kurul İzni ile beraber yüz yüze veya çevrimiçi platformlar aracılığıyla yarı yapılandırılmış görüşme için davet e-postası gönderilmiştir. Dönüş yapan temsilciler ile 4 Ekim 2024 tarihinden itibaren görüşmelere başlanmıştır. Geri dönüş sağlamayanlara ise belirli aralıklarla hatırlatmalar yapılmıştır.

Tablo 2. Görüşme yapılan yükseköğretim kurumları

No	Üniversite Adı	Birim Adı
1	Yükseköğretim Kurulu	Veri Yönetimi İzleme ve Değerlendirme Daire Başkanı
2	Ankara Üniversitesi	Kurumsal Veri Yönetimi Koordinatörlüğü
3	Atatürk Üniversitesi	Büyük Veri Yönetim Ofisi
4	Dokuz Eylül Üniversitesi	Kurumsal Veri Yönetim Koordinatörlüğü
5	Gazi Üniversitesi	Kurumsal Veri Yönetimi Koordinatörlüğü
6	Hacettepe Üniversitesi	Kurumsal Veri Yönetimi Koordinatörlüğü
7	İstanbul Üniversitesi-Cerrahpaşa	Kurumsal Veri Yönetim Ofisi
8	Lokman Hekim Üniversitesi	Akademik Veri Yönetim Birimi
9	ODTÜ	Kurumsal Büyük Veri Yönetimi Koordinatörlüğü
10	Zonguldak Bülent Ecevit Üniversitesi	Veri Merkezi Koordinatörlüğü

Tablo 2'de gösterilen üniversitelerden görüşülen temsilciler çoğunlukla birim yöneticisidir (6). Diğer temsilciler ise veri yönetişimi birimi personeli olarak görev yapmaktadır (4). Görüşmeler yüz yüze veya çevrimiçi platformlar aracılığıyla yapılması planlanmıştır. Üniversite temsilcilerinden dört yüz yüze, diğer altı tanesi çevrimiçi platform üzerinden görüşmek istemiştir. Görüşmeler ortalama 50 dakika sürmüştür (± 20 dak.).

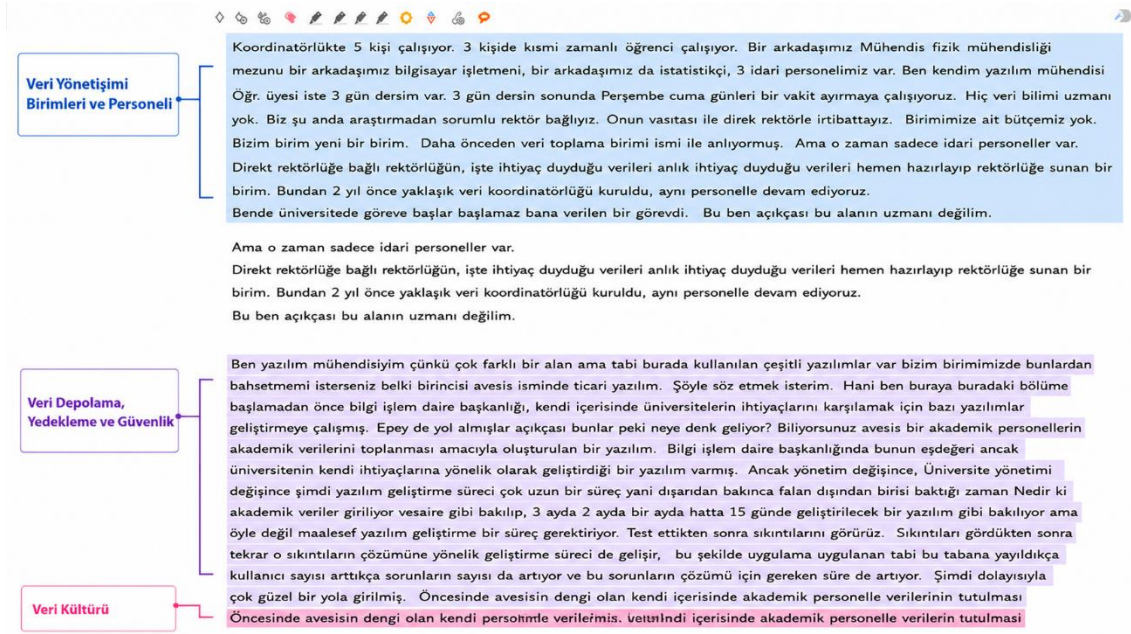
1.5.2. Verilerin Analizi

Uluslararası ve ulusal belge incelemeleri ile yarı yapılandırılmış görüşmelerden elde edilen veriler tematik analiz yöntemiyle çözümlenmiştir. Tematik analiz, nitel veriler

içerisinde yer alan anlam örüntülerinin sistematik biçimde belirlenmesi, analiz edilmesi ve raporlanmasını sağlayan bir analiz yöntemidir (Braun ve Clarke, 2006). Bu yöntem, verileri betimlemek veya görüşme sorularına göre sınıflandırmaktadır. Veri setindeki ortak anlamları yorumlamayı ve araştırma sorularıyla ilişkili temalar geliştirmeyi amaçlamaktadır (Clarke ve Braun, 2013).

Araştırmada tematik analiz, ağırlıklı olarak tündengelimsel bir yaklaşımla yürütülmüştür. Başlangıç kodlama çerçevesi, veri yönetişimi literatürü, araştırma soruları ve incelenen politika belgelerinde yer alan başlıklar doğrultusunda oluşturulmuştur. Analiz sürecinde veri yönetişimi birimleri ve personeli, veri standartları, veri erişimi ve paylaşımı, veri depolama, yedekleme, güvenlik ve gizlilik ile veri kültürü olmak üzere beş temel tema altında toplanmıştır. Bununla birlikte, veri setinde ortaya çıkan ve başlangıç kodlarıyla açıklanamayan anlamlı ifadeler de değerlendirilerek kodlama çerçevesi gözden geçirilmiştir.

Analiz süreci Braun ve Clarke'ın (2006) önerdiği altı aşama doğrultusunda gerçekleştirilmiştir. Yapılan görüşmeler içeriğin analiz edilmesi amacıyla katılımcıların onayları dahilinde cep telefonu ile kayıt altına alınmıştır. İlk aşamada kaydedilen görüşme kayıtları yazılı metne dönüştürülmüştür. Metinde oluşan hatalar düzeltmek için ses kayıtları dinlenerek elle düzeltmeler yapılmıştır. Nitel veri analizine hazır toplamda 75 sayfadan oluşan görüşme kaydı ortaya çıkmıştır. Görüşme kayıtları MaxQDA yazılımına yüklenmiştir. MaxQDA yazılımının kodlama özelliği kullanılarak tematik analiz yapılabilmesi için araştırmanın boyutları kapsamında tematik bir yelpaze oluşturulmuştur. MaxQDA yazılımının kod sistemi altında yer alan alt kodların istatistiği kullanılmıştır (Bkz. Şekil 2).



Şekil 2. MaxQDA kodlama örneği

İkinci aşamada araştırma sorularıyla ilişkili anlamlı ifadeler belirlenmiş ve başlangıç kodları oluşturulmuştur. 85 sayfadan oluşan ulusal üniversitelerin veri yönetişimi belgeleri, 984 sayfadan oluşan uluslararası veri yönetişimi politika metinleri ve 75 sayfadan oluşan görüşme metni sistematik biçimde incelenmiştir. Üçüncü aşamada benzer anlam içeren kodlar bir araya getirilerek aday temalar oluşturulmuştur. Temalar, tekrar sıklığı ve araştırma soruları bakımından anlamlı bir örüntüyü yansıtmaya düzeyine göre belirlenmiştir. Dördüncü aşamada aday temalar, kendi iç tutarlılıkları ve birbirlerinden ayrışma düzeyleri bakımından gözden geçirilmiştir. Kodlanmış veri parçalarının ilgili temayı destekleyip desteklemediği değerlendirilmiştir. Yeterli veriyle desteklenmeyen, diğer temalarla aşırı örtüşen veya kapsamı belirsiz olan temalar yeniden düzenlenmiştir. Bu süreçte bazı kodlar birleştirilmiş, bazıları ayrıştırılmış ve gerekli görülen durumlarda yeniden kodlama yapılmıştır (Bkz. Ek 6).

Beşinci aşamada temaların kapsamı, sınırları ve birbirleriyle ilişkileri açık biçimde tanımlanmış ve isimlendirilmiştir. Tema adları, ilgili veri kümesinin temel anlamını yansıtacak şekilde belirlenmiştir. Bu doğrultuda görüşme ve politika belgesi bulguları, üniversitelerde veri yönetişimi uygulamalarının örgütsel, yönetsel, süreçsel, teknik, kültürel ve yasal-etik boyutlarını ortaya koyacak biçimde yorumlanmıştır. Temaların

nihai hale getirilmesi sürecinde, her bir temanın araştırma sorularına ve veri setinin genel anlatisına nasıl katkı sağladığı değerlendirilmiştir (Braun ve Clarke, 2006; King, 2004).

Son aşamada temalar, araştırma soruları ve ilgili literatürle ilişkilendirilerek raporlaştırılmıştır. Bulgular, katılımcı görüşleri ve belge verilerinden elde edilen örneklerle desteklenmiştir. Görüşme bulguları ile uluslararası veri yönetişimi politikalarından elde edilen bulgular karşılaştırmalı olarak değerlendirilmiş ve bu bulguların geliştirilen katmanlı veri yönetişimi modeline nasıl yansıdığı açıklanmıştır. Model bileşenlerinin görüşme bulguları ile ilişkisi Ek 7’de, uluslararası politika belgelerinden elde edilen bulgularla ilişkisi ise Ek 8’de ayrıntılı olarak gösterilmiştir. Böylece veri setinden kodlara, kodlardan temalara ve temalardan model bileşenlerine uzanan analiz sürecinin izlenebilirliği sağlanmıştır.

1.5.3. Geçerlik ve Güvenirlik

Nitel araştırmaların bilimsel niteliğinin değerlendirilmesinde geçerlik ve güvenirlik temel ölçütler arasında yer almaktadır. Kirk ve Miller’a (1986, s. 19) göre güvenirlik, kullanılan araştırma işlemlerinin farklı koşullarda tutarlı sonuçlar üretme derecesini; geçerlik ise bu işlemler sonucunda doğru cevaba ulaşılma düzeyini ifade etmektedir.

Araştırmanın doğrulanabilirliğini desteklemek amacıyla veri toplama, kodlama, analiz ve yorumlama süreçleri şeffaf biçimde açıklanmış; ulaşılan sonuçların hangi veri kaynaklarına ve bulgulara dayandığı gösterilmiştir. Doğrulanabilirlik, araştırma bulgularının araştırmacının kişisel yargılarından çok araştırmada incelenen verilerin ürünü olmasıyla ilgilidir. Bu ölçütün sağlanmasında denetim izi oluşturulması; araştırmanın yöntem, analiz, bulgu ve sonuç aşamalarının verilerle ilişkisinin izlenebilir biçimde sunulması önem taşımaktadır (Guest vd., 2012). Kodlama güvenirliliğinin test edilmesi amacıyla yalnızca Birleşik Krallık üniversitelerine ait politika belgeleri ve bir adet üniversiteye ait görüşme metni bağımsız bir araştırmacı tarafından yeniden kodlanmıştır. Kodlama sonucunda Cohen’s Kappa katsayısı 0,82 olarak hesaplanmıştır. Bu değer, kodlama sürecinde yüksek düzeyde uyum bulunduğunu ve analiz sürecinin güvenirliliğinin desteklendiğini göstermektedir.

Araştırmanın geçerliğini güçlendirmek amacıyla veri toplama yöntemi, katılımcıların seçimi ve veri analizinde kullanılan araçların araştırmanın amacıyla uyumlu olmasına

dikkat edilmiştir. Bu doğrultuda, araştırmacıların ve kurum temsilcilerinin konuya ilişkin deneyimlerini ve değerlendirmelerini ayrıntılı biçimde ortaya koymaya elverişli olan yarı yapılandırılmış görüşme tekniği tercih edilmiştir. Bu tekniğin görüşme sürecinde gerektiğinde ek sorular yöneltilmesine ve ortaya çıkan yeni konuların derinlemesine ele alınmasına imkân vermesi, elde edilen verilerin kapsamını ve niteliğini artırmıştır. Katılımcılar ise konuya ilişkin farklı deneyim ve kurumsal bakış açılarını yansıtacak şekilde belirlenmiştir. Böylece araştırma olgusunun farklı yönlerden değerlendirilmesi ve bulguların benzer bağlamlar bakımından aktarılabilirliğinin desteklenmesi amaçlanmıştır. Elde edilen bulgular arasında kurumsal koşullardan kaynaklanan bazı farklılıklar bulunmakla birlikte, bulguların genel olarak birbirini desteklediği ve kendi içinde tutarlı bir yapı sergilediği görülmüştür.

Bu çalışmada şekillerin görsel düzenlenmesi ve tasarımının iyileştirilmesinde OpenAI ChatGPT'den yararlanılmıştır. Şekillerin bilimsel içeriği, kavramsal çerçevesi ve yorumları araştırmacı tarafından oluşturulmuştur.

1.6. ARAŞTIRMANIN DÜZENİ

Bu tez çalışması altı bölümden oluşmaktadır. Birinci bölümde araştırmanın konusu, önemi, amacı, problemi, araştırma soruları, kapsamı, yöntemi ve araştırma süreci açıklanmıştır. Ayrıca araştırmanın örnekleme, veri toplama teknikleri ve veri analiz süreci ayrıntılı biçimde ele alınmıştır.

İkinci bölümde veri yönetişimine ilişkin kavramsal çerçeve sunulmuştur. Bu kapsamda verinin kurumsal bir varlık olarak taşıdığı stratejik önem açıklanmıştır. Veri yönetişimi kavramı stratejik, yönetsel, teknik, kültürel ve yasal/etik boyutlarıyla incelenmiştir. Ayrıca veri yönetişimi modelleri, olgunluk modelleri ve konuya ilişkin literatürde yer alan çalışmalar değerlendirilmiştir.

Üçüncü bölümde veri yönetişimine ilişkin uluslararası standartlar, çerçeveler, yasal düzenlemeler ve politika yaklaşımları incelenmiştir. ISO/IEC standartları, DAMA, Veri Yönetişimi Enstitüsü, OECD, UNDP, Dünya Bankası, DCAM ve PwC veri yönetişimi çerçeveleri değerlendirilmiştir. ABD, AB, Avustralya, BK ve Türkiye'nin veri yönetişimi

yaklaşımları karşılaştırmalı olarak ele alınmıştır. Ayrıca yükseköğretim kurumlarının veri yönetişimi çerçeveleri analiz edilmiştir.

Dördüncü bölümde araştırma kapsamında elde edilen bulgular ve değerlendirmeler sunulmuştur. Bu bölümde uluslararası üniversitelerin veri yönetişimi yaklaşımları ile Türkiye'deki üniversitelerin mevcut durumları organizasyonel yapı, veri standartları, veri erişimi ve paylaşımı, veri güvenliği depolama, yedekleme güvenliği ve gizliliği, veri kültürü ve yönetim mekanizmaları açısından karşılaştırmalı biçimde sunulmuştur.

Beşinci bölümde araştırma bulguları doğrultusunda üniversitelere yönelik katmanlı veri yönetişimi modeli önerisi geliştirilmiştir. Önerilen model stratejik katman, yönetim katmanı, süreç katmanı, teknik katman, kültür katmanı ile yasal ve etik katmandan oluşmaktadır. Ayrıca modelin işleyiş yapısı, bileşenleri ve üniversitelerde uygulanabilirliği tartışılmıştır.

Altıncı ve son bölümde ise araştırmanın genel sonuçları değerlendirilmiştir. Elde edilen bulgular doğrultusunda üniversitelerde veri yönetişimi süreçlerinin geliştirilmesine yönelik öneriler sunulmuştur. Bunun yanında gelecekte yapılacak araştırmalar için çeşitli önerilere yer verilmiştir.

2. BÖLÜM

VERİ YÖNETİŞİMİ KAVRAMSAL ÇERÇEVE

2.1. KURUMSAL VARLIK OLARAK VERİLER

Günümüz dijital ekonomisinin temel girdilerinden biri veridir. Geleneksel ekonomilerde mal ve hizmetlerin üretim ve tüketimi gibi, veri ekonomisi de verinin üretilmesi, kullanılması ve yeniden kullanılması üzerine inşa edilmektedir. Bu nedenle veri, ekonomik değer üreten stratejik bir kurumsal varlık olarak değerlendirilmektedir (World Economic Forum, 2021).

Birçok kamu kurumu, veriyi stratejik bir kaynak olarak kabul etmektedir. Ancak verinin kurumsal bir varlık olarak değerlendirilmesi ve karar alma süreçlerine etkin biçimde entegre edilmesi hala önemli bir sorun alanıdır (Benfeldt vd., 2020; Klievink vd., 2017). Kurumların artan hesap verebilirlik ve raporlama gereksinimleri, veriyi daha sistemli bir şekilde yönetmeye zorlamaktadır (Hannila vd., 2019; Khatri ve Brown, 2010). Araştırmalar, veri varlıklarının işletme verimliliği ve süreç performansı üzerinde doğrudan etkili olduğunu göstermektedir (Hu vd., 2022; Ma vd., 2024). Bu nedenle veri, ekonomik değer üreten kurumsal bir varlık olarak değerlendirilmektedir (DAMA, 2013).

Veriden değer üretilebilmesi için verinin eksiksiz, doğru, güncel ve erişilebilir olması gerekmektedir. Ayrıca verilerin güvenli, anlaşılabilir ve birlikte çalışabilir biçimde yönetilmesi önem taşımaktadır (Jolliffe vd., 2021). Bu özellikler, verinin hem kurumsal hem de toplumsal düzeyde etkin kullanımını desteklemektedir.

Veri, kurumun süreçlerini, çalışanlarını ve çıktıları temsil eden önemli bir kaynaktır. Doğru yönetildiğinde yeniden kullanılabilir ve yüksek katma değer üretebilir hale gelmektedir (Panian, 2010). Bu nedenle kurumların veriyi paylaşılabılır ve karar alma süreçleriyle bütünleşik bir kaynak olarak ele alması gerekmektedir.

Verinin kurumsal bir varlık olarak yönetilmesi, veri standardizasyonunu da gerekli kılmaktadır. Veri standartları, kurum genelinde ortak terminoloji ve tutarlılık sağlamaktadır (Abraham vd., 2019; Otto, 2011). Ancak standartların uygulanması kurumların ihtiyaçlarına göre farklılaşabilmektedir. Bu nedenle veri standardizasyonu;

veri sahipliği, erişim ve yönetim süreçleriyle birlikte değerlendirilmelidir (Mahanti, 2019).

Veri kalitesi de veri yönetişiminin temel unsurlarından biridir. Kurumlar, kendi ihtiyaçlarına göre veri kalitesi boyutları belirlemekte ve bu boyutları ölçmektedir (Benfeldt ve Persson, 2025; DAMA, 2013). Veri kalitesinin sürdürülebilir biçimde sağlanabilmesi için güçlü bir veri yönetişimi altyapısına ihtiyaç duyulmaktadır (Askham, 2014).

Sonuç olarak veri yönetişimi verinin etkin, güvenilir ve sürdürülebilir biçimde yönetilmesini sağlayan politika, standart, süreç ve sorumlulukların ele alınmasını ifade etmektedir (Abraham vd., 2019; Brous vd., 2016a; Nielsen, 2017).

2.2. VERİ YÖNETİŞİMİ

Veri yönetişimi kavramı, 1980’li yıllarda veri kalitesi ve üst veri yönetimi alanındaki gelişmelerle birlikte ortaya çıkmıştır. İlk dönemlerde daha çok departman düzeyinde yürütülen veri uygulamaları, 2000’li yıllarda artan düzenleyici gereksinimler ve risk yönetimi ihtiyaçları nedeniyle kurumsal bir yapıya dönüşmüştür. Özellikle Enron skandalı sonrasında yürürlüğe giren Sarbanes–Oxley Yasası¹, üst düzey yöneticileri kurumsal verilerin doğruluğundan sorumlu tutarak veri yönetişimini yasal bir sorumluluk haline getirmiştir (Cheong ve Chang, 2007; SAS, 2018).

Küresel ölçekte veri yönetişimi alanındaki en önemli gelişmelerden biri de Genel Veri Koruma Tüzüğü²’nin (GDPR) yürürlüğe girmesi olmuştur. 25 Mayıs 2018 tarihinde uygulamaya alınan GDPR, kişisel verilerin korunmasını temel alan kapsamlı bir düzenleme sunmuştur. Bu düzenleme, kurumları veri işleme, depolama ve paylaşım süreçlerine ilişkin daha sistemli politika ve mekanizmalar geliştirmeye yöneltmiştir (SAS, 2018). Bu süreçle birlikte kurumlar, veri varlıklarının yönetimine yönelik strateji ve politikalar oluşturmaya daha fazla önem vermeye başlamıştır.

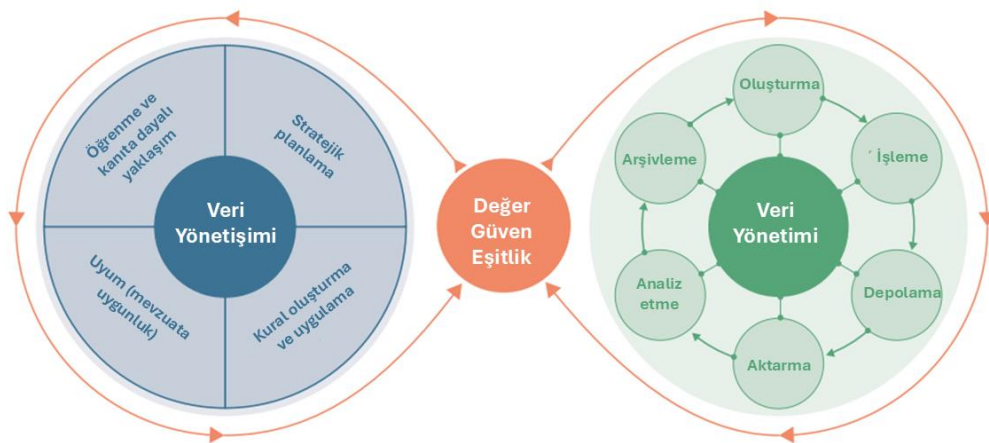
¹Bkz.

https://www.dol.gov/agencies/oalj/PUBLIC/WHISTLEBLOWER/REFERENCES/STATUTES/SARBANES_OXLEY_ACT_OF_2002

² Bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Veri yönetiřimi ve veri yönetimi kavramları birbiriyle iliřkili olmakla birlikte farklı anlamlara sahiptir. Veri yönetiřimi, verinin toplanması, iřlenmesi, kullanılması, paylařılması ve korunmasına iliřkin kuralların, politikaların ve sorumlulukların belirlenmesini ifade etmektedir. Veri yönetimi ise bu kuralların uygulamaya geöirilmesini saęlayan operasyonel süreçleri kapsamaktadır (Khatrı ve Brown, 2010). Bu yönüyle veri yönetiřimi, veri yönetimi süreçlerini yönlendiren üst çeröeveyi oluřturmaktadır. Aynı zamanda veri yönetimiyle ilgili risklerin azaltılmasına katkı saęlamaktadır (Cheong ve Chang, 2007).

Veri yönetimi, verinin oluřturulmasıyla bařlayan ve iřlenmesi, depolanması, paylařılması, analiz edilmesi, arřivlenmesi ve gerektięinde imha edilmesiyle devam eden bir süreçtir. Veri yönetiřimi ise bu süreçlerin hangi kurallar ve standartlar çeröevesinde yürütüleceęini belirlemektedir. Verinin hangi kořullarda toplanacaęı, nasıl standartlařtırılacaęı, kimlerle paylařılacaęı ve nasıl korunacaęı gibi konular veri yönetiřimi kapsamında deęerlendirilmektedir. Bu nedenle veri yönetiřimi, veri yařam döngüsünün her ařamasında karar alma süreçlerine yön veren temel yapı olarak görölmektedir. Veri yönetiřimi ile veri yönetiminin birlikte ve uyumlu biöimde yürütölmesi ise deęer üretimi, güvenin saęlanması ve kurumsal eřitlięin desteklenmesi aöısından önemli sonuçlar ortaya öıkarmaktadır (World Bank, 2021).



řekil 3. Veri yönetiřimi ve veri yönetimi (World Bank, 2021).

Veri yönetiřimi, kurumun sahip olduėu veri varlıkları üzerinde otorite, kontrol ve karar alma süreçlerinin planlanması, yürütölmesi ve izlenmesini kapsayan stratejik bir yönetim yaklaşımıdır (Askham, 2014; DAMA, 2017; Khatri ve Brown, 2010; Otto, 2011). Khatri ve Brown'a (2010) göre, veri yönetiřimi süreci verinin nasıl, hangi, kim tarafından yönetileceėine ve nasıl denetleneceėine yanıt aramaktadır. Bu bağlamda veri yönetiřimi erişim, kontrol, kullanım ve yararlanma haklarını düzenleyen bir çerçeve sunmaktadır. Dolayısıyla, veri yönetiřimi kurumsal politika, organizasyon yapısı ve karar haklarıyla doğrudan ilişkili bir yönetsel süreçtir (Wende ve Otto, 2007). Veri yönetiřimi, verinin erişilebilirliėi, kullanılabilirliėi, bütünlüėü, güvenliėi ve sorumlu biçimde toplanması, işlenmesi, paylaşılması ve yeniden kullanılması süreçlerinin yönetsel, hukuki ve teknik mekanizmalar yoluyla düzenlenmesi olarak görölmektedir (World Bank, 2020). Veri yönetiřimini, verinin ekonomik ve sosyal deėerini en üst düzeye çıkaran, şeffaf ve etik temelli bir karar alma sürecidir. Bu bakış açısına göre, veri yönetiřimi nasıl yönetileceėi sorusu ile birlikte kim tarafından, hangi yetkiyle ve hangi ilkeler doğrultusunda yönetileceėi sorusuna da yanıt üretmektedir (European Commission, 2020a).

Literatür incelendiėinde veri yönetiřiminin kapsamını belirleyen en önemli unsur, verinin nasıl ve kim tarafından kullanılacağına ilişkin kararlardır. Bu kararların açık biçimde tanımlanması, veri yönetiřiminden ne beklendiėini ve hangi düzeyde uygulanacağını belirlemektedir. Khatri ve Brown (2010) bu noktada, etkin bir veri yönetiřimi tasarlamının günlük operasyonlardan bir adım geri çekilmeyi ve veriyi kurumsal düzeyde konumlandırma gerekliliėini vurgulamaktadır.

DAMA'nın (2017) veri yönetimi ve yönetiřimi konularında uygulamaya dönük örnekleri, çoėunlukla kurumsal olgunluk düzeyini artırma ve veri politikalarını standardize etme odaklıdır. Aisyah ve Ruldeviyani (2018) tarafından DAMA modeli kullanılarak veri yönetimi ve yönetiřimi yapısı geliştirilmiřtir. Çalışmanın bulguları, veri yönetiřimi standartlarının açık biçimde tanımlanmasının kamu kurumlarında karar alma süreçlerinin etkinliėini artırdıėını göstermektedir.

Veri yönetiřimi, literatürde stratejik, örgütsel (yönetsel), teknik, kültürel ve yasal/etik olmak üzere beř temel boyut altında ele alınmaktadır. Her bir boyut, veri yönetiřiminin kurumsal düzeyde olgunluk kazanması açısından tamamlayıcı niteliktedir. Bu beř boyut birlikte ele alındıėında, veri yönetiřimi kurumun tüm işlevsel alanlarına nüfuz eden bir

yönetim anlayışını temsil etmektedir. Stratejik boyut, yönetişimin yönünü belirlerken örgütsel boyut, karar ve sorumluluk zincirini tanımlamaktadır. Teknik boyut veri altyapısını oluştururken kültürel boyut, yönetişimin kurum içinde benimsenmesini sağlamaktadır. Yasal/etik boyut ise bu sürecin meşruiyetini güvence altına almaktadır. Bu yaklaşım, kurumların veriyi toplamakla kalmayıp, onu güvenli, tutarlı ve etik biçimde değer üreten bir varlığa dönüştürmelerine olanak tanımaktadır.

2.2.1. Stratejik Boyut

Veri yönetişiminin stratejik boyutu, kurumun veriyle ilişkili misyonunu, vizyonunu, amaçlarını ve yönetsel önceliklerini belirleyen temel bir çerçeve sunmaktadır. Kurumsal veri stratejisinin oluşturulması ve kurumsal süreçlerle entegrasyonu, veri değer yönetimi, risk ve uyum mekanizmaları ile üst yönetim sahipliği gibi temel bileşenleri kapsamaktadır. Stratejik düzeyde veri yönetişimi, kurumsal politika ve karar alma süreçlerinin şekillendirilmesinde belirleyici bir dayanak oluşturmaktadır (Webber ve Zheng, 2020).

Literatürde veri, kurumlar açısından rekabet avantajı sağlayan, karar kalitesini artıran ve sürdürülebilir değer üretimini mümkün kılan stratejik bir varlık olarak ele alınmaktadır (Huff ve Lee, 2020). Bu bağlamda verinin üst yönetim düzeyinde sahiplenilmesi, veri yönetişiminin kurumsal ölçekte benimsenmesini teşvik eden kritik bir unsur olarak öne çıkmaktadır. Stratejik sahiplik perspektifinde veri, kurumsal varlıklar arasında konumlandırılmaktadır. Veri yönetişimi yapıları kurumsal hedeflerle uyumlu biçimde hiyerarşik olarak yapılandırılmaktadır (Cheong ve Chang, 2007; Otto, 2011).

Veri Yönetişimi Enstitüsü'ne (DGI, t.y.) göre veri yönetişiminin temel misyonu, kuruma değer katmaktır. Bu misyon,

- Veri neden önemlidir?
- Hangi stratejik hedefleri desteklemektedir?
- Üretilen değer nasıl ölçülmektedir?

gibi temel sorulara yanıt üretmeyi gerektirmektedir. Bu çerçevede stratejik boyut, şeffaflık, hesap verebilirlik, veri kalitesi ve erişilebilirlik gibi veri yönetişimi ilkelerinin kurumsal politika ve uygulamalarla bütünleşmesini zorunlu kılmaktadır.

Veri yönetişiminin etkinliği, kurumun genel stratejik hedefleriyle uyumlu bir yapı kurulmasına ve üst yönetim desteğiyle kurumsallaştırılmasına bağlıdır (DAMA, 2017, s. 434). Kurumsal hedeflerle uyumlu biçimde geliştirilen veri stratejisi, veri yönetişimi süreçlerinin sürdürülebilir biçimde yürütülmesini sağlamaktadır (Corban, 2021). Bu doğrultuda kurumsal hedeflerle uyumlu bir veri portföyü oluşturulmasını ve yönetilmesini amaçlayan kapsamlı bir kurumsal veri stratejisinin geliştirilmesidir (Abraham vd., 2019; ISO, 2017).

Öte yandan üst yönetim desteği ve stratejik düzeyde sahiplenme, veri yönetişiminin sürdürülebilirliği açısından kritik bir belirleyicidir (Khatri ve Brown, 2010). Veri yönetişimi yapısı, iş birimleri ile bilgi teknolojileri (BT) fonksiyonları arasındaki etkileşimi stratejik, taktiksel ve operasyonel düzeylerde koordine eden çok katmanlı bir mekanizma sunmaktadır. Bu yönüyle veri yönetişimi, kurumsal stratejinin uygulanmasını yönlendiren bir yönetsel yapı olarak değerlendirilmektedir (Cheong ve Chang, 2007, s. 1005).

2.2.2. Örgütsel (Yönetsel) Boyut

Örgütsel (yönetsel) boyut, veri yönetişiminin kurumsal hedeflerle uyumlu biçimde yürütülmesini sağlamak amacıyla liderlik, organizasyon yapısı, roller ve sorumluluklar, karar alma mekanizmaları, performans ölçümü ve hesap verebilirlik unsurlarını kapsamaktadır (ISO, 2017; ISO, 2018). Veri yönetişimi bir karar hakları sistemidir (Khatri ve Brown, 2010). Kurum genelini etkileyen veri kararlarının dengelenmesi ve bağlayıcı hale getirilmesi amacıyla bir veri yönetişimi konseyi oluşturulmaktadır. (Otto, 2011). Hesap verebilirlik ve operasyonel roller için kurum içinde veri sahipleri, veri yöneticileri ve veri kullanıcıları olmak üzere üç temel rol tanımlanmaktadır (DAMA, 2017; European Commission, 2020a; Otto, 2011). Veri sahipleri belirli veri varlıklarının doğruluğu ve tutarlılığı açısından hesap verebilir konumdadır. Veri sorumluları bu verilerin yönetimine ilişkin kural ve süreçleri geliştirerek operasyonel sorumluluğu

üstlenmektedir. Veri sorumluluğu yapısı kendi içinde baş veri sorumlusu, iş veri sorumluları ve teknik veri sorumluları şeklinde katmanlaşabilmektedir (Otto, 2011).

Mahanti'nin (2019) veri yönetiřimi yapısı, rollerin tanımlanması ile başladıđını ve bu rollerin arasındaki iletiřim, koordinasyon ve raporlama iliřkilerinin de kurumsallařtırılmasıyla iřlerlik kazandıđını vurgulamaktadır. Bu yapıların tanımlanmasının yeterli olmadıđını, aynı zamanda aralarındaki iletiřim ve koordinasyon mekanizmalarının da kurumsallařtırılması gerektiđi belirtilmektedir. Bu boyut, veri yönetiřimini bir karar hakları sistemi olarak tanımlayan Khatri ve Brown (2010) yaklařımıyla da örtüşmektedir.

Bu durumla birlikte Weber vd. (2009), veri yönetiřimi organizasyonlarının tek tip bir yapıya sahip olamayacađını, kurumun büyüklüğüne, veri olgunluk düzeyine ve yönetsel kültürüne göre deđiřebileceđini belirtmektedir. Bununla birlikte, tüm kurumlarda ortak olan unsur, veriyle ilgili kararların yetki, sorumluluk ve hesap verebilirlik ilkeleri çerçevesinde tanımlanmasıdır. Veri yönetiřimi yönetsel boyutu, hesap verebilirlik, rol netliđi ve karar alma süreçlerinin řeffaflıđı ilkelerine dayanmaktadır (Cheong ve Chang, 2007).

2.2.3. Teknik Boyut

Veri yönetiřiminin teknik boyutu, verinin bütün yařam döngüsü boyunca yönetimini sađlayan sistematik süreçleri, standartları ve teknolojik altyapıları içermektedir. Teknik altyapının veri stratejileri, veri politikaları ve kurumsal hedeflerle uyumlu çalışması ve uygulanabilirliđi temel prensiplerinden biridir. Veri yönetiřimini dinamik ve sürekli gelişen bir kurumsal kapasite olarak deđerlendirilmektedir (ISO, 2017). Veri yönetiřiminin başarısı, kurum içinde standartlara dayalı bir politika çerçevesinin uygulanmasına bađlıdır. Bu politikalar, veri tanımlama ve sınıflama, veri eriřimi, yetkilendirme, veri mimarisi řemaları ve teknik kalite eşikleri (üst veri yönetimi, veri kalitesi yönetimi, veri güvenliđi yönetimi) gibi konuları içermelidir (ISO, 2023a; Mahanti, 2019, s. 335–337).

Teknik boyut veri mimarisi, veri kalitesi, üst veri yönetimi, veri güvenliđi, veri entegrasyonu ve depolama yönetimi gibi iřlevleri kapsamaktadır (DAMA, 2017). Teknik boyutun amacı verinin dođruluk, bütünlük, erişilebilirlik ve süreklilik ilkeleri

doğrultusunda yönetilmesini sağlamaktır (European Commission, 2020a). Teknik altyapının güçlü olduğu yapılarda veri yönetişiminin daha etkin işlediğini ve bu durumun karar alma kalitesini doğrudan etkilenmektedir (DAMA, 2017; Miller vd., 2024).

Mahanti (2019), veri yönetişiminin teknik altyapısının veri kalitesi yönetimi, veri bütünlüğü ve erişilebilirlik gibi kriterleri desteklemesi gerektiğini vurgulamaktadır. Veri kalitesi aynı zamanda maliyet azaltma, yasal uyum ve müşteri memnuniyeti gibi iş hedefleriyle doğrudan ilişkilidir. Kalitesiz veri, karar alma süreçlerinde hatalara, operasyonel süreçlerde gecikmelere ve kurum itibarında kayıplara neden olabilmektedir. Bu nedenle, kurumların veri kalitesi göstergelerini sürekli ölçmesi, hatalı kayıtları belirlemesi ve neden analizleriyle iyileştirme planları geliştirmesi gerekmektedir. (Panian, 2010). Veri kalitesinin artırılması için izleme ve raporlama mekanizmalarının kurulması, veri yönetişiminin geliştirilmesi gereken alanlarından biri olarak gösterilmektedir (Eroğlu, 2025).

Veri yönetişiminin teknik boyutu, veri standardizasyonundan³ kalite denetimine kadar uzanan bir dizi operasyonel süreci içermektedir. Veri modelleme ve üst veri yönetimi bileşenleri aracılığıyla kurumsal veri alanlarının standartlaştırılması sağlanmaktadır (ISO, 2023b). Bu süreçlerin amacı, verilerin doğru, güvenli, erişilebilir ve sürdürülebilir bir biçimde yönetilmesini sağlamaktır (Liu, 2020). Bu sebeple özellikle üst veri katalogları ve veri sözlüğü ile ortak veri dili oluşturulması bu boyutu yapılandırmaktadır (ISO, 2023b).

Mahanti (2019), teknik boyutta iş birimleri ile BT departmanları arasında açık bir rol ve sorumluluk paylaşımının olması gerektiğini belirtmektedir. Koltay (2016), veri yönetişiminin teknik boyutunun sadece BT departmanlarının sorumluluğunda olmadığını, tüm organizasyonun dijital okuryazarlık düzeyiyle doğrudan ilişkili olduğunu vurgulamaktadır.

³ Kurum içindeki farklı sistemlerin veriyi ortak tanımlar üzerinden işlemesini sağlamaktadır.

Ridzuan ve Zainon (2024), teknik kapasitenin artırılabilmesi için veri yönetişimi yaklaşımlarının politika belgeleri düzeyinde kalmaması, aynı zamanda bu politikaları destekleyecek teknik standartların (örneğin veri modelleme yöntemleri, API kullanımı, veri güvenliği protokolleri) geliştirilmesi gerektiğini savunmaktadır.

Sidi vd. (2012), veri kalitesini iyileştirmeye yönelik teknik stratejileri veri odaklı⁴ (data-driven) ve süreç odaklı⁵ (process-driven) yaklaşımlar olmak üzere ayırmaktadır. Veri kalitesini değerlendirme sürecinde kullanılan doğruluk, tutarlılık, bütünlük, güncellik, erişilebilirlik, güvenlik, kullanılabilirlik ve yorumlanabilirlik gibi kalite boyutları da teknik yaklaşımın temelini oluşturmaktadır. Teknik düzeyde veri kalitesinin sistematik olarak ölçülmesini sağlamaktadır.

Hikmawati vd. (2021) veri yönetişiminin teknik boyutunun başarısı, ana veri yönetimi olgunluk düzeylerinin (veri modeli, veri kalitesi, kullanım ve sahiplik, veri koruma ve sürdürülebilirlik) değerlendirilmesiyle ölçülebilir. Bu tür ölçümler sayesinde organizasyonlar, mevcut durumlarını analiz edebilir ve iyileştirme stratejileri geliştirebilir.

⁴ Veri Odaklı Stratejiler, doğrudan veri değerlerini iyileştirmeye yönelik müdahaleleri içerir. Yeni veri edinimi, standardizasyon, hata tespiti ve düzeltme, kayıt eşleştirme, şema entegrasyonu ve kaynak güvenilirliği gibi teknikler bu kapsamda değerlendirilir. Bu teknikler kısa vadede etkili olsalar da uzun vadede maliyetli olabilirler.

⁵ Süreç Odaklı Stratejiler ise, verilerin üretildiği iş süreçlerini yeniden tasarlayarak kaliteyi artırmayı hedefler. Süreç kontrolü ve süreç yeniden tasarımı gibi yöntemlerle, verilerin oluşturulduğu noktadaki kalite sorunlarının kökenine inilerek kalıcı çözümler geliştirilir. Bu stratejiler uzun vadede daha sürdürülebilir ve düşük maliyetlidir

2.2.4. Kültürel ve Davranışsal Boyut

Kültürel boyut, veri yönetişiminin kurum içinde benimsenmesi ve sürdürülebilmesi açısından kritik bir faktördür. Veri kültürü kurumun problem çözme, karar alma ve stratejik hedeflere ulaşma süreçlerinde veriyi kullanmaya ilişkin ortak değerler, inançlar, tutumlar ve uygulamalar bütünüdür (Griffin ve Holcomb, 2023). Veri odaklı kültür ise veri kültürünün daha gelişmiş bir biçimi olarak değerlendirilmektedir. Etkili veri analizi, veri temelli karar alma ve sürekli veri kullanımını destekleyen belirli davranış kalıpları ile açıklanmaktadır (Kremser ve Brunauer, 2019). Veri yönetişiminin başarıya ulaşması kurum çalışanların veriyle ilgili tutumları, farkındalık düzeyleri ve davranış biçimleriyle de doğrudan ilişkilidir (Klievink vd., 2017). Klievink vd. (2017) çalışması, veri yönetişimi politikalarının tasarımı ve uygulanmasında kültürel uygunluk kavramının dikkate alınması gerektiğine dair güçlü bir çerçeve sunmaktadır.

Özellikle veri yöneticileri ve veri sorumlularının, veri kültürünü veri odaklı kültüre dönüştüren kritik aktörler olduğu belirtilmektedir (Kremser ve Brunauer, 2019). Veri odaklı kültürün gelişmesi, çalışanların veri kalitesini bir sorumluluk olarak görmelerini ve veri kullanımına yönelik ortak bir anlayış geliştirmelerini sağlamaktadır. Veri kalitesinin sürdürülebilirliğinde veri farkındalığı, veri okuryazarlığının artırılması, personel eğitimi ve kurum içi iletişimin kritik rol oynadığını vurgulamaktadır. (Mahanti, 2019).

Bu boyutta temel amaç, kurum genelinde bir veri kültürü oluşturmak, yani çalışanların veriyi güvenilir bir kaynak ve stratejik varlık olarak görmelerini sağlamaktır. Veri yönetişimi süreçlerinin etkili olabilmesi için bu kültürel yapıların dikkate alınması gerekmektedir. Kurum kültürünü sahip olduğu ortak değerler, inançlar ve iletişim kalıpları karar alma süreçlerini ve bireylerin/kurumun davranış biçimlerini şekillendirmektedir (Putro vd., 2016). Özellikle kurum içi işleyişi, yönetim süreçlerini ve kültürel dinamikleri merkeze alındığında veri yönetişimin kültürel boyutunu görünür kılmaktadır (Salerno ve Maçada, 2025).

DAMA (2017) uzun süreli veri yönetişimi programlarının kurumsal düşünce ve verilerle ilgili davranışlarda kültürel anlamda değişim sağlayacağını söylemiştir. Kurumların

gelecekte arzu edilen düşünceleri, davranışları, politikaları ve süreçleri desteklemesi için değişim yönetimi gerektirmektedir.

Kotter'in (2012) Büyük Değişim İçin Sekiz Aşamalı Süreci⁶ kurumsal dönüşüm süreçlerinin neden başarısız olduğunu sekiz temel hata üzerinden açıklamaktadır. Bu çerçevede, veri yönetişimi kültürünü kurumsallaştırmak isteyen organizasyonlar için de oldukça öğretici ve yol gösterici bir temel sunmaktadır.

2.2.5. Yasal ve Etik Boyut

Veri yönetişiminin yasal ve etik boyutu, verinin gizlilik, güvenlik, fikrî mülkiyet, mevzuata uyum ve etik kullanım ilkeleri doğrultusunda yönetilmesini içermektedir. Bu boyut, özellikle kamu kurumları açısından önem taşımaktadır. Yasal boyut, veri yönetişimi süreçlerinin ulusal ve uluslararası mevzuatlara uygun olarak yürütülmesini ifade etmektedir. Veri yönetişimi yasal uyum ve risk yönetimi aracı olarak işlev görmektedir (World Economic Forum, 2021). Bu sebeple veri yönetişimi kişisel verilerin kullanımı ve korunması için güvenilir bir mekanizma oluşturmayı amaçlamaktır (Janssen vd., 2020; Khatri ve Brown, 2010; Verhulst, 2021).

AB'nin GDPR, veri sahipleri için şeffaflık, erişim, düzeltme, silme, itiraz etme hakları gibi korumalar sağlayan veri yönetişimine uluslararası çerçeve sağlayan yasalardandır (Schubert ve Barrett, 2024). Mahanti (2019) çalışmasında, veri yönetişiminin GDPR gibi düzenlemelerle doğrudan ilişkili olduğunu ve kişisel verilerin korunmasına yönelik

1. Aciliyet Duygusu Oluşturmak: Veri yönetişimi kültürünü oluşturmak için de veri kalitesi sorunları, veri temelli kararların zayıflığı ya da yasal riskler gibi somut tehditler vurgulanarak veri yönetişimine neden ihtiyaç duyulduğu net bir şekilde anlatılmalıdır.

2. Güçlü Bir Yönlendirme Koalisyonu Kurmak: Veri yönetişimi kültürü, üst düzey yöneticiler, BT ekipleri, veri sahipleri ve iş birimi liderlerinden oluşan güçlü bir koalisyon oluşturulmalıdır.

3. Net ve Anlaşılır Bir Vizyon Geliştirmek: Verinin nasıl bir değer üreteceği, kurumun veriyle nasıl bir ilişki kuracağı ve bu kültürün nasıl bir işleyişe yol açacağı açıkça tanımlanmalıdır.

4. Vizyonu Yaygınlaştırmak: Veri yönetişimi vizyonunun tüm kuruma yayılması kritik önemdedir.

5. Engellerin Kaldırılması: Veri yönetişimini engelleyen mevcut iş süreçleri, rol tanımları veya direnç gösteren yöneticiler dönüşümün önünde ciddi engellerdir.

6. Kısa Vadeli Kazanımlar Sağlamak: Veri yönetişimi kültürünün başarıya ulaşması için çalışanların çabalarının kısa vadede görünür sonuçlar doğurması gerekir.

7. Başarıları Pekiştirmek ve Değişimi Derinleştirmek: Başarılar yeni projelerle pekiştirilmeli, daha derin yapısal değişikliklere zemin hazırlamalıdır. Veri yönetişimi ilkeleri iş süreçlerine ve organizasyonel yapıya entegre edilmelidir.

8. Yeni Kültürü Kurumsallaştırmak: Son aşamada veri yönetişimi uygulamaları, kurumun iş yapma biçimi haline gelmelidir. Bu, yeni davranışların kurumsal değerlerle ilişkilendirilmesini, veri odaklı liderlerin terfi ettirilmesini ve eğitim süreçlerinde bu kültürün işlenmesini içerir.

politikaların yönetim çerçevesine dahil edilmesi gerektiğini belirtmektedir. BK da AB bünyesinden ayrıldıktan sonra 2018 yılında GDPR'ye benzer BK Veri Koruma Yasası'nı⁷ (Data Protection Act, DPA) kabul etmiştir (Schubert ve Barrett, 2024). BK Genel Veri Koruma Yönetmeliği (BK GDPR) ve DPA düzenlemelerinde önemli değişiklik yapmak için Veri Koruma ve Dijital Bilgi Yasası (DPDI) geliştirilmeye başlanmıştı. DPDI sonuçlandırılmadığı için 2024 yılında Veri (Kullanım ve Erişim) Yasa Tasarısı (DUA Yasa Tasarısı) olarak yeniden adlandırılmıştır. DUA Yasa Tasarısı, 2025 yılında yürürlüğe girmiştir (Castro-Edwards, 2025).

ABD'nin GDPR'ye benzer 1974 tarihli Gizlilik Yasası⁸, federal kuruluşlar tarafından tutulan bilgilere erişim hakkı sağlamaktadır. Yine ABD'de finansal verileri Gramm-Leach-Bliley Yasası⁹ (GLBA), sağlık verilerini Sağlık Bilgilerinin Gizliliği¹⁰ (HIPAA), 13 yaşın altındaki kişilerin kişisel verilerinin toplanmasını için Çocukların Çevrimiçi Gizliliğini Koruma Yasası¹¹ (COPPA), sürücülerin kişisel verilerini koruyan Sürücü Gizliliğini Koruma Yasası¹² (Driver's Privacy Protection Act, DPPA) gibi düzenlemeler, veri sahiplerinin haklarını korumaya yönelik kapsamlı çerçeveler sunmaktadır (Schubert ve Barrett, 2024).

ABD'nin Kaliforniya eyaletinde, Gizlilik Hakları Yasası¹³ sağlık ve finansal veriler hariç GDPR'ye benzerliği ile dikkat çekmektedir. ABD'deki sadece eyalette geçerli en güçlü veri gizliliği yasası olarak vatandaşların gizlilik ihlalleri nedeniyle şirketlere dava açmasına olanak sağlanmaktadır (Schubert ve Barrett, 2024). Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Teksas, Utah ve Virginia dahil olmak üzere birçok ABD eyaleti kendi veri gizliliği yasalarını yürürlüğe koymuştur (Kirvan, 2025).

⁷ Bkz. <https://www.legislation.gov.uk/ukpga/2018/12/contents>

⁸ Bkz. [https://www.congress.gov/crs-product/R47863#:~:text=The%20Privacy%20Act%20of%201974%20\(Privacy%20Act%3B%205%20U.S.C.,may%20use%20or%20disclose%20it.](https://www.congress.gov/crs-product/R47863#:~:text=The%20Privacy%20Act%20of%201974%20(Privacy%20Act%3B%205%20U.S.C.,may%20use%20or%20disclose%20it.)

⁹ Bkz. <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>

¹⁰ Bkz. <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

¹¹ Bkz. <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312>

¹² Bkz. <https://www.congress.gov/bill/103rd-congress/house-bill/3365>

¹³ Bkz. <https://thecpra.org/>

Etik boyut ise, yasal zorunlulukların ötesine geçerek birey haklarına, mahremiyete ve toplumsal eşitliğe saygı gösterilmesini esas almaktadır. Gizlilik, güvenlik ve şeffaflık, etik veri yönetişiminin temel bileşenleri arasındadır (Ige vd., 2024). Etik konunun çerçevelendirilmesi, veri toplama ve kullanım süreçlerinde şeffaflık, hesap verebilirlik ve adalet ilkeleri doğrultusunda karar alma mekanizmalarının oluşturulmasını içermektedir (Chen, 2017). Aynı zamanda bu ilkeler güvenilir veri koruma düzenlemelerinin altyapısını oluşturmaktadır (Khatrı ve Brown, 2010; Verhulst, 2021). Verilerin gizliliği ve güvenliği sağlanırken şeffaflık ilkesinin sağlanması zorlu bir süreçtir (Ige vd., 2024).

2.3. VERİ YÖNETİŞİMİ İLE İLGİLİ ÇALIŞMALAR

Literatürde veri yönetişiminin birbirinden farklı birçok tanımı bulunmaktadır (Abraham vd., 2019). Literatür okumaları sonucu en genel geçer tanımı, Khatrı ve Brown (2010) tarafından geliştirilen “*organizasyonel veri varlıklarının etkin yönetimi için karar hakları, sorumluluklar ve kontrol mekanizmalarını kapsayan üst düzey bir yönetsel yaklaşım*” olarak belirlenmiştir (Khatrı ve Brown, 2010).

Bu durumla birlikte veri yönetimi ile veri yönetişimi arasındaki ayrım da literatürde açık biçimde vurgulanmaktadır (Khatrı ve Brown, 2010). Veri yönetişimi veri yönetimi süreçlerini yönlendiren politikaların, standartların ve kuralların belirlenmesi, uygulanması ve izlenmesini içeren bir yapı olarak tanımlanmaktadır (Brous ve Janssen, 2020). Veri yönetimi verinin teknik olarak işlenmesi ve yönetimine odaklanırken, veri yönetişimi bu süreçlere ilişkin karar alma yetkileri ve hesap verebilirlik mekanizmalarını kapsamaktadır (Abraham vd., 2019; Khatrı ve Brown, 2010; Plotkin, 2013).

Yine literatürde veri yönetişimi yaklaşımlarının uzun süre BT odaklı, parçalı ve sistem bazlı yürütüldüğü, organizasyon genelinde kurumsal bir yapıdan yoksun olduğu ifade edilmektedir (Nielsen, 2017; Panian, 2010; Weber vd., 2009). Bu durumun temel nedenlerinden biri, veri yönetişiminin hangi süreçleri kapsadığı, neyi koordine ettiği ve nasıl uygulanması gerektiğine dair somut ilkelerin olmamasıdır. Diğer önemli nedeni, veri yönetişiminin farklı tanımlarının bulunması ve kavramsal olarak net biçimde tanımlanamamasıdır (Brous vd., 2016b).

Veri yönetişimi tanımındaki çeşitlilik, standartlaşmayı zorlaştırırken uygulamada belirsizliklere yol açmaktadır (SAS, 2018). Veri yönetişimi alanlarından olan tanımlama

veri rolleri, politikalar, süreçler ve standartların belirlenmesini içeren en yoğun aşamasıdır. Uygulama ve izleme aşamalarının güçlendirilmesi gerekmektedir (Alhassan vd., 2016). Veri yönetiřimi literatüründeki en önemli boşluklar çok teorik olması, uygulama detaylarının yetersiz kalması, rollerin net tanımlanmaması, süreçlerin operasyonelleřtirilememesidir (Karkošková, 2023). Veri yönetiřiminin tanımlamasında olan çeřitlilik akademik ve kurumsal anlamda geliřtirilen çerçevelerinde de görölmektedir.

Veri yönetiřimi çerçevelerinin hemen hemen birçoğunda rol ve sorumlulukların tanımlanması, politika ve standartların oluřturulması, veri kalitesi yönetimi, güvenlik, üst veri yönetimi ve kurumsal karar alma mekanizmaları temel bileřenler olarak öne çıkmaktadır. Veri yönetiřimi hiyerarřik yapıdadır (Otto, 2011). Veri sahibi, veri sorumlusu, yönetici, karar verici gibi organizasyonel roller, sorumluluklar ve karar alma yetkileri açık biçimde tanımlanmalıdır (Alhassan vd., 2016; Brous vd., 2016b; Cheong ve Chang, 2007; DGI, t.y.; El Abed ve Njonko, 2014; Jang ve Kim, 2021; Wende ve Otto, 2007). Bu tanımlama veri yönetiřiminin hesap verebilirlik ve otorite boyutunu güçlendirmektedir (Weber vd., 2009). Karar alma yetkisinin merkezi ya da dağıtık şekilde konumlandırılması ise organizasyonel etkinliğı doğrudan etkilemektedir (Khatri ve Brown, 2010).

Veri yönetiřiminin veri sahipliğı algısına bağılı taahhüt eksikliğı ile üst düzey yönetici desteğinin yetersizliğı, veri yönetiřimi giriřimlerinin kurumsallařmasının önündeki en kritik engeller arasında deęerlendirilmektedir (Schubert ve Barrett, 2024). Ancak birçok kurumda veri yönetiřimi halen BT'nin bir sorunu olarak görölmekte ve bu durum yönetiřimin kurumsal stratejiyle bütünleřmesini engellemektedir (DGI, t.y.; SAS, 2018). Birçok veri yönetiřimi çerçevesinde veri stratejisi, politikalar, standartlar ve süreçler üzerinden veri yönetiřiminin nasıl yürütöleceğı belirlenmektedir (Al-Badi vd., 2018; Brous vd., 2016b; DAMA, 2009; DGI, t.y.; El Abed ve Njonko, 2014). Veri yönetiřiminin sadece belgelenmiř politikalarla ilgili olduğı yönünde yaygın bir yanlış anlamada vardır (Mahanti, 2019). Oysa veri politikalarının oluřturulması ve uygulanması, organizasyon genelinde veri kullanımına iliřkin tutarlılığı saęlamaktadır (Alhassan vd., 2016). Veri standartları ise birlikte çalışabilirliğı desteklemektedir (Otto, 2011).

Bunun yanı sıra organizasyonel kültür, karar alma yapıları ve kurumsal alışkanlıklar da veri yönetişiminin etkinliğini doğrudan etkilemektedir. Parçalı organizasyon yapıları, merkezi olmayan karar alma süreçleri ve kurum kültürünün yeterince dikkate alınmaması, veri yönetişimi uygulamalarını zorlaştıran diğer önemli faktörler arasında yer almaktadır (SAS, 2018).

Son dönemdeki çalışmalar, veri yönetişiminin veri okuryazarlığı eksikliği, veri borcu ve standartlaşma sorunları gibi çok boyutlu zorluklar içerdiğini ortaya koymaktadır (Legner vd., 2023). Veri okuryazarlığı, organizasyonel farkındalık ve kültürel dönüşümün veri yönetişimi başarısında kritik rol oynadığı vurgulanmaktadır (Fattah, 2024). Bu bağlamda kurumların, kendi ihtiyaçlarına uygun, esnek ve stratejik hedeflerle uyumlu veri yönetişimi yaklaşımları geliştirmesi gerekmektedir. Ayrıca veri yönetişiminin çok aktörlü ve çok düzeyli bir yapı olduğu, ekonomik değer üretiminin yanı sıra kamu yararı ve veri adaleti boyutlarını içerdiği vurgulanmaktadır. Bu doğrultuda gelecekte hibrit ve karma veri yönetişimi modellerinin daha fazla önem kazanacağı öngörülmektedir (Micheli vd., 2020).

Verinin değerini belirlemede en önemli zorluklar, kurumlar arasında farklı veri yönetişimi standartlarının bulunması, verilerin ekonomik etkilerinin doğrudan izlenememesi ve değer ölçümünde nitel verilerin nicelleştirilmesindeki sorunlar yer almaktadır (Ai vd., 2023). Birçok veri yönetişimi modelinde de veri kalitesi; doğruluk, tutarlılık, standartlara uygunluk ve izleme mekanizmaları birlikte ele alınmaktadır (Abraham vd., 2019; Al-Badi vd., 2018; Hanisch vd., 2023; Jang ve Kim, 2021; Khatri ve Brown, 2010; Wende ve Otto, 2007). Kurumlarda veri kalitesi veri tekrarları ve tutarsızlıkları sorunları verinin farklı birimler tarafından üretilmesinden kaynaklanmaktadır (Schubert ve Barrett, 2024).

Farklı birimlerde üretilen veriler, etkili veri yönetişimi politikaları ile kurum genelinde işbirliğine dayalı bir sisteme ihtiyaç duyabilirler (Schubert ve Barrett, 2024). Bireysel çıkarların ön planda olması, iş birliğini zorlaştırmakta ve veri yönetişimi uygulamalarının

başarısını sınırlamaktadır. Bu nedenle veri yönetişimini kolektif eylem teorisi¹⁴ çerçevesinde ele alan çalışma literatüre önemli bir katkı sunmaktadır (Benfeldt vd., 2020).

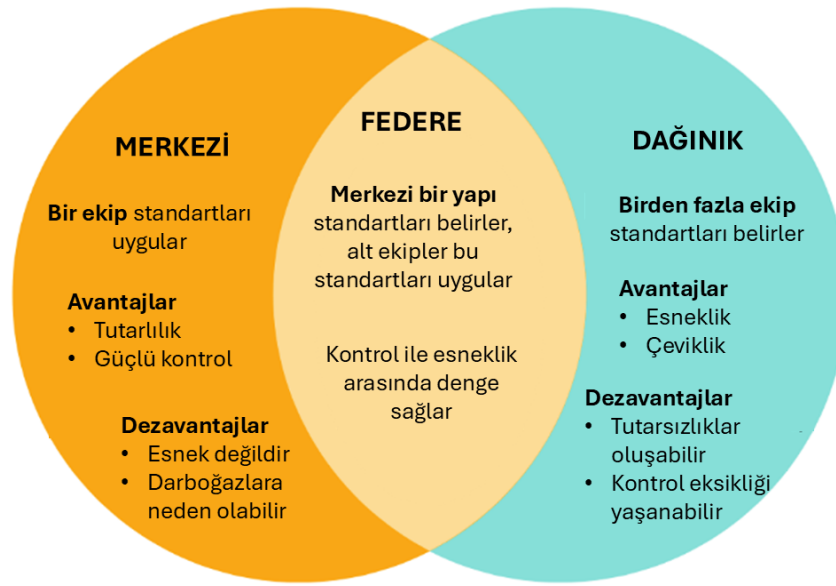
Veri yönetişimi teknolojik gelişmelerden kaynaklanan halen gelişmekte olan bir alandır. Özellikle yapay zeka, bulut bilişim büyük veri ve nesnelerin interneti gibi alanlarda veri koruma ve yönetim açısından önemli yapısal boşlukların devam ettiğini göstermektedir (Al-Ruithe vd., 2019; Bena vd., 2025; Kuzio vd., 2022). Türkiye’de veri yönetişimine ilişkin çalışmaların ağırlıklı olarak dijital dönüşüm, veri güvenliği ve kişisel verilerin korunması ekseninde geliştiği görülmektedir (Eroğlu, 2025). Bu durum, daha kapsamlı veri yönetişimi modellerine ihtiyaç olduğunu ortaya koymaktadır (Al-Ruithe vd., 2019).

2.4. VERİ YÖNETİŞİMİ MODELLERİ

Kurumsal veri yönetişimi programlarının tasarlanması sürecinde organizasyonların büyüklüğü, kurumsal yapı özellikleri ve veri kullanım gereksinimlerine uygun bir operasyonel modelin belirlenmesi gerekmektedir. Veri yönetişimi operasyonel modeli, kurum içerisinde verinin nasıl yönetileceğini, veri sahipliği ve sorumlulukların nasıl dağıtılacağını, karar alma süreçlerinin nasıl işleyeceğini ve veri yönetişimi uygulamalarının hangi mekanizmalar aracılığıyla yürütüleceğini belirleyen temel bir yönetsel çerçeve sunmaktadır. Bu model aynı zamanda veri yönetişimine ilişkin operasyonel yönergeleri tanımlamaktadır. Denetim mekanizmalarını oluşturmakta ve veri sahipliği ile karar alma süreçleri için gerekli organizasyonel altyapıyı sağlamaktadır (Acceldata, 2025; Alation, 2025; Atlan, 2023; Claravine, t.y.).

Literatürde veri yönetişimi operasyonel modelleri genel olarak merkezi (centralized), dağınık (decentralized) ve federe (hybrid/federated) modeller olmak üzere üç temel kategori altında ele alınmaktadır (Bkz. Şekil 4). Bu modeller, veri yönetişiminde kontrol düzeyi, karar alma yetkisi, veri sahipliği ve organizasyonel esneklik açısından farklı özellikler göstermektedir (Acceldata, 2025; Alation, 2025; Altexsoft, 2023; Atlan, 2023; Claravine, t.y.; Farmer, 2024; Lifebit, 2025).

¹⁴ Veri yönetişimi, farklı çıkar ve yetkinliklere sahip aktörlerin ortak bir hedef doğrultusunda hareket etmesini gerektiren bir süreçtir.



Şekil 4. Veri yönetiřimi modelleri (Alation, 2025)

Şekil 4’te merkezi, merkezi olmayan ve federe veri yönetiřimi modelleri karar verme, ölçeklenebilirlik, çeviklik, tutarlılık, mülkiyet, maliyet ve risk yönetimi gibi temel yönetsel boyutlar açısından karşılaştırılmaktadır. Tablodaki en dikkat çekici nokta, üç veri yönetiřimi modelinin kontrol, esneklik ve ölçeklenebilirlik arasında farklı öncelikler belirlediğı görölmektedir. Merkezi model kontrolü, dağıtık model esnekliğı ön plana çıkarırken, federatif model bu iki yaklaşım arasında dengeli bir yapı sunmaktadır. Bu nedenle özellikle büyük ve karmaşık veri ekosistemlerinde federatif veri yönetiřimi modeli giderek daha fazla tercih edilmektedir.

Tablo 3. Veri yönetiřimi modellerinin karřılařtırılması (Lifebit, 2025).

Boyut	Merkezi Yönetiřim	Merkezi Olmayan (Dağıtık) Yönetiřim	Federe Yönetiřim
Karar Verme	Kararlar merkezi ekip tarafından alınır.	Her birim bağımsız karar alır.	Merkezi konsey standartları belirler, birimler uygulamadan sorumludur.
Ölçeklenebilirlik	Kurum büyüdükçe yönetim zorlaşabilir.	Küçük ekiplerde hızlı, büyük ölçekte koordinasyon zayıf.	Yeni alanlar eklendikçe kolay ölçeklenir.
Çeviklik	Düşük, merkezi onay süreçleri gerektirir.	Yüksek, ekipler bağımsız hareket eder.	Orta-yüksek, merkezi çerçeve içinde yerel esneklik vardır.
Tutarlılık	Yüksek, standartlar merkezi olarak uygulanır.	Düşük, ekipler farklı standartlar kullanabilir.	Yüksek, ortak standartlar esnek uygulama ile desteklenir.
Mülkiyet	Veri sorumluluğu merkezi ekiptedir.	Veri sorumluluğu ekiplerdedir.	Sorumluluk merkez ve alan ekipleri arasında paylaşılır.
Temel Zorluk	Bürokrasi ve karar süreçlerinde yavaşlık.	Veri siloları ve standart farklılıkları.	Koordinasyon ve yönetim dengesi.
Maliyet Yapısı	Merkezi yönetim maliyetleri yüksektir.	Merkezi maliyet düşük, ekip bazlı maliyetler artabilir.	Paylaşılan altyapı sayesinde dengeli maliyet yapısı.
İnovasyon Hızı	Düşük, merkezi onay süreçleri inovasyonu yavaşlatır.	Yüksek, ekipler bağımsız inovasyon yapabilir.	Orta-yüksek, yönetim çerçevesi içinde inovasyon desteklenir.
Risk Yönetimi	Düşük risk, güçlü merkezi kontrol vardır.	Yüksek risk, kontrol ve standartlar değişken olabilir.	Orta risk, merkezi denetim ve yerel sorumluluk birlikte yürütülür.

2.4.1. Merkezi Veri Yönetiřimi Modeli

Merkezi veri yönetiřimi modelinde veri yönetiřimine iliřkin karar alma süreçleri ve operasyonel faaliyetler tek bir merkezi yapı veya birim tarafından yürütölmektedir. Modelde genellikle veri yönetiřimi lideri olarak görev yapan bir kiři veya merkezi bir ekip programın genel yönlendirilmesinden sorumludur. Söz konusu lider veya ekip, veri yönetiřimi stratejisinin belirlenmesi, veri standartlarının oluřturulması ve veri yönetiřimi süreçlerinin koordinasyonundan sorumlu olmaktadır. Bazı kurumlarda bu merkezi yapı aynı zamanda ana verilerin yönetimi ve veri kullanıcılarına dağıtımı gibi görevleri de

üstlenmektedir (Acceldata, 2025; Alation, 2025; Altexsoft, 2023; Claravine, t.y.; Farmer, 2024; Lifebit, 2025).

Merkezi veri yönetiřimi modelinin önemli avantajlarından biri, veri yönetiřimi süreçlerinde güçlü bir koordinasyon ve kontrol mekanizmasının saęlanmasıdır. Verilerin tek bir merkezden yönetilmesi, kurum genelinde veri standartlarının tutarlı biçimde uygulanmasına olanak tanımakta ve veri kalitesinin korunmasına katkı sağlamaktadır. Ayrıca merkezi yönetim sayesinde veri güvenlięi ve veri erişimi daha etkin biçimde izlenebilmektedir. Veri kullanımına ilişkin riskler daha kolay kontrol altına alınabilmektedir. Bunun yanı sıra veri yönetiřimi süreçlerinin merkezileřtirilmesi, kaynak kullanımını optimize ederek maliyetlerin azaltılmasına ve operasyonel süreçlerin sadeleřtirilmesine yardımcı olabilmektedir (Claravine, t.y.; Lifebit, 2025).

Bununla birlikte merkezi veri yönetiřimi modeli bazı sınırlılıklara da sahiptir. Yukarıdan ařaęıya işleyen karar alma mekanizması zaman zaman bürokratik süreçlerin artmasına neden olabilmekte ve organizasyonun farklı birimlerinin ihtiyaçlarına yeterince hızlı yanıt veremeyebilmektedir. Özellikle büyük ve karmařık organizasyonlarda merkezi yapı, veri yönetiřimi süreçlerinde darboęazlara yol açabilmekte ve operasyonel esneklięi sınırlayabilmektedir (Claravine, t.y.; Lifebit, 2025). Bazı sorunlar arasında özellikle řu farklı veri sistemleri ile entegrasyon zorlukları, veri silolarının oluşması, ölçeklenebilirlik sorunları, organizasyon içindeki deęiřime karřı direnç noktalar öne çıkmaktadır (Burchardi vd., 2024).

2.4.2. Daęınık (Merkezi Olmayan) Veri Yönetiřimi Modeli

Merkezi olmayan veri yönetiřimi modelinde stratejik kararlar genellikle yönetim komitesi tarafından belirlenmektedir. Veri üretimi ve veri yönetiřimi faaliyetleri organizasyonun farklı fonksiyonel birimleri tarafından yürütölmektedir. Bu modelde kurumun farklı bölümleri kendi veri kümelerini oluşturmakta, yönetmekte ve veri kullanıcılarına daęıtmaktadır. Böylece veri yönetiřimi sorumluluęu organizasyon genelinde daęıtılmış bir yapıya kavuşmaktadır (Acceldata, 2025; Alation, 2025; Altexsoft, 2023; Claravine, t.y.; Farmer, 2024; Lifebit, 2025).

Bu modelin en önemli avantajlarından biri, organizasyonun farklı iş birimlerinin ihtiyaçlarının daha iyi temsil edilebilmesidir. Verilerin doğrudan bu verileri kullanan birimler tarafından oluşturulması ve yönetilmesi, veri üretim süreçlerinin iş süreçleriyle daha uyumlu hale gelmesini sağlamaktadır. Ayrıca merkezi olmayan model, değişen iş gereksinimlerine daha hızlı uyum sağlayabilmesi nedeniyle organizasyonel çevikliği artırmaktadır. Veri yönetişimi sorumluluğunun farklı birimler arasında paylaşılması aynı zamanda veri yönetişimi uygulamalarının kurum genelinde daha geniş bir katılım ile yürütülmesine olanak tanımaktadır (Claravine, t.y.; Lifebit, 2025).

Bununla birlikte merkezi olmayan veri yönetişimi modeli bazı riskler de barındırmaktadır. Veri yönetişiminin farklı birimler arasında dağılması, veri standartlarının tutarsız biçimde uygulanmasına ve veri tekrarlarının ortaya çıkmasına neden olabilmektedir. Bu durum özellikle ana verilerin farklı versiyonlarının oluşmasına yol açarak raporlama süreçlerini, kurumsal analizleri ve karar alma mekanizmalarını olumsuz etkileyebilmektedir (Claravine, t.y.; Lifebit, 2025).

2.4.3. Federatif (Hibrit) Veri Yönetişimi Modeli

Hibrit veya federatif veri yönetişimi modeli, merkezi ve merkezi olmayan yaklaşımların özelliklerini bir araya getiren bir yapı sunmaktadır. Bu modelde kurumsal düzeyde merkezi bir veri yönetişimi yapısı bulunmakta ve bu yapı veri yönetişimine ilişkin genel çerçeveyi, standartları, teknolojileri ve en iyi uygulamaları belirlemektedir. Ancak veri yönetişiminin operasyonel uygulamaları organizasyonun farklı birimlerinde yer alan veri sahipleri ve veri yöneticileri tarafından yürütülmektedir (Acceldata, 2025; Alation, 2025; Altexsoft, 2023; Claravine, t.y.; Farmer, 2024; Lifebit, 2025).

Hibrit veri yönetişimi modelinin en önemli avantajlarından biri, organizasyon içindeki ekiplerin kendi veri varlıklarını bağımsız biçimde yönetebilmesine olanak tanımasıdır. Bu durum veri alanı¹⁵ (data domain) kavramı ile sağlanmaktadır. Veri yönetişimi süreçlerinde daha hızlı karar alınmasını ve sorunların ortaya çıktıkları yerde çözülmesini sağlamaktadır. Ayrıca ekiplerin veri üzerinde deneyler yapabilmesi ve yeni veri

¹⁵ Veri alanları organizasyon içinde belirli iş süreçleri veya iş fonksiyonlarına göre yapılandırılmış veri gruplarını ifade etmektedir.

uygulamaları geliştirebilmesi organizasyonel yenilik kapasitesini ve çevikliği artırmaktadır (Burchardi vd., 2024; Claravine, t.y.; Lifebit, 2025).

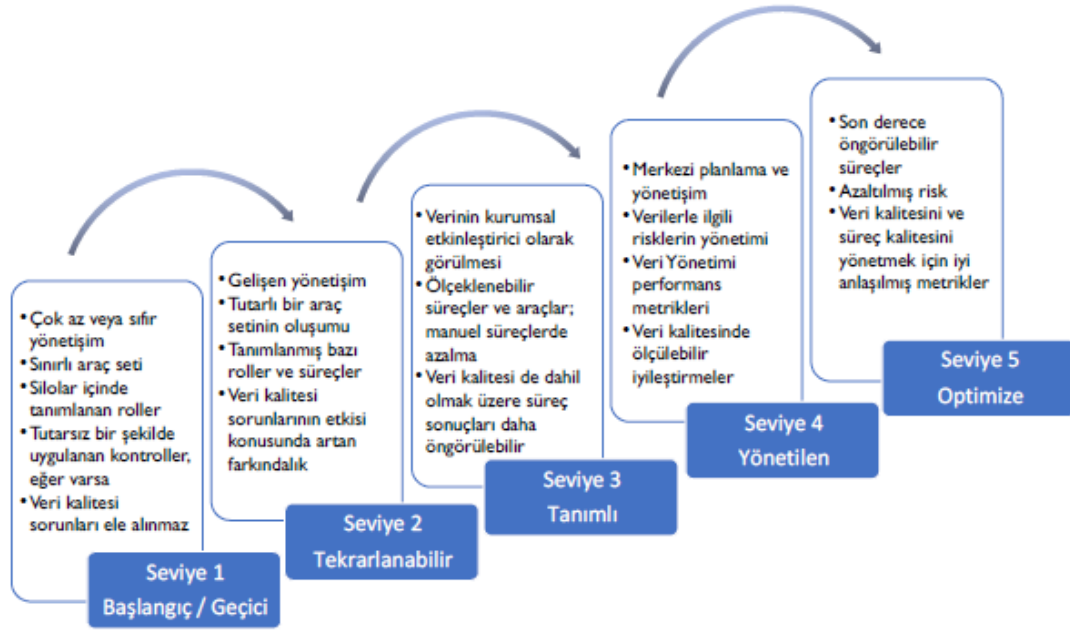
Bununla birlikte hibrit modelin başarılı biçimde uygulanabilmesi için organizasyon içerisinde güçlü veri yönetişimi uzmanlığına ihtiyaç duyulmaktadır. Ayrıca farklı birimler arasında veri tutarlılığının korunması ve koordinasyonun sağlanması için etkili yönetim mekanizmalarının oluşturulması gerekmektedir (Claravine, t.y.; Lifebit, 2025). Kurumlar hem veri tutarlılığını koruyabilmekte hem de farklı iş birimlerinin ihtiyaçlarına uygun esnek veri yönetişimi uygulamaları geliştirebilmektedir. Federatif veri yönetişiminin kurumlara veri sahipliğinin açık biçimde tanımlanması, veri kalitesi ve veri erişilebilirliğinin artırılması, iş birimleri arasında veri paylaşımının kolaylaştırılması, veri temelli karar alma süreçlerinin güçlendirilmesi avantajları sağladığı belirtilmektedir (Burchardi vd., 2024).

2.4.4. Veri Yönetişimi Olgunluk Modelleri

Kuruluşların veri varlıklarını etkin biçimde yönetebilmesi, teknik altyapıların geliştirilmesiyle veri yönetişimi süreçlerinin kurumsal düzeyde olgunlaşmasıyla mümkündür. Dijital dönüşüm süreçlerinin hız kazanmasıyla birlikte veri stratejik karar alma, hizmet geliştirme, risk yönetimi ve kurumsal performans açısından kritik bir unsur haline gelmiştir. Bu durum, kuruluşların veri yönetişimi kapasitelerini değerlendirebilecek sistematik modellerin geliştirilmesine neden olmuştur. Yazılım mühendisliği alanında geliştirilen Yetenek Olgunluk Modeli (Capability Maturity Model, CMM/CMMI) ve ISO/IEC 15504/33000 standart ailesinin etkisiyle, veri yönetimi ve veri yönetişimi alanında da çeşitli olgunluk modelleri ortaya çıkmıştır (Caballero vd., 2023). Bu modeller, kurumların veri yönetişimi süreçlerini hangi seviyede gerçekleştirdiğini belirlemeyi, eksiklikleri tespit etmeyi ve sürekli iyileştirme süreçlerine rehberlik etmeyi amaçlamaktadır.

Literatürde veri yönetişimi ve veri yönetimi alanında geliştirilen en önemli modellerden biri DAMA tarafından önerilen olgunluk modelidir. DAMA modeli hiçbir yetenek yok, başlangıç, tekrarlanabilir, tanımlanmış, yönetilen ve optimize olmak üzere altı seviyeden oluşmaktadır. Modelin ilk seviyelerinde veri yönetişimi süreçleri çoğunlukla bireysel uzmanlara bağlı ve düzensiz bir yapı gösterirken üst seviyelerde süreçlerin

kurumsallaştığı, performans ölçütlerinin kullanıldığı ve veri yönetişiminin sürekli iyileştirme anlayışıyla optimize edildiği görülmektedir. Özellikle son seviyede veri yönetişimi süreçlerinin yüksek derecede otomatikleştiği ve verilerin tüm organizasyon süreçlerinde görünür hale geldiği vurgulanmaktadır (DAMA, 2017).



Şekil 5. DAMA veri yönetimi olgunluk modeli (DAMA, 2017, s. 514)

IBM Veri Yönetişimi Olgunluk Modeli ise veri yönetişimi yetkinliklerini daha kapsamlı ve çok boyutlu biçimde ele almaktadır. Model sonuçlar, destekleyici unsurlar, temel disiplinler ve destekleyici disiplinler olmak üzere dört ana grup altında on bir olgunluk kategorisi tanımlamaktadır. Veri uyumluluğu ve risk yönetimi, veri kalitesi yönetimi, bilgi yaşam döngüsü yönetimi, veri güvenliği ve gizliliği, veri mimarisi, üst veri yönetimi ve denetim raporlama gibi alanlar modelin temel bileşenleri arasında yer almaktadır (IBM, 2007).

Gartner tarafından geliştirilen Kurumsal Bilgi Yönetimi (Enterprise Information Management IM) modeli ise veri yönetişimini uzun vadeli ve kurumsal dönüşüm odaklı bir süreç olarak ele almaktadır. Model vizyon, strateji, ölçütler, yönetişim, insanlar, süreçler ve altyapı olmak üzere yedi temel boyuttan oluşmaktadır. Beş seviyeli yapı içerisinde kuruluşların bilgi yönetimi kapasitelerinin zaman içinde geliştiği kabul edilmektedir. İlk seviyelerde kuruluşlar veriyle ilgili sorunlara daha reaktif yaklaşırken

üst seviyelerde veri yönetiřimi süreçlerinin stratejik, koordineli ve optimize edilmiř hale geldiđi görölmektedir. Özellikle modelin insan, yönetiřim ve strateji boyutlarını vurgulaması veri kültürü ve organizasyonel dönüşüm açısından önemlidir (Laney, 2017).

EDM Council tarafından geliştirilen DCAM (Data Management Capability Assessment Model), veri yönetimi yeteneklerini ölçmeye yönelik kapsamlı modellerden biridir. Veri yönetiřim stratejisi, veri kontrol ortamı, veri kalitesi, veri mimarisi, teknoloji mimarisi ve veri yönetiřimi programı gibi alanlarda toplam 38 yetenek ve 136 alt yetenek tanımlamaktadır. DCAM modeli özellikle sürdürülebilir veri yönetimi programlarının oluşturulmasına odaklanmakta ve veri yönetiřiminin operasyonel süreçlerle bütünleřik biçimde deđerlendirilmesini sağlamaktadır (EDM Association, 2025).

Stanford Veri Yönetiřimi Olgunluk Modeli, 2011 yılında Stanford Üniversitesi Veri Yönetiřimi Ofisi tarafından geliştirilmiřtir. IBM ve CMM gibi mevcut olgunluk modellerinden uyarlanmıřtır. Model, veri yönetiřimi programlarının etkinliđini deđerlendirmek amacıyla hem temel yönetiřim yetkinliklerini hem de proje süreçlerini ölçmeye odaklanmaktadır. Model iki ana yapıdan oluşmaktadır. İlk yapı olan temel bileřenler farkındalık resmileřtirme (formalization) ve üst veri yönetimini kapsamaktadır. İkinci yapı ise proje odaklı bileřenlerden oluşmakta olup veri sorumluluđu (stewardship), veri kalitesi ve ana veri yönetimi alanlarını deđerlendirmektedir. Bu bileřenler ayrıca insanlar, politikalar ve yetenekler/teknolojik kapasite boyutları altında incelenmektedir. Model, kurumların veri yönetiřimi olgunluk seviyelerini belirlemek için deđerlendirme soruları ve puanlama tabloları kullanmaktadır. Özellikle veri yönetiřimi uygulamalarının düzenli olarak ölçölmesini ve yıllık olarak yeniden deđerlendirilmesini önermektedir. Stanford modeli, yükseköğretim kurumlarının ihtiyaçlarına göre geliştirilmiř olması nedeniyle üniversite temelli veri yönetiřimi çalışmalarında önemli referans modellerden biri olarak deđerlendirilmektedir (Firican, 2020).

Oracle Veri Yönetiřimi Olgunluk Modeli, veri yönetiřiminin aşamalı ve sürekli gelişen bir süreç olduđunu vurgulamaktadır. Model, kurumların veri yönetiřimi olgunluđunu ok (None), Bařlangıç (Initial), Yönetilen (Managed), Standartlařtırılmıř (Standardized), Geliřmiř (Advanced) ve Optimize Edilmiř (Optimized) olmak üzere altı seviyede deđerlendirmektedir. İlk seviyelerde veri yönetiřimi süreçleri düzensiz ve uygulama odaklı ilerlerken üst seviyelerde veri sahipliđi, veri standartları, veri kalitesi yönetimi ve

kurumsal yönetim mekanizmaları kurumsallaşmaktadır. En yüksek seviyede ise veri yönetimi, organizasyonun temel iş süreçlerinden biri haline gelmekte ve karar alma süreçleri ölçülebilir veri analizleriyle desteklenmektedir. Oracle modeli ayrıca olgunluk gelişimini Keşfetme (Explore), Genişleme (Expand) ve Dönüşüm (Transform) olmak üzere üç aşamalı bir dönüşüm süreciyle açıklamaktadır. Veri yönetiminin kademeli, sürekli iyileştirmeye dayalı ve kurumsal stratejiyle uyumlu biçimde uygulanması gerektiğini savunmaktadır (ORACLE, 2011).

Veri yönetimi olgunluk modelleri, kurumların veri yönetimi kapasitelerini değerlendirmelerine ve geliştirmelerine yardımcı olsa da çeşitli zorluklar içermektedir. Bu modellerin uygulanması çoğu zaman karmaşık, zaman alıcı ve yüksek kaynak gerektiren süreçlerdir. Ayrıca değerlendirmelerin büyük ölçüde öz değerlendirmeye dayanması öznellik sorununa yol açabilmektedir. Veri yönetimi teknolojilerinin ve ihtiyaçlarının sürekli değişmesi nedeniyle modellerin güncellenmesi gerekmektedir. Kurumsal kültür ise değişim süreçlerine direnç gösterebilmektedir. Bunun yanında yeni veri yönetimi uygulamalarının mevcut süreç ve sistemlerle entegre edilmesi zor olabilmektedir. Bu nedenle veri yönetimi olgunluk modellerinin başarılı biçimde uygulanabilmesi için güçlü değişim yönetimi, uzman desteği ve sürdürülebilir kaynak planlaması gerekmektedir (Smith, 2026).

3. BÖLÜM

VERİ YÖNETİŞİMİ STANDARTLARI, ÇERÇEVELERİ, YASAL DÜZENLEMELERİ VE POLİTİKALARI

Veri yönetişiminin etkili biçimde uygulanabilmesi için kurumların bir çerçeve oluşturması gerekmektedir. Veri yönetişimi kavramının geniş kapsamı nedeniyle henüz üzerinde uzlaşılan tekil bir tanımın bulunmadığı ve bu durumun veri yönetişimi çerçevelerinin oluşturulmasında farklılıklara yol açtığı anlaşılmıştır. Veri yönetişimi ile ilgili yerel, ulusal ve uluslararası düzeylerde farklı amaç, yaklaşım hatta kapsamların benimsenmesi, bu çeşitliliği daha da belirginleştirmektedir (Marcucci vd., 2023).

Güçlü bir veri yönetişimi çerçevesi öncelikle kurumun veri yönetimine ilişkin uzun vadeli hedeflerini belirleyen bir vizyon ve strateji içermelidir. Bu strateji, veri güvenliği, düzenleyici uyumluluk ve veriden değer üretme gibi amaçları kurumsal hedeflerle ilişkilendirilmektedir. Çerçevenin bir diğer önemli unsuru ise yol gösterici ilkelerdir. Şeffaflık, veri sahipliği, iş birliği, veri okuryazarlığı ve gizlilik gibi ilkeler veriyle ilgili karar alma süreçlerini yönlendirmekte ve olası politika çatışmalarının çözümüne katkı sağlamaktadır (Smith, 2025).

Bunun yanında veri yönetişimi yapısı içerisinde veri sahipliği ve veri sorumluluğu (data stewardship) gibi roller tanımlanarak veri kalitesinin korunması ve düzenleyici gerekliliklere uyum sağlanması hedeflenmektedir. Veri kalitesi yönetimi kapsamında doğrulama, temizleme ve veri profillemeye gibi süreçler uygulanırken veri yönetişimi süreçleri verinin oluşturulması, depolanması, erişimi ve paylaşımı gibi yaşam döngüsü aşamalarını düzenlemektedir. Bu süreçlerin etkin biçimde yürütülmesi için veri katalogları, üst veri depoları ve güvenlik çözümleri gibi teknolojik altyapılar destekleyici rol oynamaktadır (Smith, 2025).

Veri yönetişimi kapsamında oluşturulan standartlar, politikalar ve süreçler, verilerin yaşam döngüsü boyunca kalitesinin korunması için çerçeve sağlamaktadır. Veri yönetişimi çerçeveleri, kuruluşun veri kalitesini nasıl yöneteceğini (ne yapılacak, kim yapacak ve nasıl yapılacak) göstermektedir (Askham, 2014).

Kurum içinde veriyle ilgili görev ve yetkilerin açık şekilde belirlenmesi, roller ve sorumlulukların netleşmesine katkıda bulunmaktadır. Bununla birlikte veri yönetiřimi, GDPR'ye uyumu saęlamak amacıyla risk ve uyumluluk yönetimi süreçlerini de kapsamaktadır. Son olarak veri yönetiřimi faaliyetlerinin etkinlięini deęerlendirebilmek için veri kalitesi ve bilgi güvenlięi gibi alanlarda ölçütler ve performans göstergeleri belirlenerek kurumsal performansın izlenmesi mümkün hale gelmektedir (Smith, 2025).

3.1. ULUSLARARASI STANDARTLAR

Bu kategori ve evrensel olarak kabul edilen standartların, veri yönetiřimi açısından iliřkisini ve incelemesini içermektedir.

3.1.1. ISO/IEC 38505 Serisi: Veri Yönetiřimi Standartları

ISO/IEC 38505 serisi, veri yönetiřimini kurumsal yönetiřimin bir alt alanı olarak ele alan ve verinin stratejik, güvenilir, hesap verebilir ve sürdürülebilir biçimde yönetilmesini amaçlayan uluslararası standartlar bütünüdür. Seri, özellikle veri kullanımının artması, büyük veri, bulut biliřim, nesnelerin interneti (IoT) ve yapay zeka uygulamalarının yaygınlařmasıyla birlikte kurumların veri üzerindeki yönetsel sorumluluklarını tanımlama ihtiyacından doğmuřtur (ISO, 2017; ISO, 2018; ISO, 2021).

ISO/IEC 38505-1 standardı, veri yönetiřiminin temel ilkelerini, kavramsal modelini ve yönetsel çerçevesini ortaya koymaktadır. Standartta veri yönetiřimi, BT yönetiřiminin bir alt alanı olarak organizasyonel yönetiřim yapısı içinde tanımlanmaktadır. Buna göre veri yönetiřimi verinin etkili, verimli ve kabul edilebilir biçimde kullanılmasını saęlamak amacıyla yönetsel organların veri kullanımını deęerlendirmesi, yönlendirmesi ve izlemesi süreçlerini kapsamaktadır (ISO, 2017).

ISO/IEC 38505-1'e göre iyi veri yönetiřimi kurumların veri odaklı inovasyon gerçekleřtirebilmesine, veri varlıklarından deęer üretmesine, veriyle iliřkili riskleri azaltmasına ve paydař güvenlięini artırmasına katkı saęlamaktadır. Standartta özellikle veri ihlalleri, gizlilik kayıpları, mevzuata uyumsuzluk, veri temelli karar hataları ve stratejik veri kullanımındaki yetersizliklerin kurumsal risk oluřturduęu vurgulanmaktadır. Bu bağlamda yönetiřim organlarının veri güvenlięi, gizlilik, fikri mülkiyet, veri paylařımı ve etik kullanım gibi konularda hesap verebilir olduęu belirtilmektedir (ISO, 2017).

Standart, veri yönetişimi için sorumluluk (responsibility), strateji (strategy), edinim (acquisition), performans (performance), uygunluk (conformance) ve insan davranışı (human behaviour) olmak üzere altı temel ilke tanımlamaktadır. Bu ilkeler, ISO/IEC 38500¹⁶ BT yönetişimi standardının veri alanına uyarlanmış biçimidir (ISO, 2017).

Sorumluluk ilkesi, veriyle ilişkili görev, yetki ve hesap verebilirliklerin organizasyon içerisinde açık biçimde tanımlanmasıdır. Standartta göre yönetim organı, kurum içerisindeki tüm paydaşların veri kullanımına ilişkin rollerini anlamasını ve bu sorumlulukları kabul etmesini sağlamalıdır. Veri sorumluluğu bilgi işlem ile birlikte veri kullanan, üreten, paylaşan veya işleyen tüm birimler bu sorumluluğun parçasıdır (ISO, 2017).

Strateji ilkesi, veri kullanımının kurumun genel stratejik hedefleriyle uyumlu biçimde planlanmasıdır. Veri stratejisi mevcut ve gelecekteki veri ihtiyaçlarını, teknolojik gelişmeleri, kurumsal hedefleri ve veri odaklı fırsatları kapsamalıdır. Bu ilke doğrultusunda veri, kurumsal rekabet avantajı sağlayan stratejik bir varlık olarak değerlendirilmektedir. Yönetişim organı, veri kullanımının uzun vadeli organizasyonel amaçlara hizmet etmesini sağlamaktan sorumludur (ISO, 2017).

Edinim ilkesi, veriyle ilişkili teknolojilerin, sistemlerin, veri kaynaklarının ve yatırımların kurumsal gereksinimler doğrultusunda değerlendirilmesidir. Standart, veri toplama ve veri teknolojilerine yönelik yatırımların sağlayacağı değer, oluşturacağı risk ve sürdürülebilirlik açısından da değerlendirilmesi gerektiğini vurgulamaktadır. Veri edinim süreçlerinde kalite, güvenlik, ölçeklenebilirlik ve yasal uygunluk gibi unsurlar dikkate alınmalıdır. Bu ilke, özellikle büyük veri, bulut bilişim ve yapay zeka teknolojilerinin kullanımında önem kazanmaktadır (ISO, 2017).

Performans ilkesi, veri kullanımının kurumsal hedeflere katkı sağlayacak şekilde etkin ve verimli olmasını ifade etmektedir. Veri yönetişimi mekanizmaları doğru, güvenilir, zamanında ve kaliteli veri üretimini desteklemelidir. Ayrıca veri temelli süreçlerin organizasyonel performansa katkısı ölçülmeli ve izlenmelidir. Standart, veri kalitesi, erişilebilirlik, zamanlılık ve karar desteği üretme kapasitesini performansın temel

¹⁶ Bkz. <https://www.iso.org/standard/81684.html>

göstergeleri arasında değerlendirmektedir. Böylece veri kullanımının kurumsal değer üretme kapasitesi sürekli gözlemlenebilmektedir (ISO, 2017).

Uygunluk ilkesi, veri kullanımının yasal düzenlemeler, etik ilkeler, standartlar ve kurumsal politikalarla uyumlu biçimde yürütülmesidir. Bu ilke kapsamında kurumların veri gizliliği, bilgi güvenliği, fikri mülkiyet, kişisel verilerin korunması ve düzenleyici yükümlülükler gibi alanlarda gerekli kontrolleri sağlaması beklenmektedir. Veri yönetişimi yapısı mevzuata uyumu izleyen, denetleyen ve raporlayan mekanizmalar içermelidir. Özellikle kişisel veri işleme faaliyetlerinde hesap verebilirlik ve şeffaflık bu ilkenin temel unsurlarıdır (ISO, 2017).

İnsan davranışı ilkesi, veri kullanımında insan faktörünün, organizasyon kültürünün ve etik yaklaşımın dikkate alınmasıdır. Standart, veri yönetişiminin çalışan davranışları, karar verme kültürü ve veri farkındalığının da yönetim başarısında belirleyici olduğunu vurgulamaktadır. Veri kullanımında etik ilkeler, önyargıların önlenmesi, ayrımcılığın engellenmesi, güven kültürünün oluşturulması ve kullanıcı davranışlarının yönlendirilmesi önemli unsurlar arasında yer almaktadır. Özellikle otomatik karar verme sistemleri ve yapay zeka uygulamalarında insan gözetimi ve etik değerlendirme kritik görülmektedir (ISO, 2017).

ISO/IEC 38505-1 standardının en önemli katkılarından biri veri hesap verebilirlik haritasını (data accountability map) ortaya koymasıdır. Bu modelde veri yaşam döngüsü toplama (collect), depolama (store), raporlama (report), karar verme (decide), dağıtım (distribute) ve imha etme (dispose) olmak üzere altı temel yönetim alanı üzerinden ele alınmaktadır. Standart, bu alanların her biri için yönetim organlarının politika geliştirmesi, riskleri değerlendirmesi ve kontrol mekanizmaları oluşturması gerektiğini ifade etmektedir (ISO, 2017).

ISO/IEC TR 38505-2 ise ISO/IEC 38505-1’de tanımlanan yönetim ilkelerinin veri yönetişimi süreçlerine nasıl uygulanacağını açıklayan teknik rapor niteliğindedir. Bu rapor, yönetim organları ile yönetim ekipleri arasındaki ilişkiyi açıklamaktadır. Veri stratejisinin politika, süreç ve kontrol mekanizmalarına nasıl dönüştürüleceğini göstermektedir (ISO, 2018).

Standartta göre yönetim organı veri stratejisinden sorumludur. Yönetim ise bu stratejiyi uygulayan süreçleri işletmektedir. Bu kapsamda veri yönetiřimi, strateji, politika, süreç, kontrol zinciri içerisinde ele alınmaktadır. ISO/IEC TR 38505-2, bu iliřkiyi kademeli aktarım mekanizması (cascade mechanism) olarak adlandırmakta ve veri stratejisinin organizasyonel süreçlere aktarılmasında çift yönlü geri bildirim mekanizmasının önemini vurgulamaktadır (ISO, 2018).

Standartta Deęerlendirme, Yönlendirme, İzleme (Evaluate, Direct, Monitor, EDM) modeli veri yönetiřimini ayrıntılı biçimde açıklamaktadır. Buna göre yönetim organı öncelikle veri kullanımına iliřkin fırsatları, riskleri ve teknolojik geliřmeleri deęerlendirmekte (Deęerlendirme), ardından veri stratejisi ve politikalarını belirleyerek yönlendirme yapmakta (Yönlendirme), son aşamada ise performans, uyumluluk ve risk göstergelerini izlemektedir (İzleme). Bu yaklaşım, veri yönetiřimini sürekli izlenen ve iyileřtirilen dinamik bir kurumsal yapı haline getirmektedir (ISO, 2018).

ISO/IEC TR 38505-2’de veri yönetiřimi politikalarının geliřtirilmesi için sistematik bir süreç de önerilmektedir. Bu süreç mevcut ihtiyaçların belirlenmesi, paydařların tanımlanması, politika tasarımı, uygulama, eęitim, izleme ve sürekli iyileřtirme aşamalarından oluřmaktadır (ISO, 2018).

ISO/IEC 38505 serisinin temel yaklaşımı verinin kurumsal bir varlık olarak deęerlendirilmesi ve bu varlığın deęer, risk ve kısıtlar dengesi içerisinde yönetilmesidir. Risk boyutunda veri ihlalleri, kötüye kullanım, yanlış karar üretimi ve rekabet kaybı gibi unsurlar deęerlendirilirken kısıtlar boyutunda mevzuat, etik ilkeler, toplumsal beklentiler ve kurumsal politikalar dikkate alınmaktadır (ISO, 2017).

ISO/IEC TS 38505-3 standardı, kuruluşlarda veri sınıflandırmasının sistematik, tutarlı ve yönetim odaklı biçimde yürütülmesine yönelik temel rehber ilkeleri ortaya koymaktadır. Standart, öncelikle kurumun genel veri yönetiřimi politikalarıyla uyumlu yapılandırılmış bir veri sınıflandırma sistemi geliřtirilmesini önermektedir. Bu kapsamda verilerin kurumsal deęerleri, hassasiyet düzeyleri ve kullanım amaçları doęrultusunda kategorize edilmesi gerektięi vurgulanmaktadır. Özellikle verilerin yetkisiz eriřim, ifřa veya kötüye kullanım durumunda oluřturabileceęi potansiyel zarar düzeyi dikkate alınarak veri duyarlılıęı temelinde sınıflandırılması önerilmektedir (ISO, 2021).

Ayrıca ISO/IEC 38505 serisinin uygulama araç setleri veri yönetiřimi tüzükleri, veri sınıflandırma politikaları, veri kalite çerçeveleri, erişim kontrol mekanizmaları, veri etik ilkeleri, risk kayıtları, KPI/KRI gösterge panelleri ve olgunluk değerlendirme araçları gibi uygulamaya dönük bileşenler içermektedir. Bu durum hem teorik bir çerçeve sunduğu hem de kurumlara operasyonel düzeyde uygulanabilir veri yönetiřimi yapıları geliştirme imkanı sağladığını göstermektedir (ISO, 2021).

3.1.2. ISO/IEC 25642:2025 Veri İş Birliğı Çerçevesi

ISO/IEC 25642:2025 standardı, veri yönetiřimi kapsamında veri paylaşımı, veri entegrasyonu ve veri üzerinde iş birliğinin güvenli, kontrollü ve sürdürülebilir biçimde yürütülmesine yönelik bir veri iş birliğı çerçevesi (data collaboration framework) sunmaktadır. Standart, özellikle dijital dönüşüm süreçlerinde artan veri entegrasyonu karmaşıklığına çözüm üretmek amacıyla geliştirilmiştir. Geleneksel kopya temelli veri entegrasyonu yaklaşımına alternatif olarak erişim temelli veri iş birliğı modelini önermektedir (ISO, 2025c).

Standart, ISO/IEC 38500 BT yönetiřimi standardı ile ISO/IEC 38505-1 veri yönetiřimi standardını tamamlayıcı nitelikte tasarlanmıştır. Temel amacı, kurumların yeni dijital yetenekler geliřtirmesine, veri erişim kontrollerini evrensel biçimde uygulamasına ve uygulamaya özgü veri silolarını azaltmasına rehberlik etmektir. Ayrıca insan-insan, insan-sistem ve sistem-sistem düzeyinde veri iş birliğini destekleyen kontrollü veri yönetim ortamlarının oluşturulmasını hedeflemektedir (ISO, 2025c).

ISO/IEC 25642 standardının temel yaklaşımı, verinin uygulamalardan ayrıştırılmasıdır (decouple data from applications). Standartta göre yeni BT çözümleri geliştirilirken uygulamaya özgü veri tabanları ve veri siloları oluşturulmamalıdır. Bunun yerine birden fazla uygulamanın aynı fiziksel veri üzerinde çalışabildiğı ortak veri mimarileri tercih edilmelidir. Böylece aynı verinin tekrar tekrar kopyalanması engellenmekte, veri tutarsızlıkları azaltılmakta ve veri yönetiřimi kontrollerinin merkezi biçimde uygulanması mümkün hale gelmektedir (ISO, 2025c).

Standartta özellikle sıfır kopyalı veri entegrasyonu (zero-copy data integration) yaklaşımı verinin farklı uygulamalar arasında sürekli kopyalanması yerine erişim yetkileri üzerinden paylaşılmasını ifade etmektedir. Geleneksel veri entegrasyonu yöntemlerinde

veri ambarları, veri gölleri ve uygulama bazlı veri tabanları yeni veri siloları oluşturmaktadır. ISO/IEC 25642 erişim temelli veri iş birliği modeliyle gerçek zamanlı veri paylaşımını desteklemektedir (ISO, 2025c).

Standart, veri paylaşımında üst veri katmanını merkezi bir kontrol mekanizması olarak ele almaktadır. Buna göre erişim kontrolleri üst veri katmanında tanımlanmalıdır. Böylece veri sahipleri veya veri sorumluları kullanıcıların, grupların veya uygulamaların hangi verilere erişebileceğini, hangi işlemleri gerçekleştirebileceğini ve hangi veri alanlarını görüntüleyebileceğini ayrıntılı biçimde belirleyebilmektedir. Standart, mümkün olduğunda hücre düzeyinde erişim kontrolü uygulanmasını önermektedir (ISO, 2025c).

ISO/IEC 25642 aynı zamanda verinin ürün (data as a product) yaklaşımıyla yönetilmesini önermektedir. Bu modele göre veri belirli iş süreçleri etrafında tanımlanan veri alanları (data domain) ve veri ürünleri (data product) içerisinde organize edilmektedir. Veri sahipleri, veri sorumluları ve veri temsilcileri veri üzerinde erişim kurallarını, kalite parametrelerini ve kullanım politikalarını belirlemektedir (ISO, 2025c).

Standartta veri iş birliği çerçevesinin temel ilkeleri ayrıntılı biçimde tanımlanmaktadır. Bunlar arasında uygulama odaklı veri silolarından kaçınılması, ağ bağlantılı veri mimarisinin benimsenmesi, üst veri katmanında evrensel veri korumasının sağlanması, veri sürümleme ve veri soy ağacı (lineage) süreçlerinin otomatikleştirilmesi ve modüler kurumsal mimarilerin geliştirilmesi yer almaktadır (ISO, 2025c).

ISO/IEC 25642 standardına göre geleneksel kopya tabanlı veri entegrasyonu yöntemleri veri siloları, kontrol kaybı, erişim yönetimi zorlukları ve unutulma hakkı (right to be forgotten / right to erasure) gibi düzenleyici gerekliliklerin uygulanmasında önemli sorunlar yaratmaktadır. Bu nedenle veri sahipliği ve veri erişim kontrollerinin merkezi olarak yönetildiği veri iş birliği mimarileri önerilmektedir. Ayrıca veri iş birliği çerçevesinin yapay zeka, açık bankacılık, akıllı şehirler, temiz teknoloji (cleantech) ve hassas sağlık hizmetleri gibi veri yoğun alanlarda güvenli inovasyonu desteklediğini belirtmektedir. Özellikle erişim temelli veri paylaşım modeli sayesinde veri koruma gereksinimleri ile dijital inovasyon arasında daha dengeli bir yapı kurulabilmektedir (ISO, 2025c).

ISO/IEC 25642'nin önemli katkılarından biri de kurumsal birleştirilebilirlik (enterprise composability) yaklaşımıdır. Bu yaklaşım, yeni dijital çözümlerin veri kopyalamaya ihtiyaç duymadan modüler biçimde sisteme eklenebilmesini, güncellenebilmesini veya kaldırılabilmesini ifade etmektedir. Böylece organizasyonlar değişen iş gereksinimlerine daha esnek ve sürdürülebilir biçimde uyum sağlayabilmektedir (ISO, 2025c).

3.1.3. ISO/IEC 11179 Serisi: Üst Veri Kayıtları Standardı

ISO/IEC 11179 serisi, üst veri kayıt sistemleri (Metadata Registry, MDR) için geliştirilen uluslararası standartlar bütünüdür. Standart serisi verinin anlamının, temsil biçiminin ve veri açıklamalarının sistematik biçimde kayıt altına alınmasını amaçlamaktadır. ISO/IEC 11179'un temel yaklaşımı, kurumlar arasında ortak veri anlayışının oluşturulması, veri tekrarlarının azaltılması, veri standartlaştırmasının sağlanması ve veri bileşenlerinin yeniden kullanılabilir hale getirilmesidir. Standart, özellikle veri semantiğinin açık biçimde tanımlanmasına ve verilerin organizasyonlar arasında tutarlı biçimde paylaşılmasına odaklanmaktadır (ISO, 2023b).

ISO/IEC 11179-1 standardı, serinin kavramsal çerçevesini oluşturmaktadır. Bu bölüm, üst veri kavramını veriyi tanımlayan veri olarak ele almakta ve üst veri kayıt sistemlerinin temel işlevlerini açıklamaktadır. Standartta göre bir üst veri kayıt sistemi üst veri öğelerini depolayan, yöneten ve standartlaştıran bir sistemdir. Kayıt işlemi tanımlama (identification), köken/provenans belirleme (provenance) ve kalite izleme (monitoring quality) olmak üzere üç temel amacı yerine getirmektedir (ISO, 2023b).

Standart serisinin temel hedeflerinden biri, organizasyonlar arasında ortak veri anlayışı geliştirilmesini sağlamaktır. ISO/IEC 11179, verilerin zaman, uygulama ve kurumlar arasında yeniden kullanılabilir ve birlikte çalışabilir (interoperable) biçimde tanımlanmasını desteklemektedir. Bu nedenle standart, veri tanımlarının standartlaştırılması, veri bileşenlerinin harmonizasyonu ve veri açıklamalarının tekrar kullanılabilir hale getirilmesi gibi amaçları ön plana çıkarmaktadır (ISO, 2023b).

ISO/IEC 11179 serisi, verinin anlamsal boyutlarıyla da ilgilenmektedir. Standartta veri semantiği, verinin doğru yorumlanabilmesi için temel unsur olarak görülmektedir. Bu kapsamda üst veri kayıt sistemleri veri öğeleri arasındaki ilişkileri, veri tanımlarını, veri

türlerini, temsil biçimlerini ve kavramsal bağlantıları kayıt altına almaktadır. Böylece veri kullanıcıları, aynı veri ögesini farklı sistemlerde tutarlı biçimde yorumlayabilmektedir (ISO, 2023b).

ISO/IEC 11179-1 ayrıca üst veri kayıt sistemlerinin organizasyonel veri yönetişimindeki rolünü açıklamaktadır. Standarda göre üst veri kayıtları bilgi sistemleri tasarımı, veri tabanı yönetimi, veri paylaşımı, veri sözlüğü geliştirme ve veri değişim mesajlarının oluşturulması gibi süreçlerde temel bir referans mekanizması oluşturmaktadır. Böylece veri yönetişimi, veri standardizasyonu ve veri entegrasyonu süreçleri daha sistematik biçimde yürütülebilmektedir (ISO, 2023b).

ISO/IEC TR 11179-2 standardı ise üst veri kayıt sistemlerinde kullanılan üst veri öğelerinin belirli kavramsal yapılara göre sınıflandırılmasını ve organize edilmesini ele almaktadır. Standarda göre sınıflandırma nesnelerin veya kavramların ortak özelliklerine göre gruplandırılması sürecidir. Sınıflandırma şemaları, üst veri kayıt sistemlerinde veri öğelerinin daha kolay bulunmasını, yönetilmesini ve analiz edilmesini sağlamaktadır (ISO, 2019).

ISO/IEC TR 11179-2, üst veri kayıtlarında kullanılabilecek farklı sınıflandırma türlerini ayrıntılı biçimde açıklamaktadır. Bunlar arasında kontrollü sözlükler (controlled vocabulary), kontrolsüz sözlükler (uncontrolled vocabulary), taksonomiler (taxonomy), tezauruslar (thesaurus) ve ontolojiler (ontology) bulunmaktadır. Kontrollü sözlükler, standartlaştırılmış terim listeleri aracılığıyla kavramların tutarlı biçimde kullanılmasını sağlarken taksonomiler kavramları hiyerarşik yapılar içerisinde organize etmektedir. Tezauruslar eş anlamlı ve ilişkili terimler arasında bağlantılar kurarken ontolojiler daha gelişmiş anlamsal ilişkileri ve mantıksal yapıları tanımlamaktadır (ISO, 2019).

Standart, iyi bir sınıflandırma sisteminin sahip olması gereken benzersizlik (uniqueness), tutarlılık (consistency), kapsamlılık (comprehensiveness), süreklilik (continuity), genişletilebilirlik (extensibility) ve birlikte çalışabilirlik (interoperability) ilkelerini açıklamaktadır. Özellikle birlikte çalışabilirlik ilkesi, farklı üst veri sistemleri arasında veri paylaşımını ve semantik uyumu desteklemektedir (ISO, 2019).

ISO/IEC 11179 serisinin önemli katkılarından biri, veri kalitesinin artırılmasına, veri tekrarlarının azaltılmasına ve veri paylaşım süreçlerinin iyileştirilmesine katkı sağlamaktadır. Özellikle büyük ölçekli organizasyonlarda ve farklı sistemlerin entegre çalıştığı yapılarda ISO/IEC 11179 standartları, veri bütünlüğü ve semantik uyumluluk açısından kritik bir referans çerçevesi oluşturmaktadır (ISO, 2023b; ISO, 2019).

3.1.4. ISO/IEC 27001 ve 27701 Standartları: Bilgi Güvenliği ve Gizlilik Bilgi Yönetim Sistemi

ISO/IEC 27001 ve ISO/IEC 27701 standartları, kurumlarda bilgi güvenliği ve kişisel veri gizliliğinin sistematik biçimde yönetilmesine yönelik uluslararası yönetim sistemi standartlarıdır. Bu standartlar, organizasyonların bilgi varlıklarını koruyabilmesi, bilgi güvenliği risklerini yönetebilmesi ve kişisel veri işleme süreçlerini yasal gerekliliklerle uyumlu hale getirebilmesi için yönetim çerçevesi sunmaktadır. ISO/IEC 27001 standardı bilgi güvenliği yönetim sistemini (Information Security Management System, ISMS) tanımlarken, ISO/IEC 27701 standardı ise bu yapıyı genişleterek gizlilik bilgi yönetim sistemini (Privacy Information Management System, PIMS) oluşturmaktadır (ISO, 2022; ISO, 2025b).

ISO/IEC 27001 standardı, bilgi güvenliği yönetim sistemi için gereksinimleri tanımlayan temel standarttır. Kurumların bilgi güvenliği süreçlerini kurması, uygulaması, sürdürmesi ve sürekli iyileştirmesi için sistematik bir yapı ortaya koymaktadır. ISO/IEC 27001'e göre bilgi güvenliği yönetim sistemi organizasyonun ihtiyaçları, hedefleri, riskleri, süreçleri ve organizasyon yapısıyla bütünleşik biçimde tasarlanmalıdır (ISO, 2022).

Standart, bilgi güvenliğini gizlilik üç temel ilkede (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) ele almaktadır. Gizlilik ilkesi, bilginin yetkili kişiler tarafından erişilebilir olmasını, bütünlük ilkesi bilginin doğruluğunun ve değişmezliğinin korunmasını erişilebilirlik ilkesi ise bilginin ihtiyaç duyulduğunda kullanılabilir olmasını ifade etmektedir. ISO/IEC 27001, bu üç temel unsurun risk yönetimi yaklaşımıyla korunmasını hedeflemektedir (ISO, 2022).

ISO/IEC 27001 standardı, organizasyonların bilgi güvenliği risk değerlendirme ve risk işleme süreçlerini sistematik biçimde yürütmesini zorunlu kılmaktadır. Bu kapsamda

kurumların bilgi güvenliği risk kriterlerini belirlemesi, riskleri tanımlaması, risk sahiplerini belirlemesi, risklerin olasılık ve etkilerini değerlendirmesi ve uygun kontrol mekanizmalarını uygulaması beklenmektedir. Ayrıca standart, risk işleme sürecinde uygulanacak kontrollerin seçilmesini ve bu kontrollerin gerekçelendirilmesini içeren Uygulanabilirlik Bildiriminin (Statement of Applicability, SoA) oluşturulmasını zorunlu tutmaktadır (ISO, 2022).

ISO/IEC 27001'in önemli özelliklerinden biri, üst yönetim sorumluluğunu bilgi güvenliği yönetişiminin merkezine yerleştirmesidir. Standart, üst yönetimin bilgi güvenliği politikalarını belirlemesini, gerekli kaynakları sağlamasını, organizasyonel roller ve sorumlulukları tanımlamasını ve bilgi güvenliği süreçlerini kurumsal stratejiyle uyumlu hale getirmesini zorunlu kılmaktadır. ISO/IEC 27001 standardının Ek A bölümünde bilgi güvenliği kontrollerine ilişkin ayrıntılı bir kontrol seti yer almaktadır. Bu kontroller bilgi sınıflandırması, erişim kontrolü, kimlik yönetimi, olay yönetimi, tedarikçi güvenliği, bulut hizmetleri güvenliği, bilgi aktarımı, kayıt yönetimi ve güvenlik olaylarına müdahale gibi alanları kapsamaktadır. Özellikle bilgi sınıflandırması ve erişim kontrolü, veri yönetişimi süreçleri açısından kritik öneme sahiptir (ISO, 2022).

ISO/IEC 27701 standardı ise ISO/IEC 27001 üzerine inşa edilen ve kişisel verilerin korunmasına odaklanan gizlilik bilgi yönetim sistemi standardıdır. Standart, kişisel olarak tanımlanabilir bilgilerin (Personally Identifiable Information, PII) işlenmesine ilişkin gereksinimleri ve rehberleri tanımlamaktadır. ISO/IEC 27701'in temel amacı organizasyonların kişisel veri işleme faaliyetlerini gizlilik ilkeleri doğrultusunda yönetmesini sağlamak, veri koruma yükümlülüklerini yerine getirmek ve veri sahiplerinin haklarını korumaktır (ISO, 2025b).

ISO/IEC 27701 standardı, ISO/IEC 29100¹⁷ gizlilik çerçevesi ile uyumlu biçimde geliştirilmiş olup GDPR ve benzeri veri koruma düzenlemeleriyle ilişkilendirilmektedir. Standart veri sorumluları ve veri işleyenler için ayrı kontrol hedefleri ve uygulama rehberleri sunmaktadır. Bu yapı sayesinde organizasyonlar, kişisel veri işleme

¹⁷ Bkz. <https://www.iso.org/standard/85938.html>

faaliyetlerindeki rollerine göre farklı yükümlülükleri sistematik biçimde yönetebilmektedir (ISO, 2025b).

ISO/IEC 27701'de kişisel veri işleme süreçlerinin hukuka uygunluk temelinde yürütülmesi önemli bir gereklilik olarak ele alınmaktadır. Standart veri işleme amaçlarının açık biçimde tanımlanmasını, veri işleme için uygun hukuki dayanakların belirlenmesini ve gerektiğinde açık rıza mekanizmalarının oluşturulmasını zorunlu kılmaktadır. Ayrıca kişisel veri işleme faaliyetlerine ilişkin kayıtların tutulması, veri işleme amaçlarının sınırlandırılması ve veri minimizasyonu ilkelerinin uygulanması önerilmektedir (ISO, 2025b).

Standartta tasarımda gizlilik¹⁸ (privacy by design) ve varsayılan gizlilik¹⁹ (privacy by default) ilkeleri de önemli yer tutmaktadır. Bu yaklaşım, kişisel veri koruma mekanizmalarının sistem tasarımının başlangıç aşamasından itibaren süreçlere entegre edilmesini ifade etmektedir (ISO, 2025b).

ISO/IEC veri sahiplerinin bilgilendirilmesi, erişim taleplerinin karşılanması, verilerin düzeltilmesi veya silinmesi, rızanın geri çekilmesi ve veri işleme faaliyetlerine itiraz edilmesi gibi hakların organizasyonel süreçlerle desteklenmesini öngörmektedir (ISO, 2025b).

ISO/IEC 27001 ve ISO/IEC 27701 standartları birlikte değerlendirildiğinde, bilgi güvenliği ve gizlilik yönetiminin birbirini tamamlayan iki temel alan olduğu görülmektedir. ISO/IEC 27001 daha çok bilgi güvenliği risklerinin yönetimine odaklanırken ISO/IEC 27701 kişisel veri gizliliği ve veri koruma yükümlülüklerini bu yapıya entegre etmektedir. Böylece organizasyonlar hem bilgi güvenliği hem de veri gizliliği açısından yönetim modeli oluşturabilmektedir. Özellikle veri yoğun organizasyonlarda bu standartlar veri yönetimi, risk yönetimi, yasal uyumluluk ve dijital

¹⁸ Tasarımda gizlilik, kişisel veri koruma önlemlerinin sistem veya süreç tasarımının en başından itibaren entegre edilmesini ifade etmektedir. Bu yaklaşımda gizlilik koruması sistem mimarisinin doğal bir bileşeni olarak ele alınmaktadır.

¹⁹ Varsayılan gizlilik, sistemlerin varsayılan ayarlarının en yüksek gizlilik seviyesini sağlayacak biçimde yapılandırılması anlamına gelmektedir.

güven ortamının oluşturulması açısından önemli bir referans çerçevesi sunmaktadır (ISO, 2022; ISO, 2025b).

3.1.5. ISO/IEC ISO 8000-51:2023 Veri Kalitesi: Bölüm 51: Veri Yönetişimi: Veri Politikası Bildirimlerinin Paylaşımı

ISO 8000-51:2023 standardı, veri yönetişimi kapsamında veri politikası beyanlarının oluşturulması, tanımlanması, paylaşılması ve sistemler arasında değişiminin standartlaştırılmasına yönelik bir çerçeve sunmaktadır. Standart, ISO 8000²⁰ veri kalitesi serisinin bir parçası olup veri yönetişimi politikalarının bilgisayar tarafından işlenebilir biçimde temsil edilmesini amaçlamaktadır (ISO, 2023a).

ISO 8000-51 standardının temel yaklaşımı, veri yönetişimi politikalarının kurumsal veri yönetiminin çekirdek çıktılarından biri olduğu anlayışına dayanmaktadır. Standartta göre veri politikaları veri kullanılabilirliği, veri bütünlüğü, veri güvenliği ve veri erişilebilirliği gibi temel veri yönetişimi hedeflerinin uygulanmasını sağlayan yönetsel araçlardır. Bu politikalar, veri kümelerinin oluşturulması, yönetilmesi, paylaşılması ve kullanılması süreçlerini doğrudan etkilemektedir (ISO, 2023a).

Standart, veri kalitesini organizasyonel performansın temel bileşenlerinden biri olarak değerlendirmektedir. ISO 8000-51'e göre dijital veriler operasyonel etkinlik, güvenlik, düzenleyici uyumluluk, inovasyon, kurumsal itibar ve karar alma süreçleri üzerinde doğrudan etkiye sahiptir. Veri kalitesindeki eksiklikler ise organizasyonel performansın azalmasına neden olmaktadır. Bu nedenle veri yönetişimi politikalarının standartlaştırılması, veri kalitesinin sürdürülebilir biçimde yönetilebilmesi açısından kritik görülmektedir (ISO, 2023a).

ISO 8000-51 standardı, veri yönetişimi politika beyanlarının değişimine ilişkin temel gereksinimleri tanımlamaktadır. Buna göre her veri yönetişimi politika beyanı:

- Benzersiz bir tanımlayıcıya sahip olmalı,
- Politikayı yayımlayan organizasyonu açık biçimde tanımlamalı,
- Bilgisayar tarafından işlenebilir veri spesifikasyonlarına referans vermeli,

²⁰ Bkz. <https://www.iso.org/obp/ui/en/#iso:std:iso:8000:-2:ed-5:v1:en>

- Veri kümelerinin hangi gereksinimlere uygun olması gerektiğini açıklamalıdır (ISO, 2023a).

ISO 8000-51 standardı ayrıca veri yönetişimi otoritesi kavramına göre organizasyonlar, veri politikalarının geliştirilmesi ve uygulanmasından sorumlu bir veri yönetişimi otoritesi atamalıdır. Veri yönetişimi otoritesi, veri politikalarının kayıt altına alınmasını, izlenmesini, referanslandırılmasını ve uygunluk ölçümlerinin yapılmasını sağlamaktadır (ISO, 2023a).

Standartta veri yönetişimi politika kayıt sistemi organizasyon içerisindeki veri politikaları sistematik biçimde belgelenebilmektedir. Politika referansları yönetilebilmekte ve veri kümelerinin hangi politika gereksinimlerine tabi olduğu izlenebilmektedir. Ayrıca politika beyanlarının uygulama alanı, uygunluk ölçütleri ve izleme yöntemleri kayıt altına alınabilmektedir (ISO, 2023a).

ISO 8000-51, veri yönetişimi politika beyanlarının bilgisayar tarafından işlenebilir olması sayesinde otomatik uygunluk doğrulama süreçlerini desteklemektedir. Standartta göre organizasyonlar, veri kümelerinin ilgili politika gereksinimlerine uyumunu otomatik araçlarla test edebilmekte ve uygunluk raporlaması gerçekleştirebilmektedir (ISO, 2023a).

Standart ayrıca veri yönetişimi politikalarının organizasyonel stratejik hedeflerle ilişkili olduğunu vurgulamaktadır. Buna göre veri politikaları organizasyonun yasal yükümlülükleri, iş hedefleri ve yönetim yaklaşımıyla uyumlu stratejik yönetim araçlarıdır. Veri yönetişimi rejiminin tam anlamıyla uygulanabilmesi için organizasyon içerisindeki tüm verilerin bir veya daha fazla veri yönetişimi politika beyanı kapsamında olması gerektiği belirtilmektedir (ISO, 2023a).

ISO 8000-51 standardının önemli katkılarından biri de veri yönetişimi süreçlerinde birlikte çalışabilirlik (interoperability) ve veri taşınabilirliği (data portability) kavramlarını desteklemesidir. Standartlaştırılmış politika beyanları sayesinde farklı organizasyonlar, tedarik zinciri ortakları ve düzenleyici kurumlar arasında ortak veri anlayışı geliştirilebilmekte ve veri değişimi daha güvenilir hale getirilebilmektedir (ISO, 2023a).

3.1.6. ISO/IEC 5259-5:2025 Veri Kalitesi Yönetişim Çerçevesi

ISO/IEC 5259-5 standardı, analitik ve makine öğrenmesi sistemlerinde veri kalitesinin yönetişimine yönelik kapsamlı bir çerçeve sunmaktadır. Standart, veri kalitesinin yönetişim, risk yönetimi, stratejik planlama ve organizasyonel sorumluluk mekanizmalarıyla birlikte ele alınması gerektiğini vurgulamaktadır. ISO/IEC 5259 serisinin beşinci bölümü olan bu standart, özellikle yapay zeka ve analitik sistemlerde kullanılan verilerin güvenilir, tutarlı, kullanılabilir ve yönetilebilir olmasını sağlamayı amaçlamaktadır (ISO, 2025a).

Standartta veri kalitesi yönetişimi analitik ve makine öğrenmesi faaliyetlerinde kullanılan verilerin veri yaşam döngüsü boyunca yönlendirilmesi, izlenmesi ve kontrol edilmesine yönelik yönetsel yapı olarak tanımlanmaktadır. Bu çerçeve, yönetim organı ile yönetim katmanının veri kalitesi süreçlerinde nasıl etkileşim kuracağını açıklamakta ve organizasyon genelinde veri kalitesi yönetimi için sistematik bir yapı önermektedir (ISO, 2025a).

ISO/IEC 5259-5'in temel yaklaşımı, veri kalitesi yönetişiminin organizasyonun stratejik hedefleriyle ilişkilendirilmesidir. Standartta göre yönetim organı, veri kalitesi stratejilerini organizasyonun iş hedefleriyle uyumlu biçimde belirlemeli ve veri kalitesi politikalarının uygulanmasını gözetmelidir. Veri kalitesi stratejileri organizasyonun yapay zeka destekli iş hedeflerini, yasal gerekliliklerini, paydaş beklentilerini ve risk ortamını dikkate almalıdır. Standartta veri kalitesi yönetişim çerçevesinin temel bileşenleri arasında (ISO, 2025a):

- Veri kalitesi yönetişim ilkeleri,
- Veri kalitesi stratejileri ve politikaları,
- Veri kalitesi için iş planlaması,
- Veri kalitesi sorumlulukları,
- Veri kalitesi risk yönetimi,
- Veri kalitesi yönetim süreçleri,
- Gözetim ve denetim mekanizmaları yer almaktadır.

ISO/IEC 5259-5, veri kalitesi yönetiminde yönetim organı kavramına merkezi rol vermektedir. Yönetim organı veri kalitesi hedeflerini belirlemek, veri kalitesi politikalarını onaylamak, veri kalitesi risklerini izlemek ve organizasyon genelinde veri kalitesi kültürünü desteklemekle sorumludur. Standart, yönetim organının veri kalitesini stratejik karar alma süreçlerinin ayrılmaz bir bileşeni olarak değerlendirmesi gerektiğini belirtmektedir (ISO, 2025a).

Standart ayrıca veri kalitesi yönetiminde farklı organizasyonel roller tanımlamaktadır. Bunlar arasında:

- Veri ofisi sorumlusu,
- Veri sahipleri (data owners),
- Veri sorumluları (data stewards),
- Veri küratörleri (data curators),
- Yapay zeka ve veri bilimi uzmanları,
- Dijital dönüşüm ekipleri yer almaktadır.

Özellikle veri sorumlularının veri politikalarının uygulanması, veri standartlarının korunması ve veri kalitesi sorunlarının yönetilmesinde kritik rol oynadığı ifade edilmektedir (ISO, 2025a).

ISO/IEC 5259-5 standardı, veri kalitesi yönetimini risk temelli bir yaklaşımla ele almaktadır. Veri kalitesi risk yönetimi kapsamında organizasyonların:

- Veri risklerini tanımlaması,
- Risk etkilerini değerlendirmesi,
- Risk önceliklendirmesi yapması,
- Risk azaltıcı kontroller geliştirmesi,
- Veri kalitesi risklerini sürekli izlemesi gerektiği belirtilmektedir (ISO, 2025a).

Standart, özellikle yapay zeka sistemlerinde veri kaynaklı önyargılar, etik sorunlar, doğruluk problemleri ve düzenleyici risklerin yönetilmesini önemli görmektedir. Standartta veri kalitesi politikalarının kapsamlı ve organizasyon genelinde uygulanabilir olması gerektiği vurgulanmaktadır. Veri politikalarının:

- Veri yaşam döngüsünün tüm aşamalarını kapsamaması,
- Veri mimarisiyle bütünleşmesi,
- Risk yönetim süreçleriyle ilişkilendirilmesi,
- Veri gizliliği ve güvenliğiyle uyumlu olması,
- Düzenli olarak gözden geçirilmesi önerilmektedir (ISO, 2025a).

Ayrıca veri politikalarının organizasyonel değişim süreçleriyle birlikte güncellenmesi gerektiği ifade edilmektedir. ISO/IEC 5259-5 standardı, veri kalitesinin organizasyonel kültür ve yönetim mekanizmalarıyla da ilişkili olduğunu belirtmektedir. Bu nedenle standart, veri kalitesi farkındalığının artırılması, eğitim programlarının yürütülmesi ve veri odaklı karar alma kültürünün geliştirilmesini veri yönetişiminin önemli unsurları arasında değerlendirmektedir (ISO, 2025a).

3.2. ULUSLARARASI KURUM TEMELLİ ÇERÇEVELER

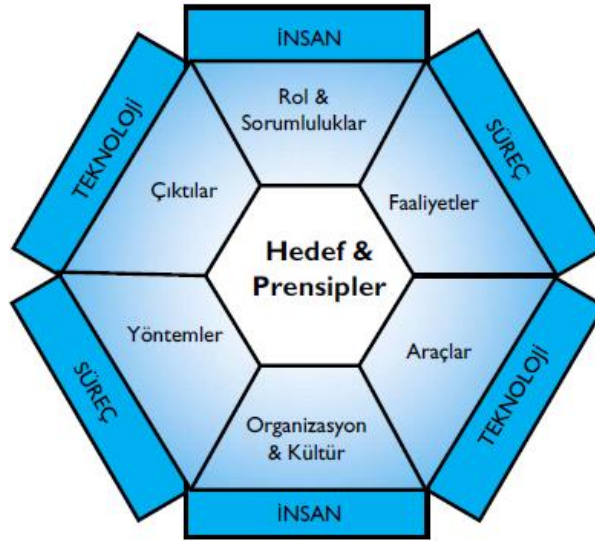
3.2.1. DAMA-DMBOK2 Çerçevesi

DAMA-DMBOK2 (Data Management Body of Knowledge 2nd Edition) Çerçevesi, veri yönetimi ve veri yönetişimi alanında en yaygın kullanılan uluslararası referans çerçevelerinden biridir. DAMA Çarkı (Bkz. Şekil 6), Çevresel Faktörler Altıgeni (Bkz. Şekil 7) ve Bilgi Alanı Bağlam Şeması (Bkz. Şekil 8) ile kurumlarda verinin etkin, güvenli ve değer üreten bir varlık olarak yönetilebilmesi için gerekli süreçleri, rolleri, politikaları ve teknik uygulamaları bir yapı içinde tanımlanmaktadır. DAMA-DMBOK2 Veri Yönetimi Çerçevesi (DAMA Çarkı) veri yönetişimini veri yönetiminin merkezine yerleştirmiştir. Çarkın etrafındaki 11 adet Bilgi Alanları, olgun veri yönetimi için gereklidir. Bilgi Alanları kurumun ihtiyaç ve beklentilerine göre değişiklik gösterebilir (Bkz. Şekil 6; DAMA, 2017, s. 36).



Şekil 6. DAMA-DMBOK2 veri yönetimi çerçevesi (DAMA Çarkı) (DAMA, 2017, s. 36)

DAMA-DMBOK2 veri yönetimi bilgi alanlarını tanımlarken bu alanların nasıl uygulanacağını belirleyen temel çevresel bileşenleri ortaya koymaktadır. Çevresel Faktörler Altıgeni veri yönetimi faaliyetleri insan, süreç ve teknoloji boyutlarının etkileşimi içerisinde değerlendirmektedir. Bu üç temel unsur, veri yönetimi uygulamalarının kurumsal bağlamda sürdürülebilir ve etkili biçimde yürütülmesini sağlayan temel yapı taşlarını oluşturmaktadır. Altıgenin merkezinde yer alan *hedef ve prensipler*, veri yönetiminin kurumsal amaçlarını ve veriyle ilgili temel ilkeleri ifade etmektedir. Kurumun veri stratejisi, veri kullanımına ilişkin etik ilkeler, veri paylaşım politikaları ve veri değerinin nasıl üretileceği gibi konular bu kapsamda ele alınmaktadır. Veri yönetimi politikaları da genellikle bu merkezde tanımlanan hedef ve prensiplere dayanmaktadır (Bkz. Şekil 7; DAMA, 2017, s. 36).



Şekil 7. DAMA çevresel faktörler altıgeni (DAMA, 2017, s. 36).

DAMA-DMBOK2 çerçevesinde kullanılan Bilgi Alanı Bağlam Şeması, veri yönetimi bilgi alanlarının nasıl çalıştığını üst düzeyde açıklamaktadır. Şema, her veri yönetimi alanının belirli hedefler, girdiler, faaliyetler, çıktılar ve performans ölçütleri doğrultusunda işlediğini göstermektedir. Diyagramın en üst kısmında tanım ve hedefler yer almaktadır. Tanım bölümü, ilgili veri yönetimi bilgi alanının kapsamını ve temel amacını açıklarken hedefler ise bu alanın kurum içinde ulaşmayı amaçladığı sonuçları ifade etmektedir. Diğer unsur girdiler, veri yönetimi faaliyetlerinin başlamasını sağlayan bilgi veya kaynakları ifade etmektedir. DAMA-DMBOK2 yaklaşımında girdiler çoğunlukla diğer veri yönetimi alanlarından gelen çıktılardan oluşmaktadır.

Diyagramın merkezinde faaliyetler yer almaktadır. Bu faaliyetler planlama²¹ (P), kontrol²² (C), geliştirme²³ (D) ve operasyonlar²⁴ (O) olmak üzere dört ana grupta ele alınmaktadır. Bu dört faaliyet grubu, veri yönetiminin sürekli bir yaşam döngüsü içerisinde yürütüldüğünü göstermektedir.

²¹ Planlama faaliyetleri, veri yönetimi stratejilerinin ve politikalarının belirlenmesini içermektedir.

²² Kontrol faaliyetleri, belirlenen standartların uygulanıp uygulanmadığının izlenmesini kapsamaktadır.

²³ Geliştirme faaliyetleri, veri yönetimi süreçlerinin iyileştirilmesi ve yeni çözümlerin geliştirilmesine odaklanmaktadır.

²⁴ Operasyonel faaliyetler ise veri yönetimi uygulamalarının günlük işleyişini ifade etmektedir.

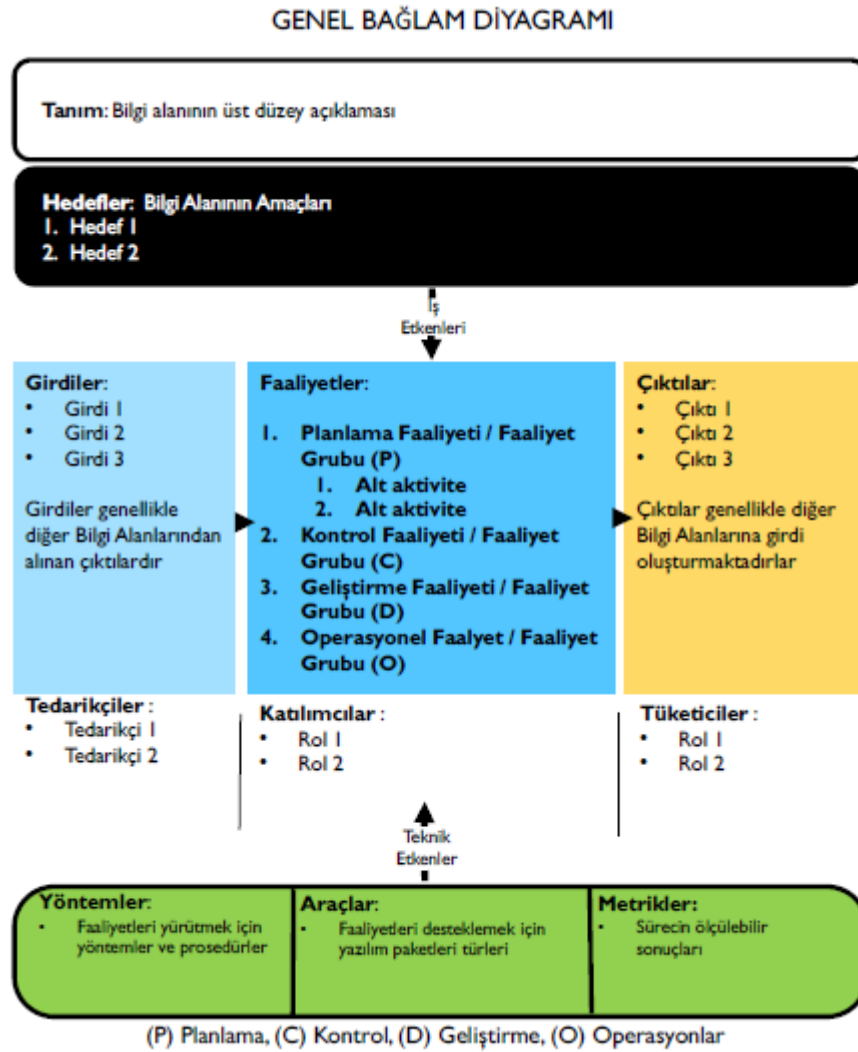
Faaliyetlerin sonucunda ortaya çıkan çıktılar, veri yönetimi uygulamalarının somut sonuçlarını temsil eder. Veri sözlükleri, veri standartları, veri kalite raporları, üst veri katalogları ve veri yönetişimi politikaları bu çıktılar arasında yer alabilir. Bu çıktılar çoğu zaman diğer veri yönetimi alanları için girdi oluşturmakta ve böylece veri yönetimi ekosisteminde sürekli bir bilgi akışı meydana gelmektedir.

Şemada veri yönetimi sürecine dahil olan tedarikçiler²⁵, katılımcılar²⁶ ve tüketiciler²⁷ gibi paydaşları da tanımlamaktadır. Veri yönetiminin kurum içinde çok paydaşlı bir süreç olduğunu göstermektedir. Şemanın alt bölümünde yöntemler, araçlar ve metrikler yer almaktadır. Bu unsurlar, veri yönetimi faaliyetlerinin sistematik ve ölçülebilir bir şekilde yürütülmesini sağlamaktadır (Bkz. Şekil 8; DAMA, 2017, s. 37).

²⁵ Tedarikçiler veri veya bilgi sağlayan birimleri temsil etmektedir

²⁶ Katılımcılar veri yönetimi faaliyetlerini yürüten rol ve sorumluluklara sahip aktörleri ifade etmektedir.

²⁷ Tüketiciler ise veri yönetimi çıktılarından yararlanan kişi veya kurumları kapsamaktadır.



Şekil 8. Bilgi alanı bağlam şeması (DAMA, 2017, s. 37).

Peter Aiken'in çerçevesi, DAMA-DMBOK2 DAMA Çarkı yaklaşımına dayalı olarak Bilgi Alanları arasındaki ilişkiyi ifade etmektedir. Piramidin alt seviyeleri veri yönetiminin temel altyapısını oluştururken, üst seviyeler daha gelişmiş veri analitiği ve stratejik veri kullanımını temsil etmektedir.

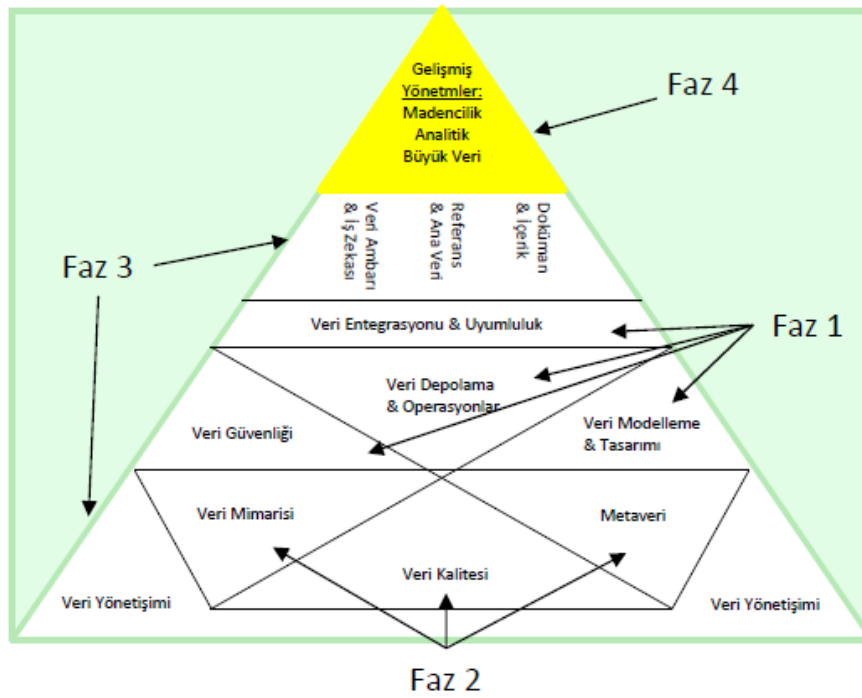
Piramidin ilk aşaması olan Faz 1, kurumlarda veri yönetiminin teknik ve operasyonel temellerinin oluşturulmasını ifade etmektedir. Bu aşamada özellikle veri modelleme ve tasarımı, veri depolama ve operasyonlar ile veri entegrasyonu ve uyumluluk gibi alanlar ön plana çıkmaktadır. Bu süreçler kurum içerisindeki farklı sistemlerde bulunan verilerin standartlaştırılması, veri akışlarının düzenlenmesi ve verilerin sistematik bir şekilde saklanması sağlamaktadır. Faz 1, veri yönetimi altyapısının oluşturulması açısından

kritik bir aşamadır ve sonraki veri yönetimi süreçlerinin sağlıklı bir şekilde yürütülebilmesi için gerekli teknik temeli sağlamaktadır.

Piramidin alt bölümünde yer alan Faz 2, veri yönetiminin kurumsal ve yönetsel boyutunu temsil etmektedir. Bu aşamada veri yönetiřimi, veri mimarisi, veri kalitesi ve üst veri yönetimi gibi temel yönetim bileřenleri ön plana çıkmaktadır. Veri yönetiřimi bu aşamada veri politikalarının oluřturulması, veri sorumluluklarının belirlenmesi ve veri standartlarının tanımlanması gibi görevleri üstlenmektedir. Aynı zamanda veri mimarisi ve üst veri yönetimi, veri varlıklarının kurumsal düzeyde tanımlanmasını ve anlamlandırılmasını sağlamaktadır. Veri kalitesi yönetimi ise verinin doğruluęu, tutarlılıęı ve güvenilirlięinin saęlanmasıya yönelik süreçleri kapsamaktadır.

Faz 3, veri yönetimi uygulamalarının kurumsal karar verme süreçlerine daha aktif biçimde entegre edildięi aşamayı temsil etmektedir. Bu aşamada veri ambarı ve iř zekası, referans veri ve ana veri yönetimi ile doküman ve içerik yönetimi gibi alanlar ön plana çıkmaktadır. Bu süreçler sayesinde kurumsal veriler analiz edilebilir hale getirilmekte ve karar destek sistemlerinde kullanılmaktadır. Ayrıca ana veri yönetimi uygulamaları, kurum içinde kullanılan kritik veri varlıklarının tek bir doğruluk kaynaęına dayanmasını sağlamaktadır.

Piramidin en üst kısmını oluřturan Faz 4 ise veri yönetimi olgunluęunun en ileri aşamasını temsil etmektedir. Bu aşamada kurumlar ileri analitik yöntemler, veri madencilięi ve büyük veri teknolojileri gibi gelişmiř veri iřleme tekniklerini kullanmaya başlamaktadır. Kurumlar veri analitięi ve veri bilimi uygulamaları aracılıęıyla yeni bilgi üretmekte ve rekabet avantajı elde etmektedir (Bkz. Şekil 9; DAMA, 2017, s. 40).



Şekil 9. DMBOK piramidi (Aiken) (DAMA, 2017, s. 40).

DAMA Bilgi Alanları arasındaki ilişkiyi Sue Geunes tarafından geliştirilen Şekil 10'daki DAMA Fonksiyonel Alan Bağımlılıkları, veri yönetimi ve veri yönetişimi süreçlerinin katmanlı bir mimari yapı içinde nasıl organize edildiğini göstermektedir. Model, veri yönetişiminin kurumsal veri ekosisteminin temelinde yer aldığını ve veri yönetimi süreçlerinin bu temel üzerinde geliştiğini ortaya koymaktadır. İş Zekası ve Analitiği katmanının en üstte olması veri yönetimi süreçlerinin sonucunda elde edilen verilerin analiz edilerek kurumsal karar verme süreçlerinde kullanılmasını temsil etmektedir. Veri yönetiminin temel yönetişim mekanizmalarından başlayarak analitik ve karar destek uygulamalarına kadar uzanan bir sistem olduğunu göstermektedir (DAMA, 2017, s. 41).



Şekil 10. DAMA fonksiyonel alan bağımlılıkları (DAMA, 2017, s. 41).

DAMA Çarkının bir diğer alternatifi olarak Şekil 11’de gösterilen Veri Yönetimi Fonksiyon Çerçevesi, DAMA Bilgi Alanları arasında mimari konseptlerden yararlanarak ek bilgiler sağlamaktadır. Veri yönetimi faaliyetlerini yönetim, yaşam döngüsü yönetimi ve temel destek faaliyetleri olmak üzere üç ana katmanda ele almaktadır.

Modelin üst bölümünde yer alan veri yönetimi, veri yönetiminin stratejik ve yönetsel boyutunu temsil etmektedir. Bu kapsamda veri stratejisinin belirlenmesi, veri değerinin tanımlanması, etik ilkelerin oluşturulması, veri politikalarının geliştirilmesi ve veri sorumluluklarının belirlenmesi gibi faaliyetler yürütülmektedir. Ayrıca veri yönetiminin kurum içinde benimsenebilmesi için organizasyonel kültür değişimi de önemli bir unsur olarak ele alınmaktadır.

Orta bölümde yer alan veri yaşam döngüsü yönetimi, verinin oluşturulmasından kullanılmasına ve değer üretmesine kadar geçen süreçleri kapsamaktadır. Bu süreçler genel olarak planlama ve tasarım, kullanım ve geliştirme ve değer üretme ve sürdürme aşamalarından oluşmaktadır. Veri mimarisi ve veri modelleme tasarımı planlama aşamasında yer alırken veri depolama, veri entegrasyonu, ana veri yönetimi ve veri ambarı gibi faaliyetler verinin kullanım ve geliştirme aşamasında gerçekleştirilmektedir. Son aşamada ise iş zekası, veri bilimi ve analitik uygulamalar aracılığıyla veriden kurumsal değer üretilmektedir.

Modelin alt kısmında yer alan temel aktiviteler ise veri yönetimi süreçlerini destekleyen sürekli faaliyetleri göstermektedir. Bu kapsamda veri riski yönetimi (güvenlik, gizlilik ve uyum), üst veri yönetimi ve veri kalitesi yönetimi veri yönetimi fonksiyonlarının sürdürülebilir ve güvenilir şekilde yürütülmesini sağlayan temel alanlar olarak ele alınmaktadır (DAMA, 2017, s. 42).



Şekil 11. DAMA veri yönetimi fonksiyon çerçevesi (DAMA, 2017, s. 42).

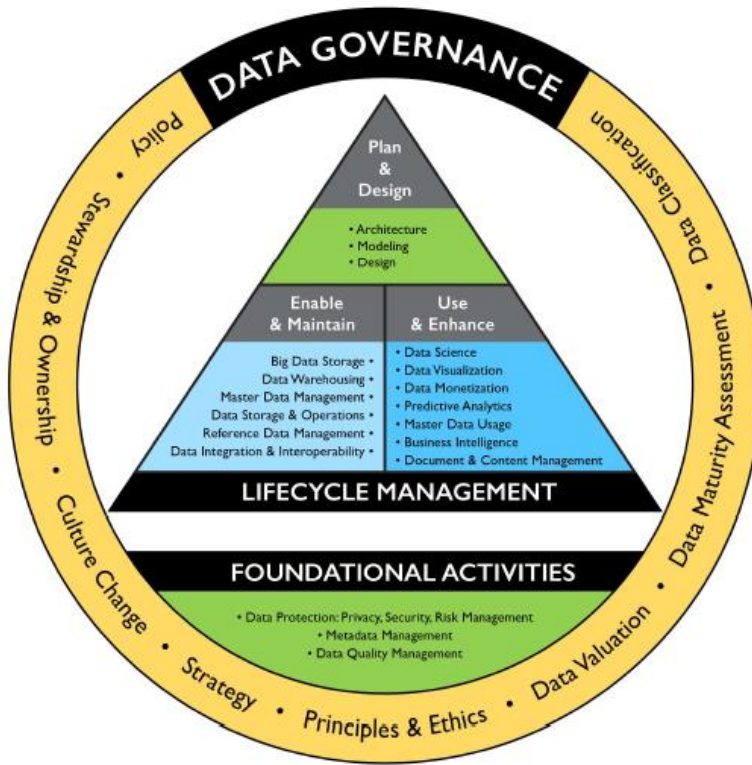
Şekil 12'deki Gelişmiş DAMA Çarkı, veri yönetimi faaliyetlerini veri yönetişimi, veri yaşam döngüsü yönetimi ve temel destek faaliyetleri olmak üzere üç temel katman üzerinden ele alan bir çerçeve sunmaktadır. Gelişmiş DAMA Çarkı, Şekil 6'dan Şekil 11'e kadar olan yaklaşımların bütünsel bir özeti niteliğinde olduğu görülmektedir.

Gelişmiş DAMA Çarkında veri yönetişimi katmanı veri yönetiminin stratejik ve yönetsel boyutunu temsil etmektedir. Veri stratejisi, politikalar, veri sahipliği, veri değerlendirme, etik

ilkeler ve veri olgunluk deęerlendirmesi gibi unsurlar bu katmanda yer almakta ve veri yönetimi süreçlerinin kurumsal hedeflerle uyumlu biçimde yürütölmesini sağlamaktadır. Bu durum, özellikle DAMA Çarkı veri yönetişiminin tüm Bilgi Alanları alanlarını yönlendiren bir üst yapı olarak tanımlanmasıyla uyumludur.

Çarkın merkezinde yer alan veri yaşam döngüsü yönetimi, üç aşamalı bir yapıdan oluşmaktadır. İlk aşama olan planlama ve tasarım sürecinde veri mimarisi, veri modelleme ve veri tasarımı faaliyetleri yürütölmektedir. Bu aşama, verinin kurumsal sistemlerde nasıl yapılandırılacağını belirleyen temel mimari süreçleri kapsamaktadır. İkinci aşama olan sağlama ve sürdürme aşamasında veri depolama, veri entegrasyonu, veri ambarı, ana veri yönetimi ve büyük veri depolama gibi veri altyapısı süreçleri yer almaktadır. Son aşama olan kullanım ve geliştirme aşamasında ise veri bilimi, veri görselleştirme, tahmine dayalı analitik ve iş zekası gibi analitik faaliyetler aracılığıyla veriden deęer üretilmektedir. Aiken piramidi modelindeki veri altyapısından analitik deęere doğru ilerleyen gelişim süreciyle örtüşmektedir.

Modelin alt kısmında yer alan temel faaliyetler ise veri yönetiminin sürdürülebilirliğini sağlayan destek mekanizmalarını temsil etmektedir. Veri koruma (gizlilik, güvenlik ve risk yönetimi), üst veri yönetimi ve veri kalitesi yönetimi bu kapsamda ele alınmaktadır. Bu alanlar, Fonksiyonel Alan Bağımlılıkları ile uyum göstermektedir (DAMA, 2017, s. 44).



Şekil 12. Gelişmiş DAMA çarkı (DAMA, 2017, s. 44).

3.2.2. Veri Yönetişimi Enstitüsü Çerçevesi

Veri yönetişimi alanında Veri Yönetişimi Enstitüsü (Data Governance Institute, DGI) tarafından ortaya konulan DGI Veri Yönetişimi Çerçevesi kurumsal verilerle ilgili karar alma süreçleri ve uygulamaların sınıflandırılması, organize edilmesi ve kurum içinde etkin biçimde iletişiminin sağlanması amacıyla geliştirilmiş mantıksal bir yapı sunmaktadır. Çerçeve, kurumların veri yönetimine ilişkin kararları sistematik biçimde ele almasına yardımcı olmakta ve veri varlıklarından değer elde edilmesini destekleyen yönetim mekanizmalarını tanımlamaktadır (DGI, t.y.).

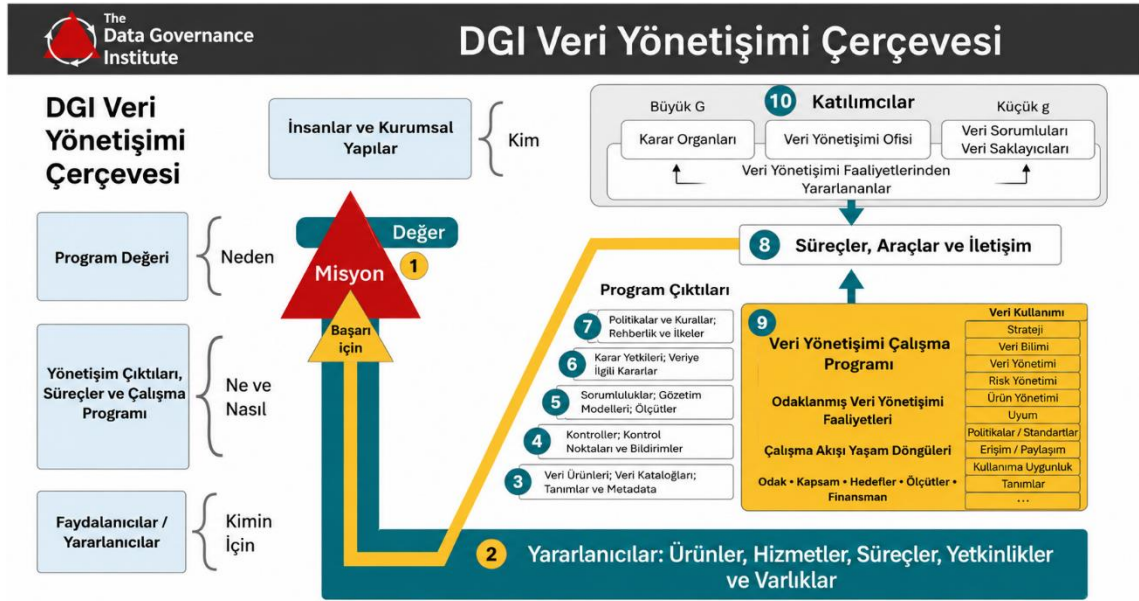
DGI veri yönetişimi çerçevesi, veri yönetişimi faaliyetlerini neden, kim, ne ve nasıl ve kimin için soruları etrafında toplam 10 adımda yapılandırmaktadır. Çerçevenin başlangıç noktası değer odaklı bir veri yönetişimi programıdır. Bu yaklaşımda veri yönetişimi programı, kurum için belirlenen değer ifadeleri doğrultusunda oluşturulmakta ve programın temel misyonu bu değerlerin kurum paydaşlarına ölçülebilir biçimde sunulmasını sağlamaktır (DGI, t.y.).

Çerçevede dikkat çeken yaklaşımlardan biri olan küçük g yönetiřimi²⁸ (little g governance) ve büyük G yönetiřimi²⁹ (Big G governance) olarak adlandırılan ifadelerdir. DGI çerçevesinde veri yönetiřimi faaliyetleri süreçler, araçlar ve iletiřim mekanizmaları tarafından desteklenmektedir. Veri yönetiřimi programı, farklı faaliyetlerden oluřan bir çalışma programı portföyü olarak yönetilmektedir. Bu portföyde yer alan her faaliyet belirli bir odak alanına, kapsamına, hedeflerine, performans ölçütlerine, yařam döngüsüne ve finansman modeline sahiptir. Böylece veri yönetiřimi uygulamaları planlı ve sürdürülebilir bir program çerçevesinde yürütölmektedir (DGI, t.y.).

Çerçevenin uygulanmasında merkezi rol oynayan yapı Veri Yönetiřimi Ofisi (Data Governance Office, DGO) veri yönetiřimi çalışma programının koordinasyonundan sorumlu olup programın yürütölmelerini saęlamaktadır. Bunun yanında veri yönetiřimi sürecinde karar organları, veri sorumluları (data stewards), veri saklayıcıları (data custodians) ve programın çıktılarından yararlanan paydařlar gibi farklı katılımcılar yer almaktadır. Bu çok paydařlı yapı, veri yönetiřiminin kurum genelinde benimsenmesini ve uygulanmasını kolaylařtırmaktadır (DGI, t.y.).

²⁸ Veri ürünleri, veri katalogları, veri tanımları, üst veri yönetimi, kontrol mekanizmaları, kontrol noktaları ve ölçüm süreçleri gibi veri yönetimine iliřkin uygulamalardır.

²⁹ Veri ile ilgili karar yetkilerinin belirlenmesi, veri odaklı karar alma süreçlerinin tanımlanması, hesap verebilirlik mekanizmalarının oluřturulması, gözetim ve denetim modellerinin geliřtirilmesi ile veri politikaları ve kurallarının belirlenmesi gibi yönetiřim faaliyetleri bulunmaktadır.



Şekil 13. Veri yönetişimi enstitüsü çerçevesi (DGI, t.y.)

3.2.3. OECD Veri Yönetişimi Çerçevesi

OECD'nin 2020 yılında yayımladığı *Dijital Hükümet Politikası Çerçevesi*³⁰ kamu kurumlarında veri yönetişiminin nasıl kuracağına odaklanmaktadır. 2022 yılında yayımladığı *Dijitalleşmeye Geçiş: Veri Yönetimi Politikası Oluşturma Rehberi*³¹ ise bir ülkenin veya kurumun veri politikalarını nasıl tasarlayacağını ile ilgilenmektedir. Bu nedenle biri operasyonel, diğeri politika düzeyinde tamamlayıcı rol oynamaktadır.

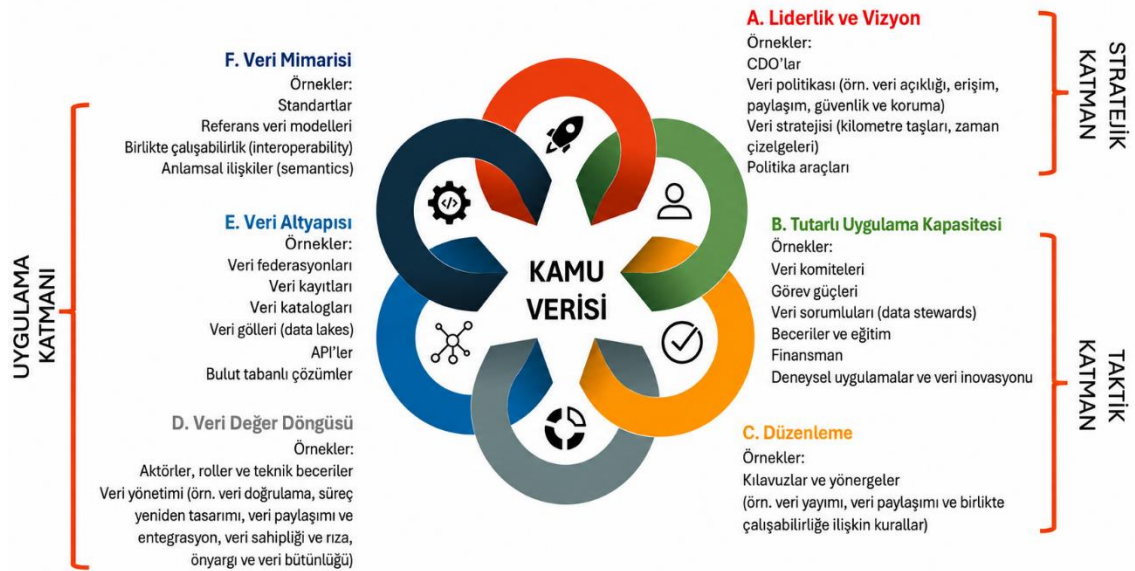
Dijital Hükümet Politikası Çerçevesi, Dijital dönüşümü e-devlet uygulamalarından daha kapsamlı bir çerçeveye taşıyarak *dijital hükümet* anlayışını altı boyut³² üzerinden tanımlamaktadır. Bu altı boyut ülkelerin kurumsal olgunluk düzeylerini tanımlamakta,

³⁰ Bkz. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/the-oecd-digital-government-policy-framework_11dd6aa8/f64fed2a-en.pdf

³¹ Bkz. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/going-digital-guide-to-data-governance-policy-making_28519d90/40d53904-en.pdf

³² Dijital olarak tasarlanmış politika, süreç ve hizmetlerin ilk aşamadan itibaren dijitali merkeze alarak kurgulanması), veri odaklı kamu sektörü (kamu yönetiminin karar alma, uygulama ve değerlendirme süreçlerinde verinin belirleyici olması), platform olarak devlet (kamu hizmetlerinin modüler, paylaşılan altyapılar ve ortak standartlar üzerinden sunulması), açıklık ilkesi (veri, bilgi, süreç ve kararların kural olarak açık olması, istisnaların gerekçelendirilmesi), kullanıcı odaklı (hizmetlerin tasarımında kullanıcı ihtiyaçlarının, davranışlarının ve geri bildirimlerinin belirleyici olması), proaktif devlet (devletin vatandaşların ihtiyaçlarını önceden görerek harekete geçmesi, talep gelmeden hizmet sunabilmesi.)

dijital hükümet olgunluk seviyeleri OECD'nin Dijital Hükümet Endeksi³³ ile ölçülmektedir. Veri odaklı kamu sektörü ve ona eşlik eden kurumsal veri yönetişi modeli dikkat çekmektedir. Çerçeve, kamu verisinin *stratejik varlık* olarak yönetilmesi ve politika tasarımı, hizmet sunumu ve izleme/değerlendirmede sistematik olarak kullanılmasını amaçlamaktadır. OECD'nin Arjantin kamu sektörü için geliştirdiği veri yönetişi çerçevesi stratejik, taktik ve uygulama katmanlarında liderlik, düzenleme, kapasite, veri değer döngüsü, veri altyapısı ve veri mimarisi bileşenlerinin etkileşimini göstermektedir (Bkz. Şekil 14). Bu çerçeve, daha çok kamu idaresi için kurumsal model ve altyapı tasarımı perspektifinden veri yönetişimine bakmaktadır (OECD, 2020).



Şekil 14. Kamu sektöründe veri yönetişimi (OECD, 2019, s. 164)

Dijitalleşmeye Geçiş: Veri Yönetimi Politikası Oluşturma Rehberi, ülkelerin veri ekonomisi, veri paylaşım ekosistemleri, dijital piyasa düzenlemeleri ve sektörel veri yönetişimi (sağlık, araştırma, ticaret vb.) için kapsamlı bir analiz ve tasarım sunmaktadır. Bu metin, doğrudan veri yönetişimi politikası üretmek isteyen politika yapıcılara rehberlik etmektedir. Bu rehberde veri yönetişimi üç³⁴ temel alanı üzerine

³³ Bkz. <https://goingdigital.oecd.org/en/indicator/58>

³⁴ **Açıklık, Kontrol, Güven Dengesi:** Veriye erişim ve veri paylaşımı ilkeleri, mahremiyet, güvenlik ve etik ile dengelenmelidir. OECD, veri açıklığını tam açık veriden kontrollü erişime uzanan bir süreklilik olarak sunmaktadır.

şekillendirilmektedir. Rehber bu üç temel alanı için politika soruları, kontrol listeleri, düzenleyici seçenekler, sözleşmesel araçlar, risk yönetimi yaklaşımları ve uluslararası işbirliği önerileri sunmaktadır. Böylece rehber, veri yönetişimini makro düzeyde politika tasarımına rehberlik eden bir üst çerçeve haline getirmiştir (OECD, 2022).

Her iki OECD belgesi de verinin stratejik bir varlık olduğu, kamu değerini artırdığı, güven, etik ve şeffaflıkla desteklenmesi gerektiği, çok paydaşlı yönetim gerektirdiği konularında benzerlik göstermektedir. Ayrıca her iki belge de veri yönetişimini kurumsal kapasite, hukuk, etik ve stratejik planlamayı içeren çok boyutlu bir dönüşüm olduğunu vurgulamaktadır. Bu nedenle OECD'nin iki belgesinden elde edilen çerçeveler, üniversiteler için güçlü bir kuramsal temel sağlamaktadır. OECD'nin 2020 ve 2022 belgeleri birlikte değerlendirildiğinde, üniversitelerde veri yönetişimi için iki katmanlı bir teorik çerçeve ortaya çıkmaktadır. Kurumsal yapı, roller, süreçler, dijital mimari ve etik ilkelerin yer aldığı operasyonel-kurumsal katman (OECD, 2020) açıklık, güven, düzenleyici uyum, yatırım gereksinimleri ve çok paydaşlı yönetim başlıklarının yer aldığı politika-tasarım katmanı (OECD, 2022). Bu iki katman bir araya getirildiğinde, üniversiteler için hem iç işleyişi düzenleyen hem de dış paydaşlar ve düzenleyici çerçevelerle uyumlu bir veri yönetişimi modelinin temeli oluşturulabilir.

3.2.4. UNDP Dijital Strateji 2022–2025

UNDP Dijital Stratejisi, dijital dönüşümünde kurumsal kapasite, yönetim ve kültürel dönüşüm süreci olarak kurgulayan çok katmanlı bir çerçeve sunmaktadır. Stratejinin omurgası yönetim, insan/kültür ve teknoloji oluşmaktadır. Bunların üzerinde yükselen veriye dayalı karar alma ve sürdürülebilir kalkınma adımları vardır. Kurumsal dönüşüm

Çakışan Çıkarların ve Çoklu Düzenleyici Çerçevelerin Yönetimi: Veri değer döngüsü boyunca kişisel haklar, fikri mülkiyet, rekabet hukuku, tüketici hakları ve sektörel düzenlemeler gibi birbiriyle çatışan normatif yapılar bulunur. Bu nedenle veri yönetişimi, bütüncül bir koordinasyon ve çok paydaşlı yönetim gerektirmektedir.

Veriye ve Tamamlayıcı Varlıklara Yatırım ve Teşvikler: Veri altyapıları, analitik kapasite, veri yetkinlikleri ve sektörler arası veri paylaşım mekanizmaları için finansman ve uzun vadeli stratejik yatırımlara ihtiyaç vardır.

örgütsel zihniyet değişimine bağlamaktadır. Bu kapsamda veri, kurum içinde paylaşılan stratejik bir varlık olarak konumlandırılmaktadır. Tüm personele yönelik veri okuryazarlığı eğitimleri, uzmanlaşmış analitik programları ve sürekli öğrenme mekanizmaları oluşturulmaktadır. Veri topluluğu (data community) yaklaşımıyla paylaşım, açıklık ve iş birliği normları güçlendirilmektedir. Kültürel dönüşüm, kurumsal veri yönetişiminin en kritik bileşenlerinden biri olarak değerlendirilmektedir (UNDP, 2021).

Teknoloji ve veri mimarisi boyutunda strateji, UNDP'nin veriyle güçlendirilmiş kurum haline gelmesini hedeflemektedir. Bu çerçevede bir birleşik veri merkezi kurumsal veri gölü ve veri kataloğu oluşturulmaktadır. Sistemler arası veri entegrasyonu ve birlikte çalışabilirlik güçlendirilmektedir. Ayrıca sürdürülebilirlik ilkeleri doğrultusunda geleceğe hazır yeşil veri altyapısı yaklaşımı benimsenmektedir. Böylece teknolojik dönüşüm çevresel sorumlulukla bütünleştirilmektedir (UNDP, 2021).

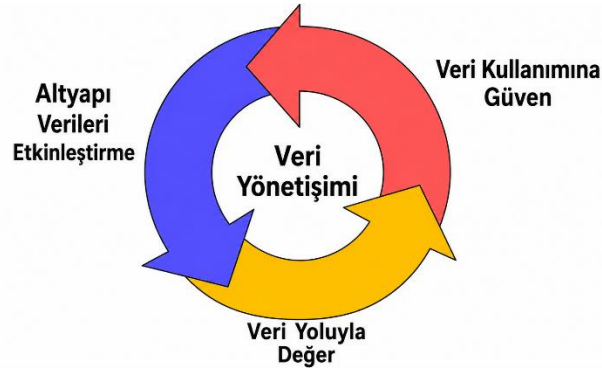
3.2.5. Dünya Bankası Veri Yönetişimi Tanı Aracı

Dijital dönüşüm sürecinde verinin ekonomik ve toplumsal değer üretme kapasitesinin artması, ülkeleri veri yönetimine ilişkin daha kurumsallaşmış yönetim modelleri geliştirmeye zorlamaktadır. Bu bağlamda Dünya Bankası tarafından geliştirilen Veri Yönetişimi Tanı Aracı (Data Governance Diagnostic Tool), ülkelerin veri yönetişimi kapasitesini ölçmek ve politika geliştirme süreçlerine yön vermek amacıyla oluşturulmuş kapsamlı bir değerlendirme çerçevesi sunmaktadır (World Bank, 2020).

Araç, veri yönetişiminin politika üretimi, kurumsal yapılanma ve hukuki denetim boyutlarını kapsayan çok katmanlı bir alan olarak ele almaktadır. Aracın temel amacı, verinin tüm yaşam döngüsü boyunca güvenilir, şeffaf ve hesap verebilir biçimde yönetilmesini sağlayarak veri temelli kalkınma için gerekli olan kurumsal zemini oluşturmaktır (World Bank, 2020).

Dünya Bankası çerçevesi, veri yönetişimini etkinleştiriciler (enablers), güvenlik önlemleri (safeguards) ve sonuçlar (outcomes) olmak üzere üç ana sütun üzerine inşa etmektedir. Bu çerçeve, veri ekosisteminin işleyiş mantığını altyapı (infrastructure), güven (trust) ve değer (value) döngüsü üzerinden açıklayan yönetim mimarisi

sunmaktadır. Bu döngüye göre teknik ve kurumsal altyapı olmadan veri üretilemez. Güven mekanizmaları olmadan veri paylaşımı ve kullanımı sürdürülebilir olmaz. Değer üretimi olmadan ise veri yönetişimi politikaları toplumsal ve ekonomik geçerlilik kazanamaz (Bkz. Şekil 16).



Şekil 16. Veri yönetişimi tanı aracı (World Bank, 2020, s. 10)

Araçtaki altyapı, veri yönetişiminin teknik ve yönetsel altyapısını oluşturan politika, kurum ve sistemleri kapsamaktadır. Bu boyut, verinin üretilmesi, depolanması, paylaşılması ve analiz edilmesini mümkün kılan yapısal koşulları değerlendirmektedir. Ulusal dijital dönüşüm vizyonu, geniş bant altyapısı, 5G kapasitesi, bulut bilişim sistemleri, ulusal veri altyapısı, devletler arası birlikte çalışabilirlik çerçeveleri ve açık veri politikaları bu sütunun temel bileşenleri arasında yer almaktadır. Bunun yanında kurumsal kapasite, veri yönetişimi rollerinin tanımlanması, insan kaynağı gelişimi ve veri kültürünün kurumsallaşması da altyapıların ayrılmaz parçalarıdır (World Bank, 2020).

Altyapı, verinin ekonomik ve toplumsal değer üretimine dönüşebilmesi için gerekli olan kurumsal üretim hattını temsil etmektedir. Yetersiz altyapı, parçalı kurumsal yapı ve düşük insan kaynağı kapasitesi, veri yönetişimi politikalarının kağıt üzerinde kalmasına neden olmaktadır. Bu da dijital dönüşüm yatırımlarının beklenen faydayı üretmesini engellemektedir (World Bank, 2020).

Güven, veri kullanımına duyulan güvenin tesis edilmesini amaçlayan hukuki ve kurumsal mekanizmaları kapsamaktadır. Kişisel veri koruma mevzuatı, siber güvenlik politikaları, siber suçla mücadele, tüketici haklarının korunması, elektronik ticaret düzenlemeleri ve sınır ötesi veri akışlarına ilişkin düzenlemeler bu sütunun ana unsurlarını oluşturmaktadır.

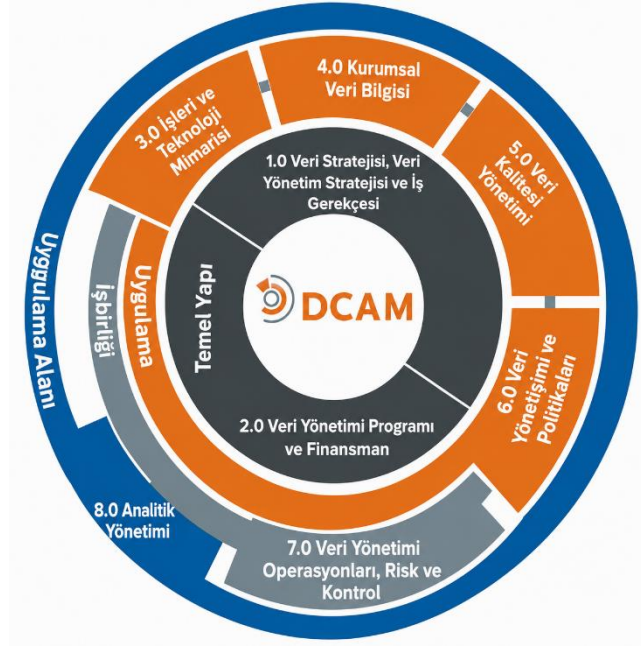
Güven boyutu, veri yönetişiminin verimlilik ve yenilik üretme işlevini, bireysel hakları, hukukun üstünlüğünü ve kamu güvenliğini koruyan bir çerçeve sunduğunu göstermektedir. Güvencelerin zayıf olduğu sistemlerde veri paylaşımı sınırlanmaktadır. Dijital hizmetlere duyulan güven azalmakta ve veri ekonomisi gelişmemektedir. Bu nedenle güven boyutu, veri yönetişimi ekosisteminin bağımsızlık zemini olarak işlev görmektedir (World Bank, 2020).

Değer boyutu, kurulan veri yönetişimi altyapısının ekonomik ve yönetsel çıktılara dönüşmesini temsil etmektedir. Veri odaklı kamu hizmetleri, dijital devlet uygulamaları, veri temelli özel sektör faaliyetleri, dijital girişimcilik ekosistemi ve veri odaklı sanayi bu sütunun temel göstergeleri arasında yer almaktadır. Bu boyut, veri yönetişiminin amacının kalkınma, rekabet gücü ve toplumsal refah üretmek olduğunu göstermektedir. Böylece veri yönetişimi, uzun vadeli ekonomik ve yönetsel kapasite inşasının temel politika araçlarından biri haline gelmektedir (World Bank, 2020).

Dünya Bankası'nın geliştirdiği bu tanı modeli, veri yönetişimini teknik altyapıdan hukuki güvenlik mekanizmalarına ve ekonomik çıktılara uzanan çok katmanlı yönetim sistemi olarak ele almaktadır. Ülkelerin veri politikalarını parçalı düzenlemeler yerine bir mimari çerçeve içinde inşa etmeleri gerektiğini ortaya koymaktadır. Bu yaklaşım, veri yönetişimini modern devlet kapasitesinin ve dijital egemenliğin temel unsurlarından biri olarak konumlandırmaktadır (World Bank, 2020).

3.2.6. DCAM Çerçevesi

Veri yönetimi uygulamalarının kurumsal düzeyde sistematik ve sürdürülebilir bir biçimde yürütülmesini sağlamak amacıyla Veri Yönetimi Yeteneği Değerlendirme Modeli (Data Management Capability Assessment Model, DCAM) Çerçevesi geliştirilmiştir. Model, veri yönetimi faaliyetlerini stratejik, organizasyonel ve operasyonel boyutlarıyla ele alarak kurumların veri yönetimi yetkinliklerini geliştirmeyi amaçlamaktadır (EDM Association, 2025).



Şekil 17. DCAM v3 çerçevesi (EDM Association, 2025)

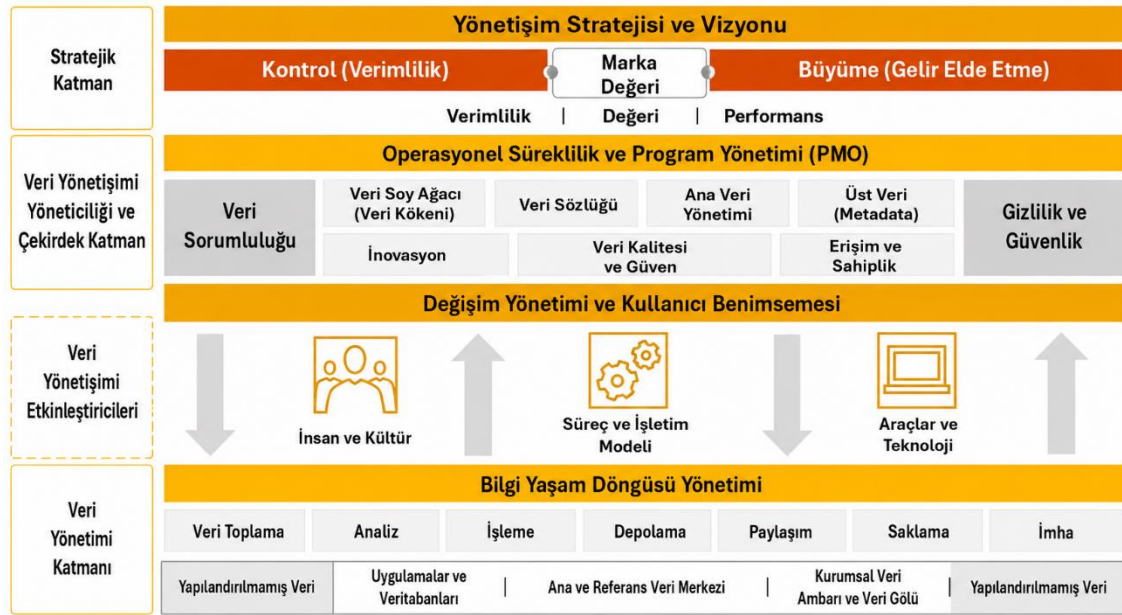
EDM Konseyi tarafından geliştirilen DCAM v3, modelin önceki sürümlerinin önemli bir evrimini temsil etmektedir. Veri, günümüzde yapay zeka uygulamalarından bulut stratejilerine, düzenleyici uyumluluk süreçlerinden sürdürülebilirliğe kadar birçok kritik kurumsal faaliyetin temelini oluşturmaktadır (EDM Association, 2025).

Modelde veri yönetimi ve veri güvenliği konularına daha güçlü bir vurgu yapılmıştır. Kurumların artan düzenleyici yükümlülükleri, veri gizliliği ve veri güvenliği gibi konuların veri yönetimi çerçevelerinde daha kapsamlı şekilde ele alınmasını gerektirmektedir. DCAM, kurumların veri odaklı bir kültür geliştirmelerine katkı sağlayan stratejik bir araç olarak değerlendirilmektedir. Model kapsamında gerçekleştirilen değerlendirmeler, kurumların veri yönetimi olgunluk seviyelerini belirlemelerine ve veri yönetimi uygulamalarını geliştirmek için gerekli yol haritalarını oluşturmalarına olanak tanımaktadır. Bu yönüyle DCAM, veri odaklı organizasyonların oluşturulmasında ve veri temelli karar verme süreçlerinin güçlendirilmesinde önemli bir referans çerçevesi olarak kabul edilmektedir (EDM Association, 2025).

3.2.7. PwC Kurumsal Veri Yönetişimi Çerçevesi

PwC tarafından geliştirilen kurumsal veri yönetişimi çerçevesi, kurumların veri varlıklarını etkin yönetebilmesi, riskleri azaltabilmesi ve veriden değer üretebilmesi amacıyla tasarlanmıştır. Bu çerçeve, organizasyonun tüm veri ekosistemini kapsayacak şekilde dört temel katmandan oluşmaktadır (Bkz. Şekil 18).

Stratejik katman, veri yönetişiminin kurumsal hedeflerle hizalanmasını sağlayarak verimlilik (kontrol) ve değer üretimi (büyüme) arasında denge kurmayı ve performans göstergeleri aracılığıyla yönetim çıktılarının ölçülmesini mümkün kılmaktadır. Bu stratejik yönelim, veri yönetişimini bir kontrol mekanizması olmaktan çıkarıp kurumsal değer yaratma aracına dönüştürmektedir. Çekirdek katman ise veri sorumluluğu, veri kalitesi, üst veri, veri soy ağacı, ana veri yönetimi, erişim ve güvenlik gibi temel yönetim fonksiyonlarını kapsayarak veri üzerinde standartlaşma, güven ve hesap verebilirlik sağlamaktadır. Bu katman aynı zamanda program yönetimi ve değişim yönetimi süreçleriyle desteklenerek yönetişimin kurumsal ölçekte sürdürülebilirliğini güçlendirmektedir. Veri yönetişimi etkinleştiricileri katmanı, insan ve kültür, süreç ve işletim modeli ile araç ve teknoloji boyutlarını bir araya getirerek yönetişimin organizasyonel bir dönüşüm gerektirdiğini ortaya koymaktadır. Son olarak veri yönetimi katmanı, verinin yaşam döngüsü boyunca (toplama, işleme, depolama, paylaşım, saklama ve imha) sistematik biçimde yönetilmesini sağlayarak yönetim ilkelerinin operasyonel düzeyde uygulanmasına olanak tanımaktadır. PwC çerçevesinin veri yönetişimini kurumun tüm katmanlarına entegre eden kapsamlı ve uygulanabilir bir model sunduğunu göstermektedir (PwC, 2019).



Şekil 18. PwC veri yönetiřimi çerçevesi

3.3. ÜLKELERİN VERİ YÖNETİřİMİ ÇERÇEVELERİ

Veri yönetiřimi çerçeveslerinin kurumlara uyarlanması, organizasyonel, teknik ve kültürel boyutları içeren çeşitli zorluklar barındırmaktadır. Bu süreçte en yaygın sorunlardan biri, çerçevenin tüm bileşenlerinin aynı anda uygulanmaya çalışılması sonucu ortaya çıkan karmaşıklık ve kurumsal dirençtir. Bu nedenle veri yönetiřimi uygulamalarının aşamalı bir yaklaşımla hayata geçirilmesi ve öncelikle yüksek etki yaratabilecek alanlara odaklanması önerilmektedir. Ayrıca veri yönetiřimi hedeflerinin kurumların stratejik ve operasyonel ihtiyaçlarıyla uyumsuz olması da uygulama sürecini zorlaştırmaktadır. Bu durumun aşılabilmesi için iş birimleri ve ilgili paydaşların sürece aktif biçimde dahil edilmesi ve veri yönetiřimi hedeflerinin kurumsal stratejik amaçlarla uyumlu hale getirilmesi gerekmektedir (Smith, 2025).

Veri yönetiřimi uygulamalarında düzenleyici gerekliliklerin karmaşıklığı da önemli bir zorluk oluşturmaktadır. Bu nedenle veri politikalarının oluşturulmasında hukuk ve uyum birimleriyle iş birliği yapılması gerekmektedir (Smith, 2025). Nitekim Marcucci vd. (2023) tarafından gerçekleştirilen karşılaştırmalı analiz, küresel veri yönetiřimi çerçeveslerinde önemli kavramsal ve kurumsal boşluklar bulunduğunu göstermektedir. İncelenen 58 ülkenin yarısının yönettiği veri türünü açık biçimde tanımladığı, %24'ünün

veri yaşam döngüsünü kapsamlı ele aldığı ve sadece %22,4'ünde veri yönetişimi birimlerinin bulunduğu görülmektedir. Ayrıca veri sahiplerinin politika geliştirme süreçlerine katılım oranının %5 olması, yönetişim mekanizmalarının katılımcılık açısından da sınırlı kaldığını ortaya koymaktadır. Bu bulgular, küresel veri yönetişiminin temel sorununun kavramsal uyum eksikliği ve kurumsal kapasite yetersizliği olduğunu göstermektedir (Marcucci vd., 2023).

Kurumsal düzeyde karşılaşılan diğer zorluklar arasında teknolojik araçların veri yönetişimi çerçevesiyle uyumsuzluğu, kurumsal kültürden kaynaklanan direnç ve nitelikli insan kaynağı eksikliği yer almaktadır. Bu sorunların aşılması için mevcut teknolojik altyapının süreçlere uyarlanması, veri yönetişiminin kurumsal karar alma süreçlerini destekleyen bir araç olarak konumlandırılması ve veri yönetimi, veri kalitesi, veri güvenliği ile veri okuryazarlığı alanlarında personel yetkinliklerinin geliştirilmesi gerekmektedir. Ayrıca veri yönetişimi programlarının kurum genelinde tutarlı biçimde uygulanabilmesi için üst yönetim desteği ve performans göstergeleri önemli bir rol oynamaktadır (Smith, 2025).

Benzer eğilimler ülke düzeyinde de görülmektedir. Chen (2021) tarafından gerçekleştirilen Küresel Veri Düzenlemesi Teşhisi çalışması, 80 ülkeyi kapsayan analizinde veri yönetişimi düzenlemelerinin henüz olgunlaşma aşamasında olduğunu ortaya koymaktadır. Çalışmaya göre ülkeler veri korumaya yönelik önlemlerin yaklaşık %41'ini, veri kullanımını kolaylaştıran politikaların ise %47'sini uygulamaya almış durumdadır. Yüksek gelirli ülkeler görece daha iyi performans sergilese de hiçbir gelir grubunun tam anlamıyla gelişmiş bir düzenleyici çerçeveye sahip olmadığı görülmektedir. Bu durum, küresel veri yönetişimi alanındaki temel sorunun mevzuat eksikliğinden ziyade uygulama derinliği ve kurumsal kapasite yetersizliği olduğunu göstermektedir (Chen, 2021).

Bu bulgular, ülkelerin veri yönetişimi alanında mevzuat oluşturma konusunda belirli bir ilerleme kaydetmiş olmalarına karşın, düzenlemelerin sağlamlığı ve uygulamayı destekleyen kurumsal kapasite bakımından önemli eksiklikler bulunduğunu ortaya koymaktadır. Başka bir ifadeyle küresel veri yönetişimi alanındaki temel sorun, mevzuat eksikliğinden ziyade uygulama derinliği, kurumsal koordinasyon ve sürdürülebilir

yönetişim mekanizmalarının yetersizliğidir. Bu doğrultuda, aşağıdaki bölümde çalışma kapsamında ele alınan ABD, AB, Avustralya, BK ve Türkiye'nin veri yönetişimi yaklaşımları incelenerek bu ülkelerin veri yönetişimi çerçeveleri karşılaştırmalı olarak ortaya konulmuştur. Bu ülkeler üniversitelerde veri yönetişimi uygulamalarının yaygınlığı ve politika olgunluğu nedeniyle seçilmiştir.

3.3.1. ABD Yaklaşımı

ABD veri yönetişimi yaklaşımında politika ve uygulama araçları, veri yönetişimi süreçlerini standartlaştırmak, veri kalitesini artırmak ve açık veri ekosistemini güçlendirmek amacıyla geliştirilen kapsamlı rehberler ve çerçeveler üzerinden şekillenmektedir. Bu kapsamda, açık veri uygulamalarına ilişkin temel ilkeler Açık Devlet Verisine İlişkin Açıklamalı Sekiz İlke³⁵ gibi kaynaklarla belirlenirken, kamu kurumlarının veri yönetişimi süreçlerini olgunlaştırmasına yönelik Veri Yönetişimi Rehberi³⁶, Veri Becerilerinin Değerlendirilmesi Rehberi³⁷ ve Veri İnovasyonu Etkinlik Rehberi³⁸ gibi uygulama rehberleri önemli bir rol oynamaktadır. Veri etiği ve sorumlu veri kullanımı ise Veri Etiği Çerçevesi³⁹ ile desteklenerek, kamu kurumlarında etik karar alma süreçlerinin güçlendirilmesi hedeflenmektedir. Bunun yanı sıra, veri güvenliği ve siber güvenlik boyutu, özellikle Sıfır Güven Federal Veri Güvenliği Rehberi⁴⁰ gibi rehberlerle ele alınmakta ve sıfır güven yaklaşımı doğrultusunda veri koruma mekanizmaları geliştirilmektedir.

Kurumsal yapıların oluşturulması ve yönetim süreçlerinin standartlaştırılması açısından çeşitli şablon ve rehber dokümanlar da dikkat çekmektedir. Veri Becerileri Danışma Grubu Tüzüğü Şablonu⁴¹ ve Baş Veri Yöneticisi Ofisi Şablonu⁴² gibi araçlar, kurumların veri yönetişimi organizasyonlarını yapılandırmalarına yardımcı olmaktadır. Ayrıca, veri kalitesi ve yaşam döngüsü yönetimine ilişkin standartlar Federal İstatistiksel Yöntemler

³⁵ Bkz. <https://opengovdata.org/>

³⁶ Bkz. Bkz. <https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf>

³⁷ Bkz. <https://resources.data.gov/assets/documents/assessing-data-skills-playbook.pdf>

³⁸ Bkz. Bkz. <https://resources.data.gov/assets/documents/data-innovation-event-playbook.pdf>

³⁹ Bkz. <https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf>

⁴⁰ Bkz. https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf

⁴¹ Bkz. [https://resources.data.gov/assets/documents/DA-CoE-Data-Governance-Advisory-Group-\(DGAG\)-Charter-Template.pdf](https://resources.data.gov/assets/documents/DA-CoE-Data-Governance-Advisory-Group-(DGAG)-Charter-Template.pdf)

⁴² Bkz. <https://resources.data.gov/categories/data-management-governance/>

Komitesi (FCSM) Veri Kalitesi Çerçevesi⁴³ ile tanımlanırken, veri kullanımının web ortamında etkin ve sürdürülebilir şekilde gerçekleştirilmesine yönelik ilkeler Web Üzerinde Veri İçin En İyi Uygulamalar⁴⁴ tarafından ortaya konmaktadır.

ABD’de veri yönetişimi uygulamalarının izlenmesi ve şeffaflığın sağlanması ise Data.gov Gösterge Paneli⁴⁵ gibi platformlar aracılığıyla gerçekleştirilmektedir. Bu sayede kurumların açık veri politikalarını uygulama düzeyleri takip edilebilmektedir. Kamuya açık veri erişimi ve katılım süreçleri Bilgi Edinme Özgürlüğü (FOIA) Yasası⁴⁶ ve ABD Kamu Katılımı Rehberi⁴⁷ gibi araçlarla desteklenirken, açık veri etkileşimini artırmaya yönelik rehberler (Açık Veri Katılımı Rehberi⁴⁸) ve veri federasyonu girişimleri (ABD Veri Federasyonu⁴⁹) kurumlar arası veri paylaşımını kolaylaştırmaktadır.

ABD’nin veri yönetişimi için attığı en büyük temellerden bir tanesi 2018 yılında hazırlıklarına başlanan Federal Veri Stratejisi⁵⁰ (Federal Data Strategy), ABD federal hükümetinin veriyi kamu hizmetleri, politika üretimi ve toplumsal fayda için stratejik bir varlık olarak kullanmasını hedeflemektedir. Strateji, federal kurumların veri yönetişimi, veri paylaşımı ve veri kullanımını geliştirmek amacıyla ortak ilkeler, uygulamalar ve yıllık eylem planları içeren uzun vadeli bir yol haritası oluşturmaktadır (Federal Data Strategy, t.y.-b). Stratejiye dayanarak oluşturulan 2020 Eylem Planı⁵¹ ve 2021 Eylem Planı⁵², 10 yıllık vizyonu ortaya koymuştur. Bu planlar, federal kurumların veriyi stratejik bir kamu varlığı olarak yönetmesini desteklemek amacıyla veri yönetişimi yapılarının kurulması, veri altyapısının geliştirilmesi, veri becerilerinin artırılması, veri envanterlerinin oluşturulması ve açık veri uygulamalarının yaygınlaştırılması gibi faaliyetleri içermektedir (Federal Data Strategy, 2020a; Federal Data Strategy, 2021).

2020 Eylem Planı, veri yönetişimi için gerekli kurumsal yapıların oluşturulması, veri envanterlerinin hazırlanması ve veri yönetişimi kapasitesinin geliştirilmesi gibi temel

⁴³ Bkz. https://nces.ed.gov/FCSM/pdf/FCSM.20.04_A_Framework_for_Data_Quality.pdf

⁴⁴ Bkz. <https://www.w3.org/TR/dwbp/>

⁴⁵ Bkz. <https://catalog.data.gov/dataset/>

⁴⁶ Bkz. <https://www.foia.gov/>

⁴⁷ Bkz. <https://digital.gov/guides/public-participation/>

⁴⁸ Bkz. <https://resources.data.gov/resources/odeg/>

⁴⁹ Bkz. <https://resources.data.gov/resources/us-data-federation/>

⁵⁰ Bkz. <https://strategy.data.gov/>

⁵¹ Bkz. <https://strategy.data.gov/assets/docs/2020-federal-data-strategy-action-plan.pdf>

⁵² Bkz. <https://strategy.data.gov/assets/docs/2020-federal-data-strategy-action-plan.pdf>

faaliyetlere odaklanmaktadır (Federal Data Strategy, 2020a). 2021 Eylem Planı bu altyapının geliştirilmesini ve veri yönetiřimi süreçlerinin kurumsal karar alma mekanizmalarına daha etkin řekilde entegre edilmesini amaçlamaktadır (Federal Data Strategy, 2021). Bu nedenle 2020 planı veri yönetiřiminin kuruluş aşamasını temsil ederken, 2021 planı veri yönetiřiminin olgunlařtırılması ve kurumsallařtırılması sürecini ifade etmektedir.

Yine Federal Veri Stratejisi kapsamında geliştirilen Veri Yönetiřimi Rehberi (Data Governance Playbook), veri yönetiřimini verinin stratejik bir varlık olarak yönetilmesine yönelik kurumsal bir süreci tanımlamaktadır. Kılavuzda veri yönetiřimi yapılarının oluşturulması, veri envanterlerinin geliştirilmesi, veri yönetiřimi politikalarının belirlenmesi ve veri kültürünün güçlendirilmesi gibi unsurları veri yönetiřiminin temel bileřenleri olarak ele almaktadır. Bu yaklaşım, federal kurumlarda verinin sistematik biçimde yönetilmesini ve veri temelli karar alma süreçlerinin geliştirilmesini sağlamaktadır (Federal Data Strategy, 2020b).

Federal Veri Stratejisi kapsamında geliştirilen DOL Veri Stratejisi, veri yönetiřimi faaliyetlerini uyumlařtırmak, veri yönetiřimini geliřtirmek ve verinin karar alma süreçlerinde daha etkin kullanılmasını saęlamayı amaçlamaktadır. Bu amaç doęrultusunda veri, kurum içindeki operasyonlar, politika geliřtirme süreçleri ve program yönetimi için kritik bir kaynak olarak görölmektedir (U.S. Departman of Labor, t.y).



Şekil 19. DOL veri stratejisi (U.S. Departman of Labor, t.y).

Şekil 19'da ABD Çalışma Bakanlığı tarafından hazırlanan Kurumsal Veri Stratejisi⁵³ (Enterprise Data Strategy), yaklaşımda veri, kurumun faaliyetlerini destekleyen stratejik bir kurumsal varlık olarak ele alınmakta ve veri yönetişiminin geliştirilmesi için FAIR veri ilkeleri (verinin bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olması) temel rehber olarak benimsenmektedir. Strateji ayrıca verinin varsayılan olarak açık olması, anlaşılabilir ve amaca uygun şekilde yönetilmesi, öngörülebilir biçimde erişilebilir hale getirilmesi ve kurum genelinde stratejik bir varlık olarak kullanılması gibi hedefler belirlemektedir. Bunun yanında veri kalitesinin artırılması, veri mimarisinin geliştirilmesi, veri analitiği kapasitesinin güçlendirilmesi ve veri alanında uzman insan kaynağının geliştirilmesi gibi alanlar veri yönetişiminin güçlendirilmesi için öncelikli iyileştirme alanları olarak tanımlanmaktadır. Bu çerçevede DOL veri stratejisi, verinin kamu programlarının etkinliğini değerlendirmek, politika geliştirme süreçlerini desteklemek ve kamu hizmetlerinin daha etkili sunulmasını sağlamak amacıyla kullanılmasını hedefleyen veri temelli bir yönetim anlayışını yansıtmaktadır (U.S. Departman of Labor, t.y).

⁵³ Bkz. <https://www.dol.gov/sites/dolgov/files/Data-Governance/DOL-Enterprise-Data-Strategy.pdf>

Kurumların kurumsal bir varlık olarak yöneten veri yönetişimi yaklaşımı geliştirmesi için geliştirilen Sıfır Güven Federal Veri Güvenliği Rehberi, veri yönetişimi ile siber güvenlik süreçlerini birleştirerek verinin yaşam döngüsü boyunca yönetilmesini sağlamaktır. Veri yönetişimi açısından bakıldığında ilk olarak, verinin tanımlanması ve envanterinin oluşturulması veri yönetişiminin temel adımı olarak ele alınmaktadır. Kurumların sahip oldukları tüm veri varlıklarını belirlemesi, bunları kataloglaması ve sınıflandırması gerektiği belirtilmektedir. İkinci olarak, verinin güvenliğinin veri yaşam döngüsünün tüm aşamalarına entegre edilmesi gerektiğini belirtmektedir. Sıfır Güvenlik (Zero Trust, ZT) yaklaşımına göre güvenlik ağın çevresini korumak yerine doğrudan verinin kendisine odaklanmalıdır. Bu nedenle veri yönetişimi süreçleri veri tasarımından depolanmasına, paylaşımından imhasına kadar tüm aşamalarda güvenlik, erişim kontrolü ve risk yönetimini içermelidir. Üçüncü belge, veri yönetişimi rollerinin ve kurumsal sorumlulukların açık biçimde tanımlanmasını önermektedir. Veri yönetişimi kurulları, veri sorumluları (data steward) gibi roller veri varlıklarının yönetiminde birlikte çalışmalıdır. Veri sorumluları veri varlıklarının tanımlanması, sınıflandırılması ve risklerinin değerlendirilmesinde kilit aktörler olarak görülmektedir (Federal CDO Council vd., 2025).

ABD federal kurumlarında verinin etik, sorumlu ve hesap verebilir biçimde yönetilmesini sağlayan Veri Etiği Çerçevesi şeffaflık, hesap verebilirlik ve kamu yararı gibi yönetim değerleriyle ilişkilendiren bir yaklaşım sunmaktadır. Veri yönetişimi açısından en önemli katkısı, veri faaliyetlerinin veri yaşam döngüsünün tüm aşamalarında (toplama, işleme, paylaşma, kullanma, depolama ve imha) etik ve yönetsel ilkelerle yürütülmesi gerektiğini vurgulamasıdır. Veri yönetişimini destekleyen yedi temel ilke arasında yasal düzenlemelere ve etik standartlara uyma, kamu yararını gözetme, mahremiyet ve gizliliği koruma, dürüstlük ve bütünlükle hareket etme, hesap verebilirlik sağlama, şeffaflığı teşvik etme ve veri yönetimi ile veri bilimi alanındaki gelişmeleri takip etme yer almaktadır (Federal Data Strategy, t.y.-a).

ABD’de veri yönetişimi yaklaşımı, farklı alanlarda yürürlüğe konulmuş çok sayıda federal yasa ve düzenlemenin oluşturduğu kapsamlı bir hukuki çerçeveye dayanmaktadır. Federal kurumların veri toplama, yönetme, paylaşma ve kullanma süreçleri özellikle mahremiyet, veri güvenliği, veri kalitesi ve şeffaflık ilkeleri doğrultusunda

düzenlenmiştir. ABD'nin GDPR'ye benzer olarak nitelendirilebilecek 1974 Gizlilik Yasası, federal kurumlarda kişisel verilerin toplanması, saklanması, kullanımı ve yayılmasına Adil Bilgi Uygulama İlkeleri (FIPP'ler) (Fair Information Practice Principles, FIPPs) ile sağlamaktadır. Yasa, kurumların veriyi yasal amaçlarla toplamasını ve korumasını zorunlu kılmaktadır. Bireylerin kendileriyle ilgili hangi kayıtların tutulduğunu bilmesini ve verilere erişim ve düzeltme hakkı sağlamaktadır. Eğer herhangi bir bireye ait veri amaçları dışında kullanılacaksa amaç dışı kullanımı için rıza gerektirmektedir (United States Department Of Justice, 2020, s. 1-3).

Gizlilik Yasası, kurumların *ilgili ve gerekli* verileri tutmasını zorunlu kılarak veri minimizasyonu⁵⁴ ilkesini benimsemektedir. Bilgilerin mümkün olduğunca doğrudan bireyden toplanmasını ve veri toplama sırasında bireyin bilgilendirilmesini şart koşarak şeffaflık ve veri kalitesi mekanizmaları kurmaktadır (United States Department Of Justice, 2020, s. 155-156). Ayrıca kurumların tuttukları kayıtları doğru, ilgili, güncel ve tam biçimde muhafaza etmesi ve verileri yaymadan önce gözden geçirmesi gerekmektedir. Bunun yanında Federal Resmî Gazete⁵⁵'ye (Federal Register) göre her kurum kişisel veri içeren her kayıt için Sistem Kayıt Bildirimi⁵⁶ (System of Records Notice (SORN)) yayımlaması zorunlu tutulmuştur. Bu bildirimlerde veri kategorileri, kullanım amaçları, erişim kontrolleri, saklama ve imha politikaları ile sorumlu yetkililerin açıkça belirtilmesi istenmiştir (United States Department Of Justice, 2020, s. 167-168).

Bir diğer uygulama, federal kurumların kişisel veri içeren bilgi sistemleri için Gizlilik Etki Değerlendirmesi (Privacy Impact Assessment, PIA) gerçekleştirmesi E-Devlet Yasası⁵⁷ (E-Government Act) ile zorunlu kılınmıştır. Kanun, veri toplama, veri kullanımı ve veri paylaşım süreçlerinin sistematik biçimde değerlendirilmesini öngörmektedir. Ayrıca bu değerlendirmelerin BT Yöneticisi (Chief Information Officer) tarafından incelenmesi ve mümkün olduğunda kamuya açıklanması, veri yönetiminde şeffaflık ve

⁵⁴ Belirli bir amaç için gerekli olan kişisel bilgilerin gerekli miktarda toplanması, işlenmesi ve saklanması ilkesidir.

⁵⁵ Federal Resmî Gazete ABD federal hükümetinin resmî günlük yayımlama gazetesidir. Federal kurumlar yeni düzenlemeleri, önerilen kuralları, bildirimleri ve kamuya açıklanması gereken önemli kararları burada yayımlar.

⁵⁶ Federal kurumların kişisel veri içeren kayıt sistemlerini kamuya ilan ettiği resmî bildirimdir. Gizlilik Yasası kapsamında şeffaflık ve hesap verebilirliğin temel aracıdır.

⁵⁷ Bkz. <https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

hesap verebilirliği güçlendirmektedir. Kanun ayrıca kurum genelinde bilgi güvenliği programlarının oluşturulmasını ve kayıt yönetimi stratejilerinin geliştirilmesini zorunlu kılarak veri güvenliği, veri yönetimi ve bilgi erişimi gibi veri yönetişiminin bileşenlerini desteklemektedir (United States Department Of Justice, 2002).

3.3.2. AB Yaklaşımı

AB son on yıl içerisinde kamu politikalarının hazırlanması, uygulanması ve değerlendirilmesinde veri odaklı karar verme süreçlerini güçlendirmek amacıyla kurumsal ölçekte bir veri yönetişimi çerçevesi geliştirmiştir. Bu çerçeve, dijital dönüşüm stratejisinin temel bileşeni olup, kurumları veri ile çalışan yapıdan veri tarafından yönlendirilen bir organizasyona dönüştürmeyi hedeflemektedir. AB, veri yönetişimini politik, stratejik, yönetsel ve operasyonel olarak görmektedir (European Commission, 2020a).

Dijital dönüşüm vizyonunun temel bileşenlerinden biri olan Avrupa Veri Stratejisi⁵⁸, 2030 yılına kadar küresel ölçekte rekabetçi, veri merkezli ve insan odaklı bir dijital ekosistem haline getirmeyi hedeflemektedir. Strateji'nin temel kaynaklarından biri olan Avrupa Veri Yönetişimi Yasası⁵⁹ (DGA) ile birlikte çoğunlukla dağınık platformlarda ve uyumsuz formatlarda bulunana kamu verisinin tüm ekonomik sektörlerde ve kamu politikalarında dönüştürücü rolünü kullanmak amacıyla ortak veri alanları⁶⁰ oluşturulması ve geliştirilmesini hedeflemektedir. Ortak veri alanlarının verinin bulunabilir, erişilebilir, birlikte çalışabilir, yeniden kullanılabilir ilkelerine dayanması öngörülmektedir. Stratejinin merkezinde yer alan açıklık ve koruma ilkeleri, sürekli bir denge arayışına işaret etmektedir. Aynı zamanda, dijital egemenlik⁶¹ (digital sovereignty) söylemi, AB üyesi ülkelerin mevcut altyapı kapasitelerindeki farklılıklar ve ulusal çıkar öncelikleri nedeniyle birlik düzeyinde tam uyumun sağlanmasını zorlaştırmaktadır. Rekabetin kolaylaşması, kişisel verilerin korunması, ticari sırların güvenliği ve rekabetin

⁵⁸ Bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>

⁵⁹ Bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>

⁶⁰ AB'nin dijital stratejisi kapsamında geliştirilen ve farklı sektörlerde üretilen verilerin güvenli, birlikte çalışabilir ve kontrollü biçimde paylaşılmasını sağlayan ortak bir dijital ekosistem modelidir. Parçalanmış veri ortamlarını birbiriyle konuşabilen ve ortak kurallarla yönetilen bir yapıya dönüştürmektedir.

⁶¹ AB'nin dijital altyapılar, veri akışları, dijital platformlar, yapay zekâ ve bulut hizmetleri gibi temel dijital kaynaklar üzerinde bağımsız karar alma, düzenleme, kontrol etme ve yönlendirme kapasitesine sahip olması anlamına gelmektedir.

bozulmaması için veri aracılık hizmetleri⁶² ve veri altruizm⁶³ mekanizmaları geliştirmiştir. Daha öncesinde AB, ile kişisel verilerin korunmasını 2016 yılında kabul edilen ve 2018 yılında yürürlüğe giren GDPR temel haklar çerçevesinde güvence altına almıştır. GDPR ve DGA aynı veri ekosisteminin farklı boyutlarına müdahale etmektedir (European Commission, 2020b; European Parliament and Council of the European Union, 2016, 2022).

DGA ve Avrupa Veri Stratejisi'nin bahsi geçen veri alanlarının teknik ve hukuki temelini sağlama tamamlayıcı düzenlemelerden olan Kişisel Olmayan Verilerin Serbest Dolaşımına İlişkin Çerçeve Hakkında Tüzük⁶⁴, veri yönetişimi vizyonunda veri serbestisi, güvenlik, şeffaflık üçlüsünü kurumsallaştırmaktadır. Aynı zamanda GDPR'nin kapsamı dışında kalan kişisel olmayan verilerin serbest dolaşımı için bir çerçeve oluşturmaktadır. Tüzük, dijital tek pazarın işleyişini güçlendirmek üzere, üye devletler arasında veri yerelleştirme gerekliliklerini ortadan kaldırmayı ve veri hareketliliğini artırmayı hedeflemektedir (The European Parliament and of The Council, 2018).

AB'nin veri yönetişimi yaklaşımı, kamu verilerinin ekonomik ve toplumsal değerini artırmayı amaçlayan açık veri politikaları, veri erişimi, yeniden kullanım ve veri koruma ilkeleri üzerine kuruludur. Avrupa Parlamentosu ve Konseyinin 2019/1024 sayılı Açık Veri ve Kamu Sektörü Bilgilerinin Yeniden Kullanımı Direktifi⁶⁵, kamu sektörü tarafından üretilen verilerin mümkün olduğunca geniş ölçekte yeniden kullanılmasını teşvik ederek veri temelli yenilik ve ekonomik büyümeyi desteklemeyi amaçlamaktadır. Direktife göre kamu sektörü verileri, uygun teknik araçlar ve standartlar aracılığıyla erişilebilir hale getirilmeli, mümkün olduğunda açık ve makine tarafından okunabilir formatlarda sunulmalı ve yeniden kullanım için gerekli koşullar şeffaf, ayrımcı olmayan ve orantılı olmalıdır. Bununla birlikte AB veri yönetişimi yaklaşımı kişisel verilerin korunması ve veri güvenliğinin sağlanmasını da temel bir ilke olarak benimsemektedir. (The European Parliament ve The Council of The European Union, 2019).

⁶² Verinin sahibi ile veri kullanıcısı arasında köprü görevi gören, veriyi kendisi kullanmayan kurumsal aktördür. Bu kavram, AB Veri Yönetimi Yasası ile hukuki statü kazanmıştır.

⁶³ Kişilerin veya kurumların kendi verilerini kamu yararı için gönüllü olarak paylaşması esasına dayanan yeni bir veri yönetişimi modelidir.

⁶⁴ Bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>

⁶⁵ Bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024&qid=1772716573669>

3.3.3. Avustralya

Avustralya kamu sektöründe veri yönetişimini güçlendirmeye yönelik olarak geliştirilen temel kaynaklar, kurumsal kapasiteyi artırma, standartlaştırma ve güven temelli veri kullanımını sağlama amacıyla bir yapı sunmaktadır. Bu kapsamda, Avustralya Ulusal Denetim Ofisi tarafından yayımlanan içgörü denetim raporları⁶⁶, veri yönetişimi uygulamalarına ilişkin önemli yönetim dersleri sunarken Avustralya Kamu Hizmeti Komisyonu tarafından geliştirilen Veri Yetkinlik Çerçevesi⁶⁷, kamu personelinin veri rollerine ilişkin gerekli becerileri tanımlamaktadır. Veri profesyonellerine yönelik Avustralya Kamu Hizmeti Komisyonu tarafından hazırlanan kariyer yolları ve veri uzmanlığı⁶⁸, kamu kurumlarında veri odaklı insan kaynağının geliştirilmesini desteklemektedir. Bunun yanı sıra, Avustralya Hükümeti Veri Kataloğu⁶⁹, kamu verilerinin bulunabilirliğini ve erişilebilirliğini artırarak veri paylaşımını teşvik etmektedir. Veri ve Dijital Hükümet Stratejisi⁷⁰, ülkenin dijital dönüşüm hedeflerini ortaya koyarken, Yerli Veri Yönetişimi Çerçevesi⁷¹, yerli topluluklara ait verilerin etik ve saygılı biçimde yönetilmesine yönelik ilkeleri belirlemektedir. Siber güvenlik bağlamında Bilgi Güvenliği El Kitabı⁷² ve Koruyucu Güvenlik Politikası Çerçevesi⁷³, veri güvenliğine ilişkin teknik ve yönetsel gereklilikleri düzenlemektedir. Ayrıca, Ulusal Arşivler tarafından geliştirilen kamu kayıtlarında güven inşa etmeye yönelik yaklaşımlar⁷⁴, veri kullanımında şeffaflık ve hesap verebilirliği desteklemektedir. Maliye Bakanlığı tarafından belirlenen üst düzey yönetici sorumlulukları⁷⁵ ile veri olgunluk değerlendirme araçları⁷⁶ ise kurumların veri yönetişimi kapasitelerini ölçmelerine ve geliştirmelerine olanak tanımaktadır.

⁶⁶ Bkz. <https://www.anao.gov.au/work/insights/governance-of-data>

⁶⁷ Bkz. <https://www.apsc.gov.au/publication/aps-data-capability-framework>

⁶⁸ Bkz. <https://www.apsprofessions.gov.au/data-profession>

⁶⁹ Bkz. <https://www.datacommissioner.gov.au/data-users>

⁷⁰ Bkz. <https://www.dataanddigital.gov.au/strategy>

⁷¹ Bkz. <https://www.niaa.gov.au/our-work/data-evaluation-and-research/framework-governance-indigenous-data-gid>

⁷² Bkz. <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism>

⁷³ Bkz. <https://www.protectivesecurity.gov.au/>

⁷⁴ Bkz. <https://www.naa.gov.au/information-management/information-management-policies/building-trust-public-record>

⁷⁵ Bkz. <https://www.finance.gov.au/government/public-data/public-data-policy/ses-accountabilities-data>

⁷⁶ Bkz. <https://www.finance.gov.au/government/public-data/public-data-policy/data-maturity-assessment-tool>

Avustralya'nın kamu verisinin stratejik bir ulusal varlık olarak yönetilmesi, açık veri politikalarının benimsenmesi, kurumlar arası veri paylaşımının teşvik edilmesi ve veri güvenliği ile gizlilik ilkelerinin korunması üzerine kuruludur (Australian Government, 2015). Avustralya Hükümeti tarafından yayımlanan Veri Stratejisi 2025–2029⁷⁷ (2025, s. 10), kurumların doğru veriye erişebilmesini, veriye güvenilebilmesini ve veriyi etkili biçimde kullanabilmesini sağlayacak kapsamlı ve uzun vadeli bir veri yönetim planı oluşturmaktır. Stratejinin (2025, s. 11) temel vizyonu *akıllı veri kullanımının iyi kararları desteklemesi* olarak ifade edilmekte ve veri kullanımının kamu yönetiminde kanıta dayalı politika geliştirme süreçlerini güçlendirmesi hedeflenmektedir. Strateji, veri yönetişimi yaklaşımını FAIR⁷⁸ ve CARE⁷⁹ ilkeleri aracılığıyla verinin erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olması sağlanırken aynı zamanda etik kullanım ve toplumsal fayda da gözetilmektedir. Kurumsal düzeyde veri yönetişimi ise CDO, veri yönetişimi komitesi ve veri sorumlularından oluşan ağ yapıları aracılığıyla yürütülmektedir. Bu sorumluluklar kurum genelinde veri yönetişimi uygulamalarının tutarlı biçimde uygulanmasını sağlamaktadır (Australian Government, 2025b).

Avustralya Hükümeti Veri Yönetişimi Çerçevesi, Avustralya Kamu Hizmeti genelinde veri yönetişimine ilişkin ortak bir anlayış oluşturarak kurumsal veri olgunluğunun geliştirilmesini hedeflemektedir. Bu doğrultuda, kurumların kendi ihtiyaç ve önceliklerine göre uyarlayabilecekleri temel veri yönetişimi ilkeleri sunulmaktadır. Yönetişim uygulamalarına yönelik kontrol listeleri ve ilgili politika ile kaynaklara erişim sağlayan kapsamlı bir referans yapısı oluşturulmaktadır. Ayrıca söz konusu çerçeve, Veri ve Dijital Hükümet Stratejisi⁸⁰'nin Veri ve Dijital Temeller⁸¹ misyonunu destekleyerek, verinin stratejik bir varlık olarak yönetilmesini teşvik etmektedir. Bu yönüyle çerçeve, kamu hizmetlerinde tutarlı ve bütünlük bir veri yönetişimi yaklaşımının geliştirilmesine yönelik hükümet düzeyindeki taahhüdün somut bir yansıması olarak değerlendirilmektedir (Australian Government, 2025a).

⁷⁷ Bkz. <https://www.infrastructure.gov.au/sites/default/files/documents/ditdrc-data-strategy-2025-2029.pdf>

⁷⁸ Verinin bulunabilir (Findable), erişilebilir (Accessible), birlikte çalışabilir (Interoperable) ve yeniden kullanılabilir (Reusable) olmasını hedeflemektedir.

⁷⁹ CARE ilkeleri ise özellikle yerli topluluklara ilişkin verilerin yönetiminde kolektif fayda, kontrol yetkisi, sorumluluk ve etik kullanım ilkelerini ön plana çıkarmaktadır.

⁸⁰ Bkz. <https://www.dataanddigital.gov.au/strategy>

⁸¹ Bkz. <https://www.dataanddigital.gov.au/strategy/missions/data-and-digital-foundations>

Avustralya Veri Yönetişimi Çerçevesi stratejik uyum, hukuki düzenlemeler, kurumsal roller, kültürel dönüşüm ve teknolojik altyapıyı entegre eden çok katmanlı bir politika modeli sunmakta ve kamu sektöründe sürdürülebilir veri yönetişimi için kapsamlı bir referans çerçevesi oluşturmaktadır. Çerçevenin kavramsal ve bağlamsal bölümlerine bakıldığında veri yönetişimi politikalarının temelinde hesap verebilirlik, rol ve sorumlulukların netleştirilmesi ve veri yaşam döngüsü boyunca kontrol mekanizmalarının kurulması yer almaktadır. Veri yönetişimi liderlik, süreçler, standartlar ve sürekli iyileştirme döngüsü ile desteklenen kurumsal bir yapı olarak ele alınmakta ve veri stratejileri ile doğrudan ilişkilendirilmektedir (Australian Government, 2025a, s. 5).

Çerçevede veri, finansal ve fiziksel varlıklarla eşdeğer bir kurumsal değer olarak ele alınmaktadır. Bu kapsamda politikalar veri kalitesi, erişilebilirlik, güvenlik ve yeniden kullanım gibi unsurlar üzerinden veri değerinin artırılmasını hedeflemektedir. Ayrıca kanıta dayalı karar verme, politika geliştirme ve hizmet sunumunun iyileştirilmesi gibi çıktılar, veri yönetişimi politikalarının temel gerekçeleri arasında yer almaktadır (Australian Government, 2025a, s. 7).

Strateji ve planlama boyutu, veri yönetişiminin kurumsal stratejiler ve özellikle veri stratejileri ile uyumlu olmasını zorunlu kılarken veri gizliliği ve güvenlik boyutu, yasal uyum, etik kullanım ve risk yönetimi ekseninde şekillenen güçlü bir düzenleyici çerçeveye işaret etmektedir. Organizasyonel yapı ve liderlik boyutlarında ise veri rollerinin tanımlanması ve üst yönetimin veri yönetişimindeki sorumluluğunun vurgulanması, politika uygulamalarının kurumsal sahipliğini güçlendirmektedir. Bunun yanında veri kültürü ve teknoloji boyutları, veri yönetişiminin kurallar ve süreçlerden ibaret olmadığını aynı zamanda organizasyonel davranış ve teknolojik kapasite ile desteklenmesi gerektiğini ortaya koymaktadır (Australian Government, 2025a, s. 10-15).

Avustralya’da veri yönetişimi, güçlü bir yasal ve politik çerçeve ile desteklenmektedir. Kamu kurumlarının veriyi nasıl yöneteceği, koruyacağı ve paylaşacağı bu düzenlemeler aracılığıyla belirlenmektedir. Bu kapsamda, kamu kayıtlarının oluşturulması, saklanması ve erişimine ilişkin esaslar 1983 Arşiv Yasası⁸² ile düzenlenirken istatistiksel verilerin

⁸² Bkz. <https://www.legislation.gov.au/C2004A02796/latest/text>

toplanması ve kullanımı Avustralya İstatistik Bürosu Yasası 1975⁸³ çerçevesinde yürütülmektedir. Sağlık ve refah verilerinin yönetimi Avustralya Sağlık ve Refah Enstitüsü Yasası 1987⁸⁴ ile güvence altına alınırken, ulusal veri toplama süreçlerine ilişkin temel kurallar 1905 Nüfus Sayımı ve İstatistik Yasası⁸⁵ ile belirlenmiştir. Kurumlar arası veri paylaşımını düzenleyen temel mevzuat ise Veri Erişilebilirliği ve Şeffaflık Yasası 2022⁸⁶ olup, bu düzenleme verinin güvenli ve kontrollü biçimde paylaşılmasını amaçlamaktadır. Bunun yanı sıra, yargı süreçlerine ilişkin veri yönetişimi Avustralya Federal Mahkemesi Kanunu 1976⁸⁷ kapsamında ele alınırken, kamuya ait bilgilere erişim hakkı Bilgi Edinme Özgürlüğü Yasası 1982⁸⁸ ile güvence altına alınmaktadır. Veri gizliliği ve kişisel verilerin korunmasına yönelik temel düzenleme olan 1988 tarihli Gizlilik Yasası⁸⁹, Avustralya Gizlilik İlkeleri⁹⁰ ile birlikte kişisel verilerin işlenmesine ilişkin standartları belirlemektedir. Ayrıca kritik altyapıların korunmasına yönelik hükümler Kritik Altyapı Güvenliği Yasası 2018⁹¹ ile düzenlenirken, ciddi veri ihlallerinin yönetimi ve raporlanması ise Avustralya Bilgi Komiserliği Ofisi tarafından yürütülen Bildirilmesi Gereken Veri İhlalleri Şeması⁹² kapsamında ele alınmaktadır. Bu çok katmanlı mevzuat yapısı, Avustralya'nın veri yönetişimi yaklaşımının hukuki, kurumsal ve etik boyutlarını güvence altına almaktadır.

Kamu sektöründe üretilen verilerin güvenli, şeffaf ve kamu yararına uygun biçimde paylaşılmasını düzenleyen Veri Erişilebilirliği ve Şeffaflık Yasası (Data Availability and Transparency Act) ile kurumsal ve hukuki bir çerçeveye oluşturulmuştur. Yasa, veri paylaşımı esnasında uygulanması gereken beş temel ilke⁹³ ile verilerin belirli kamu yararı amaçları doğrultusunda paylaşılabilirliğini belirtmektedir. Ulusal Veri Komiseri (National Data Commissioner), veri paylaşımı süreçlerinin izlenmesi, veri paylaşım

⁸³ Bkz. <https://www.legislation.gov.au/C2004A03450/latest/text>

⁸⁴ Bkz. <https://www.legislation.gov.au/C2004A03450/latest/text>

⁸⁵ Bkz. <https://www.legislation.gov.au/C1905A00015/latest/text>

⁸⁶ Bkz. https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/daata2022312/

⁸⁷ Bkz. <https://www.legislation.gov.au/C2004A01586/latest/text>

⁸⁸ Bkz. <https://www.legislation.gov.au/C2004A02562/latest/text>

⁸⁹ Bkz. https://www5.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

⁹⁰ Bkz. <https://www.oaic.gov.au/privacy/australian-privacy-principles>

⁹¹ Bkz. <https://www.legislation.gov.au/C2018A00029/latest/text>

⁹² Bkz. <https://www.oaic.gov.au/privacy/australian-privacy-principles>

⁹³ Proje ilkesi, kişi ilkesi, ortam ilkesi, veri ilkesi ve çıktı ilkesi. Bu ilkeler veri paylaşımının kamu yararına uygun olup olmadığının değerlendirilmesini, veriye yetkili ve uygun kişilerin erişmesini, verinin güvenli ortamlarda kullanılmasını, gerekli verinin paylaşılmasını ve veri kullanımından elde edilen çıktının kontrol altında tutulmasını sağlamayı amaçlamaktadır.

kuruluşlarının akreditasyonu, veri yönetişimi uygulamalarına ilişkin rehberlik sağlanması ve veri paylaşımıyla ilgili şikayetlerin değerlendirilmesi gibi görevleri yürütmektedir (The Office of Parliamentary Counsel, 2024).

Veri paylaşım süreçlerinin Gizlilik Yasası (Privacy Act) ile uyumlu olması zorunlu tutulmakta ve kişisel verilerin korunması için çeşitli güvenlik mekanizmaları öngörülmektedir (The Office of Parliamentary Counsel, 2024). Avustralya veri yönetişimi yaklaşımının önemli bileşenlerinden biri açık veri politikasıdır. Politika belgesine göre kamu kurumları, hassas olmayan verileri mümkün olduğunca açık veri olarak yayımlamakla yükümlüdür (Australian Government, 2015b). Bu kapsamda gerekli verinin paylaşılması, kişisel verilerin mümkün olduğunca anonimleştirilmesi ve veri kullanımının veri paylaşım anlaşmalarında belirtilen amaçlarla sınırlı olması gibi kurallar getirilmiştir. (The Office of Parliamentary Counsel, 2024).

Kamu verisinin kullanılabilirliğini artırmak, veri paylaşımının önündeki engelleri kaldırmak ve veri paylaşımında en iyi uygulamaları oluşturmak için DATA Scheme⁹⁴ adlı veri paylaşım sistemi kurulmuştur. Bu sistemde veri paylaşımı beş temel ilke, kurumsal roller ve güçlü güvenlik mekanizmaları ile yönetilmektedir. Ulusal Veri Komiseri tarafından denetlenen, kamu kurumları, üniversiteler ve diğer yetkilendirilmiş kuruluşlar arasında veri paylaşımını düzenlemektedir. Ayrıca Dataplace⁹⁵ ve Avustralya Hükümeti Veri Kataloğu gibi dijital platformlar aracılığıyla veri paylaşım süreçlerinin şeffaf ve izlenebilir olması sağlanmaktadır (Office of the National Data Commissioner, 2025).

3.3.4. Birleşik Krallık

BK'da veri yönetişimi yaklaşımı, veri sahipliği, veri paylaşımı, veri kalitesi, standartlar ve kurumsal kapasiteyi politika ve çerçeveler üzerinden şekillenmektedir. Bu kapsamda Devlet Yönetiminde Veri Sahipliği⁹⁶ ve Veri Paylaşımı Yönetişim Çerçevesi⁹⁷ gibi belgeler, kamu kurumları arasında verinin etkin, güvenli ve sorumlu biçimde

⁹⁴ Bkz. <https://www.datacommissioner.gov.au/data-scheme>

⁹⁵ Bkz. <https://www.dataplace.gov.au/>

⁹⁶ Bkz. <https://www.gov.uk/government/publications/essential-shared-data-assets-and-data-ownership-in-government/data-ownership-in-government-html>

⁹⁷ Bkz. <https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework>

paylaşılmasına yönelik ilkeleri ortaya koyarken Ulusal Veri Stratejisi⁹⁸, BK'nin veri odaklı bir ekonomi oluşturma hedefini ve veri kullanımına yönelik kamu güveninin artırılmasını temel bir politika amacı olarak belirlemektedir.

Veri kalitesinin artırılmasına yönelik olarak geliştirilen Devlet Veri Kalitesi Çerçevesi⁹⁹ ve Veri Kalitesi Eylem Planı¹⁰⁰, kamu sektöründe veri kalitesinin ölçülmesi, izlenmesi ve iyileştirilmesine yönelik sistematik bir yaklaşım sunmaktadır. Bunun yanı sıra, Veri Standartları Kurumu Stratejisi¹⁰¹ ve ilgili operasyonel model belgeleri, hükümet genelinde ortak veri standartlarının benimsenmesini sağlayarak veri bütünlüğünü ve birlikte çalışabilirliği güçlendirmeyi hedeflemektedir. Kurumsal kapasitenin geliştirilmesi ise Devlet Veri Olgunluğu Merkezi¹⁰² ve Veri Olgunluk Değerlendirme Çerçevesi¹⁰³ aracılığıyla desteklenmekte, kamu kurumlarının veri ekosistemlerini değerlendirmesi ve iyileştirmesi sağlanmaktadır. Ayrıca, Devlet Dijital ve Veri Meslek Yeterlilik Çerçevesi¹⁰⁴ ile insan kaynağına yönelik yetkinlikler tanımlanırken, Veri ve Yapay Zeka Etik Çerçevesi¹⁰⁵ veri kullanımında etik, şeffaflık ve hesap verebilirlik ilkelerini güçlendirmektedir. BK'nin veri yönetişimi yaklaşımının stratejik, kurumsal ve etik boyutları entegre eden gelişmiş bir politika ekosistemine dayandığını göstermektedir.

BK'nin veri yönetişimi yaklaşımı, veriyi ekonomik büyüme, inovasyon ve kamu hizmetlerinin geliştirilmesi için stratejik bir kaynak olarak ele alan bir politika çerçevesine dayanmaktadır. BK Ulusal Veri Stratejisi veri yönetişimini hayata geçirmek için beş temel politika hedefi belirlemiştir. Bunlar verinin ekonomik değerinin açığa çıkarılması, güvenilir ve büyümeyi destekleyen bir veri düzenleyici çerçevenin oluşturulması, kamu sektöründe veri kullanımının dönüştürülmesi, veri altyapısının güvenliğinin sağlanması ve uluslararası veri akışının desteklenmesidir (Department for Digital, Culture, Media ve Sport, 2020).

⁹⁸ Bkz. https://data.parliament.uk/DepositedPapers/Files/DEP2020-0521/UK_National_Data_Strategy.pdf

⁹⁹ Bkz. <https://www.gov.uk/government/publications/the-government-data-quality-framework>

¹⁰⁰ Bkz. <https://www.gov.uk/government/publications/implementing-a-data-quality-action-plan/data-quality-action-plan-implementation-guide>

¹⁰¹ Bkz. <https://www.gov.uk/guidance/data-standards-authority-strategy-2020-to-2023>

¹⁰² Bkz. <https://www.gov.uk/government/collections/data-maturity-assessment-for-government>

¹⁰³ Bkz. <https://www.gov.uk/government/publications/data-maturity-assessment-for-government-framework/data-maturity-assessment-for-government-framework-html>

¹⁰⁴ Bkz. <https://ddat-capability-framework.service.gov.uk/>

¹⁰⁵ Bkz. <https://www.gov.uk/government/publications/data-ethics-framework/data-and-ai-ethics-framework>

Strateji kapsamında veri yönetişimi dört temel politika sütunu üzerine inşa edilmiştir. İlk olarak veri temelleri, verinin standart formatlarda tutulması, yüksek veri kalitesinin sağlanması ve verinin bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olması gibi unsurları kapsamaktadır. İkinci olarak veri becerileri boyutu, veri odaklı bir ekonomi için veri analitiği ve veri bilimi alanlarında yetkin insan kaynağının geliştirilmesini ve tüm iş gücünde veri okuryazarlığının artırılmasını öncelikli bir hedef olarak belirlemektedir. Üçüncü boyut olan veri erişilebilirliği, kamu, özel sektör ve sivil toplum kuruluşları arasında veri paylaşımının teşvik edilmesini ve veri akışının kolaylaştırılmasını içermektedir. Dördüncü boyut ise sorumlu veri kullanımı ilkesidir. Strateji, veri kullanımının hukuka uygun, güvenli, etik, hesap verebilir ve sürdürülebilir şekilde gerçekleştirilmesi gerektiğini vurgulamaktadır (Department for Digital, Culture, Media ve Sport, 2020).

3.3.5. Türkiye

Türkiye’de veri yönetişimi yapısı, tarihsel olarak kamu odaklı ve merkezi veri üretim kapasitesi üzerine inşa edilmiştir. Özellikle 2000’li yıllarla birlikte e-Devlet uygulamaları aracılığıyla verinin kamusal hizmet üretiminde stratejik bir kaynak olarak konumlandırılması, veri temelli karar alma kültürünü güçlendirmiştir. Bu dönüşüm süreci, 2003 tarihli Bilgi Edinme Hakkı Kanunu ile şeffaflık ve hesap verebilirlik ilkelerinin kurumsallaştırılması, 2005 tarihli Türkiye İstatistik Kanunu ile veri üretim ve paylaşım süreçlerinin standartlaştırılması ve kurumsal koordinasyonun sağlanması, 2016 tarihli Kişisel Verilerin Korunması Kanunu ile veri güvenliği ve mahremiyetin hukuki güvence altına alınması ve 2020 tarihli Coğrafi Bilgi Sistemleri Kanunu ile sektörel veri yönetişimi mekanizmalarının güçlendirilmesi gibi düzenlemelerle pekiştirilmiştir. Bu çerçevede Türkiye’de veri yönetişimi veri güvenliği, standartlaşma, şeffaflık, erişilebilirlik ve hesap verebilirlik ilkeleri etrafında şekillenmeye çalışmaktadır. Kamu ağırlıklı ve düzenleme temelli değerlendirilmektedir (Eroğlu, 2025).

Türkiye’de veri yönetişimi alanındaki son yıllardaki gelişmeler özellikle kişisel verilerin korunması, dijital dönüşüm politikaları ve yapay zeka stratejileri doğrultusunda ivme

kazanmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)¹⁰⁶, kişisel verilerin işlenmesine ilişkin temel ilkeleri tanımlayarak veri koruma alanında önemli bir hukuki çerçeve oluşturmuştur. Bunun yanında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda geliştirilen Ulusal Yapay Zeka Stratejisi¹⁰⁷, kaliteli veriye erişim, veri paylaşımı ve teknik altyapı geliştirme hedeflerini öncelikli stratejik alanlar arasında göstermektedir.

Birleşmiş Milletler Kalkınma Programı (UNDP) tarafından hazırlanan Veri Yönetişimi Çerçevesi: Türkiye için Tavsiye Raporu¹⁰⁸ ise Türkiye için bir veri yönetişimi modeli önererek politika, insan kaynağı, teknoloji, kurumlar ve iş birlikleri temelinde ulusal bir çerçeve sunmaktadır. Raporda Türkiye’de henüz kapsamlı bir ulusal veri yönetişimi stratejisinin bulunmamaktadır. Bu alanda önemli kurumsal girişimlerin başlatıldığı vurgulanmaktadır.

Özellikle son yıllarda dijital dönüşüm politikaları doğrultusunda veri paylaşımı, yapay zeka, büyük veri ve kamu veri altyapıları konusunda önemli adımlar atılmıştır. UNDP (2024) raporuna göre Türkiye’de veri yönetişimine ilişkin başlıca yapılar şunlardır:

- KVKK,
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DTO),
- TÜİK,
- Ulusal Veri Sözlüğü Projesi,
- TUCBS (Türkiye Ulusal Coğrafi Bilgi Sistemi),
- Açık veri girişimleri,
- Ulusal yapay zeka stratejisi çalışmaları.

¹⁰⁶Bkz. chrome-

extension://efaidnbmnnnibpcajpcglefindmkaj/https://mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

¹⁰⁷ Bkz. chrome-extension://efaidnbmnnnibpcajpcglefindmkaj/https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TR-UlusalYZStratejisi2021-2025.pdf

¹⁰⁸ Bkz. https://www.undp.org/tr/turkiye/publications/veri-yonetisimi-cercevesi-turkiye-icin-tavsiye-raporu

Bununla birlikte mevcut yapıda bazı temel sorun alanları bulunmaktadır. Türkiye, veri yönetişimi farkındalığında belirli bir ilerleme kaydetmiştir. Kurumlar arasında merkezi bir veri yönetişimi stratejisinin olmayışı uygulamada parçalı ve kurumsal kapasitelerde dengesiz bir görünüm sergilemektedir. Kamu kurumlarında veri yönetişimine yönelik çeşitli girişimler olsa da bunlar çoğunlukla proje bazlı ve sürdürülebilirlikten uzak bir yapıdadır. Veriye dayalı karar alma kültürü henüz kurumsallaşmamıştır. Aynı zamanda veri yönetişimi konusunda yetkin insan kaynağı eksikliği, uygulamaların başarısını kısıtlamaktadır (UNDP, 2024).

Türkiye'de veri yönetişimi konusunda bir çerçeve bulunduğunu söylemek güçtür. Mevcut düzenlemeler (örneğin, Kişisel Verileri Koruma Kanunu) daha çok veri koruma ve gizlilik odaklıdır. Açık veri, veri sınıflandırması ve veri kalitesi gibi yönetim bileşenlerine dair yasal rehberlik eksiktir. Veri tanımları, formatları ve kod sistemleri arasında uyumsuzluklar, sistemler arası veri entegrasyonunu zorlaştırmaktadır. KVKK önemli bir yasal temel oluştursa da AB Veri Yönetişimi Yasası ve GDPR ile tam uyum konusunda geliştirilmesi gereken alanlar bulunmaktadır. KVKK'nın veri güvenliği konusunda güçlü hükümler içeriyor olsa da kurumların veri paylaşımı konusunda halen çekingen davrandıkları ifade edilmektedir (UNDP, 2024).

Türkiye'deki kurumlar arasında veri yönetişimi olgunluğu farklılık göstermektedir. Bazı kamu kurumlarında veri yönetişimi birimleri kurulmuşken, çoğunda bu yapılar ya hiç oluşmamış ya da etkin değildir. Veri sahipliği, sorumluluk ve roller açık bir şekilde tanımlanmadığı için karar alma ve uygulama süreçlerinde tutarsızlıklar yaşanmaktadır (UNDP, 2024).

Kurumlar arası veri paylaşımı çoğunlukla bireysel ilişkiler veya resmi yazışmalar üzerinden yürümektedir. Ortak veri sözlüğü, üst veri yönetimi ve veri kalitesi standartları gibi teknik yönetim bileşenleri eksiktir. Merkezi bir veri paylaşım platformu ve mimarisi yaygın değildir. Veri, birçok kamu kurumu tarafından paylaşılmaması gereken bir mülkiyet gibi görülmekte, bu da şeffaflığı ve iş birliğini engellemektedir. Stratejik karar süreçlerinde veriye dayalı düşünme yerine hiyerarşik karar mekanizmaları ön plandadır (UNDP, 2024).

Ulusal Yapay Zeka Stratejisi (2021–2025), veri yönetişimi açısından incelendiğinde belgede özellikle veriden değer üretme, dijital Türkiye, milli teknoloji hamlesi ve kaliteli veriye erişim kavramları ön plana çıkmaktadır. Strateji kapsamında kaliteli veri, güçlü teknik altyapı ve kurumsal koordinasyon mekanizmaları yapay zeka gelişiminin temel bileşenleri olarak değerlendirilmiştir. Bu bağlamda kamu kurumları arasında güvenli veri paylaşımı, anonimleştirilmiş veri kümeleri, Açık Devlet Verisi Portalı, Ulusal Veri Sözlüğü ve Kamu Veri Alanı gibi veri yönetişimi araçları önerilmektedir (Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021).

Bu doğrultuda Türkiye için geliştirilecek veri yönetişimi çerçevesinin hukuki düzenlemeler, stratejik yönetim mekanizmaları, teknik standartlar, veri paylaşım modelleri, etik ilkeler, kurumsal roller ve dijital egemenlik yaklaşımını bütünlük biçimde ele alması gerekmektedir.

3.4. YÜKSEKÖĞRETİM KURUMLARININ ÇERÇEVELERİ

Yükseköğretim kurumlarında veri yönetişimi, akademik ve idari süreçlerde üretilen verilerin elde edilmesi, işlenmesi, kullanılması ve korunmasına yönelik ilke, politika ve uygulamaların bütünü ifade etmektedir. Üniversiteler öğrenci bilgileri, akademik veriler, finansal veriler, araştırma çıktıları ve performans göstergeleri gibi çok çeşitli ve büyük hacimli veriler üretmektedir. Bu nedenle veri yönetişimi, veri kalitesinin korunması, güvenliğin sağlanması ve mevzuata uyumun gerçekleştirilmesi açısından kritik bir rol oynamaktadır. Ayrıca veri yönetişimi, veriye dayalı karar alma süreçlerini destekleyerek stratejik planlama, kurumsal etkinlik ve akademik mükemmelliğin geliştirilmesine katkı sağlamaktadır. Yükseköğretim kurumlarında veri yönetişiminin temel bileşenleri arasında veri kalitesi yönetimi, veri güvenliği ve gizliliği, erişim ve yetkilendirme mekanizmaları, veri etiği ve hesap verebilirlik yer almaktadır. Bu kapsamda geliştirilen politikalar veri sınıflandırma, erişim kontrolü, veri saklama, veri paylaşımı ve ihlal yönetimi gibi alanları kapsayarak kurumsal veri ekosisteminin sürdürülebilirliğini sağlamaktadır (Winks, 2023).

Veri yönetişimi politikalarını uygulanmasında genel yönü belirleyebilmek amacıyla veri yönetim çerçeveleri geliştirilmiştir. Yükseköğretim kurumlarında veri yönetişimi çerçevesinin oluşturulması, kurumsal ihtiyaçlar, teknolojik gelişmeler ve düzenleyici

gerekliliklerle uyumlu, ölçeklenebilir ve sürdürülebilir bir yapı geliştirilmesini gerektiren stratejik bir süreçtir (Smith, 2025). Bu sebeple özellikle uluslararası üniversitelerin geliştirdikleri bazı farklı çerçeveler dikkat çekmektedir.

Wisconsin Üniversitesi, Madison¹⁰⁹ kurumsal verinin ortak bir kaynak olarak yönetilmesi yaklaşımı ile oluşturduğu çerçevede, veri sahipliği yerine veri paylaşımı ve ortak kullanım kültürünü ön plana çıkarmaktadır. Üniversite misyonunu çerçevenin en üst katmanına koyması kurumsal değer üretimi sağlamaktadır. Literatürde yer alan veri yönetişimi çerçeveleriyle büyük ölçüde uyumlu olan çerçevenin beş ana sütunu veri sorumluluğu, veri kalitesi, gizlilik-uyum-etik, erişim ve güvenlik ile veri standartları olarak belirlenmektedir. Birçok klasik modelde dolaylı olarak ele alınan etik boyut açık şekilde konumlandırılmaktadır. Ayrıca veri okuryazarlığına ayrı bir katman olarak yer verilmesi, üniversite bağlamına özgü önemli bir farklılıktır (University of Wisconsin, 2023).

Akron Üniversitesi¹¹⁰ çerçevesi, özellikle bilgi okuryazarlığı ve değişim yönetimi boyutlarını merkeze alan daha dönüşüm odaklı bir yaklaşım sunmaktadır. Çerçevenin en üstünde yer alan *veri odaklı iyileştirmeler* ifadesi ile veri yönetişiminin amacı açık biçimde tanımlamakta ve sürekli iyileştirme aracı olarak konumlandırmaktadır. Çerçevenin ana bileşenleri politikalar ve standartlar, bilgi kalitesi, gizlilik-uyum-güvenlik, bilgi mimarisi ve entegrasyonlar ile raporlama ve analitik olmak üzere beş ana sütundan oluşmaktadır. Çerçevede bilgi kavramının veri kavramına göre daha baskın kullanılması ve değişim yönetiminin döngüsel bir yapı ile gösterilmesi diğer çerçevelerden ayıran özelliklerindendir (University of Akron, 2026).

Kansas State Üniversitesi¹¹¹ çerçevesinin merkezine veri yönetişimi programını alması, veri yönetişimini tekil uygulamalardan ziyade kurumsal düzeyde yönetilen bir program olarak ele alması fark yaratmaktadır. Diğer üniversitelerin çerçevelerine benzer şekilde veri sorumluluğu, veri kalitesi, üst veri yönetimi, veri standartları ve gizlilik, süreç yönetimi temel bileşenlerinden oluşmaktadır. Çerçeve veri yönetişimi kültürü oluşturabilmek için program ve bileşenleri hiyerarşik olarak kullanmaktadır. Aynı

¹⁰⁹ Bkz. <https://data.wisc.edu/data-governance/>

¹¹⁰ Bkz. <https://www.uakron.edu/datamanagement/governance/governance-framework>

¹¹¹ Bkz. <https://www.k-state.edu/data/data-governance/>

zamanda birçok üniversitede geliştirilmesi gereken üst veri yönetiminin ayrı bir sütun olarak konumlandırılmıştır. Karar alma süreçleriyle doğrudan ilişkilendirilmesi, veri yönetişimini çıktı odaklı bir çerçeveye dönüştürmektedir (Kansas State University, 2026).

Tennessee Üniversitesi, Knoxville¹¹² döngüsel, sade, kavramsal ve net bir veri yönetim çerçevesi tercih etmektedir. Çerçevenin sütunları insan, süreçler, teknoloji, kalite, iletişim ve sorumluluklar üzerine oturulmaktadır. Döngüsel yapı sayesinde çerçeve, sürdürülebilir bir yaklaşım sunmaktadır. Diğer çerçevelerden farklı olarak iletişim bileşeninin dahil edilmektedir (University of Tennessee, 2017).

Maine Üniversitesi çerçevesi, veri yönetiminde rol ve sorumlulukların açık şekilde tanımlanması için veri sorumluluğu kavramını merkezde konumlandırmaktadır. Merkezi katmanın altında uyum ve risk yönetimi, güvenlik ve erişim, veri bütünlüğü ve tutarlılığı ile standartlar ve politikalar sütunları yer almaktadır. Temel sütunlar veri kalitesi, veri erişilebilirliği, veri koruma gereksinimlerinin kurumsal düzeyde uyumluluk ve standardizasyon açısından da ele alındığını göstermektedir. İletişim katmanının altında yer alan felsefe, temel, değerler katmanları veri yönetişimini etik bir çerçeveye oturtmaktadır (University of Maine Systems, 2017).

Oxford Üniversitesi¹¹³ hiyerarşik katmanlar ve organizasyonel roller üzerinden yapılandıran, aynı zamanda topluluk temelli katılımı (community of practice) içeren bir çerçeve sunmaktadır. Topluluk temelli yaklaşım, diğer veri yönetişimi modellerine kıyasla daha katılımcı ve öğrenme odaklı bir yapı sunmaktadır. Stratejik–taktik–operasyonel katmanların ayrımının net olması, veri yönetişimi rollerinin ve sorumluluklarının açık biçimde tanımlanmasını sağlamaktadır. Üst yönetim (executive level) sahipliği, veri yönetişiminin kurumsal öncelik haline gelmesini desteklemektedir. Veri stratejisi ile uygulama arasındaki bağlantının kurulması, modelin uygulanabilirliğini artırmaktadır. Uyum, risk yönetimi ve karar destek süreçlerine vurgu, veri yönetişiminin stratejik değer üretme rolünü güçlendirmektedir. İletişim ve koordinasyonun açık şekilde vurgulanması, organizasyonel hizalanmayı desteklemektedir. Teknik bileşenlerin ve

¹¹² Bkz. <https://data.utk.edu/governance/>

¹¹³ Bkz. <https://governance.admin.ox.ac.uk/data-governance#collapse3490701>

analitik boyutun sınırlı ele alınması, modelin daha çok yönetsel ve organizasyonel bir çerçeve olarak konumlandığını göstermektedir (University of Oxford, t.y).

Denver Üniversitesi¹¹⁴ çerçevesi, veri yönetişimini program temelli, kültür odaklı ve yetkinlik geliştirici bir yapı içerisinde sunmaktadır. Çerçeve, diğer üniversitelerin çerçevelerine birçok yönden benzerlik göstermektedir. Benzer şekilde çerçeve veri sorumluluğu, veri kalitesi, gizlilik ve etik, veri standartları olmak üzere dört sütun üzerine oturtulmaktadır. Farklı olarak veri okuryazarlığının yatay bir katman olarak tüm bileşenleri kesmesi, modelin kullanıcı odaklı bir yaklaşım benimsediğini göstermektedir. Etik boyutun açık şekilde vurgulanması dikkat çeken özellikler arasındadır. Belkide çerçevenin en dikkat çekici noktası olan döngüsel yapı (kırmızı halka), veri yönetişiminin sürekliliğini ve geri besleme mekanizmalarını simgelemektedir (University of Denver, 2025).

Western Üniversitesi¹¹⁵ tarafından geliştirilen veri yönetişimi çerçevesi, veri yönetişimini özellikle kavramsal/operasyonel bütünleşme, veri taksonomisi ve rol temelli hesap verebilirlik ekseninde ele almaktadır. Modelin en üst katmanında yer alan stratejik düzey, kurumlar arası ve birim bazlı katmanlar veri yönetişiminin farklı organizasyonel seviyelerde nasıl uygulandığını göstermektedir. Çerçevenin en dikkat çekici yönlerinden biri, kavramsal ve gerçek veri yapılarının ayrıştırılarak ele alınmasıdır. Kavramsal düzeyde veri varlıkları, veri alanları ve fonksiyonel veri alanları şeklinde sınıflandırılırken, gerçek düzeyde bu yapı veri uygulamaları, veri öğeleri ve veri alanları üzerinden somutlaştırılmaktadır. Bu yaklaşım, veri yönetişiminin teorik çerçevesi ile teknik uygulamaları arasında güçlü bir köprü kurmaktadır (Western University, 2026).

Royal College of Art¹¹⁶, Edinburgh Üniversitesi¹¹⁷, Saskatchewan Üniversitesi¹¹⁸, York Üniversitesi¹¹⁹ çerçeveleri yükseköğretim kurumlarında veri yönetişiminin genel olarak benzer temel bileşenler üzerine kurulduğu görülmektedir. Tüm çerçeveler veriyi stratejik bir varlık olarak ele almaktadır. Veri kalitesi, güvenlik, gizlilik, yasal uyum ve hesap

¹¹⁴ Bkz. <https://www.du.edu/data-governance/news/2025-february-newsletter>

¹¹⁵ Bkz. <https://data.uwo.ca/governance/framework.html>

¹¹⁶ Bkz. https://rca-media2.rca.ac.uk/documents/Data_Governance_Framework_2024.pdf

¹¹⁷ Bkz. https://governance-strategic-planning.ed.ac.uk/sites/default/files/2025-04/Information%20Governance%20Framework_0.pdf

¹¹⁸ Bkz. <https://policies.usask.ca/documents/data-governance-framework.pdf>

¹¹⁹ Bkz. <https://www.yorku.ca/oipa/data-analytics-governance/>

verebilirlik gibi unsurları merkeze almaktadır. Ayrıca veri sahipliği, veri sorumluluğu ve yönetim yapılarının tanımlanması ile veri yaşam döngüsünü kapsayan bir yaklaşımın benimsendiği dikkat çekmektedir. Bununla birlikte çerçeveler arasında önemli farklılıklar da bulunmaktadır. Edinburgh Üniversitesi daha geniş bir bilgi yönetimi perspektifi benimseyerek veri, kayıt ve uyum süreçlerini entegre ederken Saskatchewan Üniversitesi ve Royal College of Art daha operasyonel, rol ve sorumluluk temelli veri yönetimi yapıları sunmaktadır. York Üniversitesi ise veri yönetimini analitik kapasite ve karar destek süreçleriyle ilişkilendirerek veri odaklı yönetim yaklaşımını ön plana çıkarmaktadır.

Sonuç olarak, yükseköğretim kurumlarında veri yönetiminin tek tip bir modelden ziyade kurumsal önceliklere göre farklılaşan yapıdadır. Her çerçevenin kendi bağlamı içinde güçlü yönler geliştirdiği anlaşılmaktadır.

4. BÖLÜM

BULGULAR VE DEĞERLENDİRME

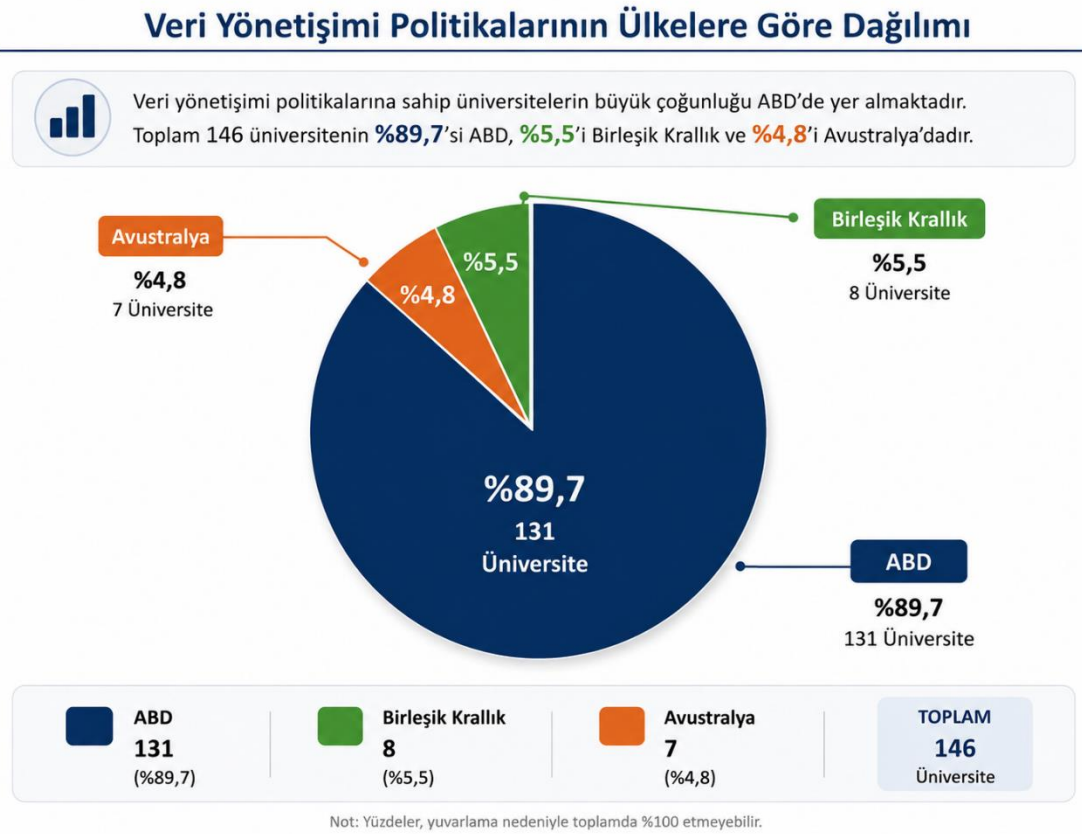
Bu bölüm araştırmanın amaçları doğrultusunda uluslararası ve ulusal üniversiteler olmak üzere iki ana başlık altında ele alınmıştır. ABD, Avustralya ve BK'deki 1174 adet uluslararası üniversitelerden 146 adet veri yönetiřimi politikası, ulusal düzeyde ise Yükseköğretim Kurulu ile veri yönetiřimi yapılanmasına sahip 24 adet üniversitenin politika belgeleri, yönergeleri, yönetmelikleri, resmî web sayfaları ve 10 adet üniversitenin görüşme verileri birlikte analiz edilmiştir. Uluslararası ve ulusal veri yönetiřimi belgelerinin tematik analizi ve yarı yapılandırılmış görüşmeler yoluyla elde edilen bulgular bu bölümde değerlendirilmiştir.

Uluslararası ve ulusal üniversitelerin durumları, veri yönetiřimi birimi ve personeli, veri standartları, veri erişimi ve paylaşımı, veri depolama, yedekleme, güvenlik ve gizlilik, veri kültürü başlıkları altında tematik şekilde sunulmuştur. Bu bölüm üniversitelerde veri yönetiřiminin mevcut durumunu ortaya koymak ve araştırmanın sonunda geliştirilen katmanlı veri yönetiřimi modelinin oluşturulmasına temel oluşturacak gereksinimlerin belirlenmesini amaçlamaktadır. Bu kapsamda uluslararası uygulamalarda öne çıkan başarılı yaklaşımlar ile Türkiye'deki mevcut durum birlikte analiz edilerek güçlü yönler, eksiklikler ve geliştirilmesi gereken alanlar ortaya konulmuştur.

Bu doğrultuda modelin *yönetişim katmanı*, üniversitelerde veri yönetiřimi birimlerinin kurumsal yapılanmaları, rol ve sorumluluk dağılımlarına ilişkin bulgular temel alınarak yapılandırılmıştır. *Teknik katman*, veri standartları, veri sözlüğü, üst veri yönetimi, veri kalitesi, veri entegrasyonu ve veri yaşam döngüsüne ilişkin bulgular doğrultusunda geliştirilmiştir. *Süreç katmanı*, veri erişimi ve paylaşımına ilişkin yetkilendirme, onay, izleme ve veri paylaşım süreçlerini kapsayacak şekilde oluşturulurken, bu süreçleri destekleyen teknik uygulamalar *teknik katman* ile bütünleştirilmiştir. *Yasal ve etik katman*, veri güvenliği, gizlilik, saklama, yedekleme ve yasal uyum gerekliliklerine ilişkin bulgular temel alınarak tasarlanmıştır. Teknik güvenlik kontrolleri ise *teknik katman* ile ilişkilendirilmiştir. Son olarak *kültür katmanı*, üniversitelerde veri kültürü, eğitim, farkındalık, liderlik desteği ve kurumsal sahiplenmeye yönelik bulgular doğrultusunda yapılandırılmıştır.

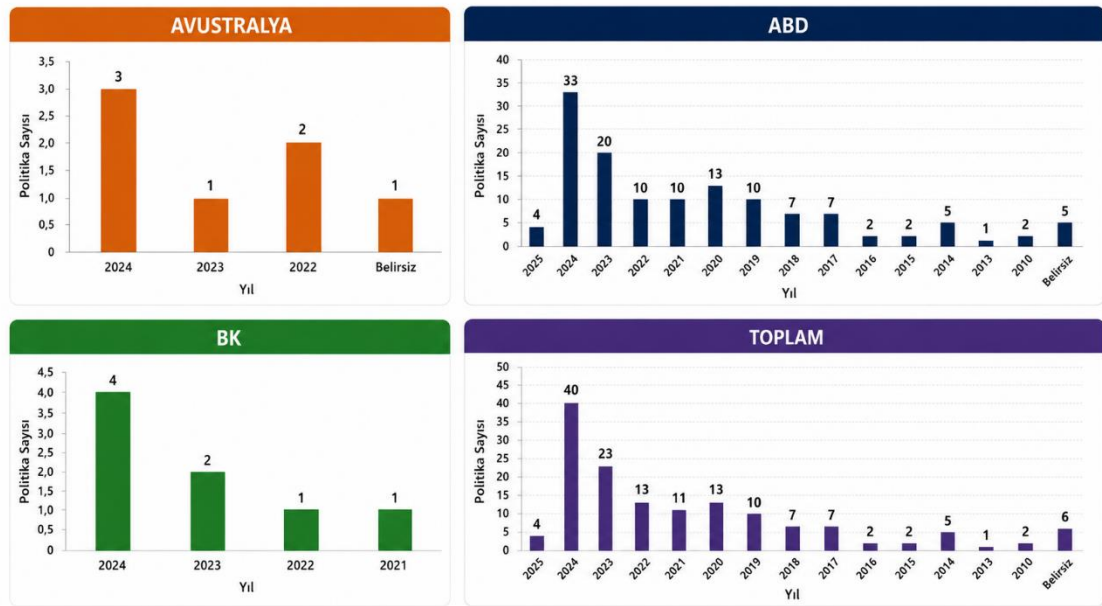
4.1. ULUSLARARASI ÜNİVERSİTELERİN MEVCUT DURUMLARI

Bu bölümde veri yönetiřimi konusunda uluslararası bir deęerlendirme yapabilmek amacıyla ABD, Avustralya ve BK'deki 1174 adet üniversitenin 146 adet veri yönetiřimi politikası tematik analiz yöntemiyle incelenerek sunulmuřtur.



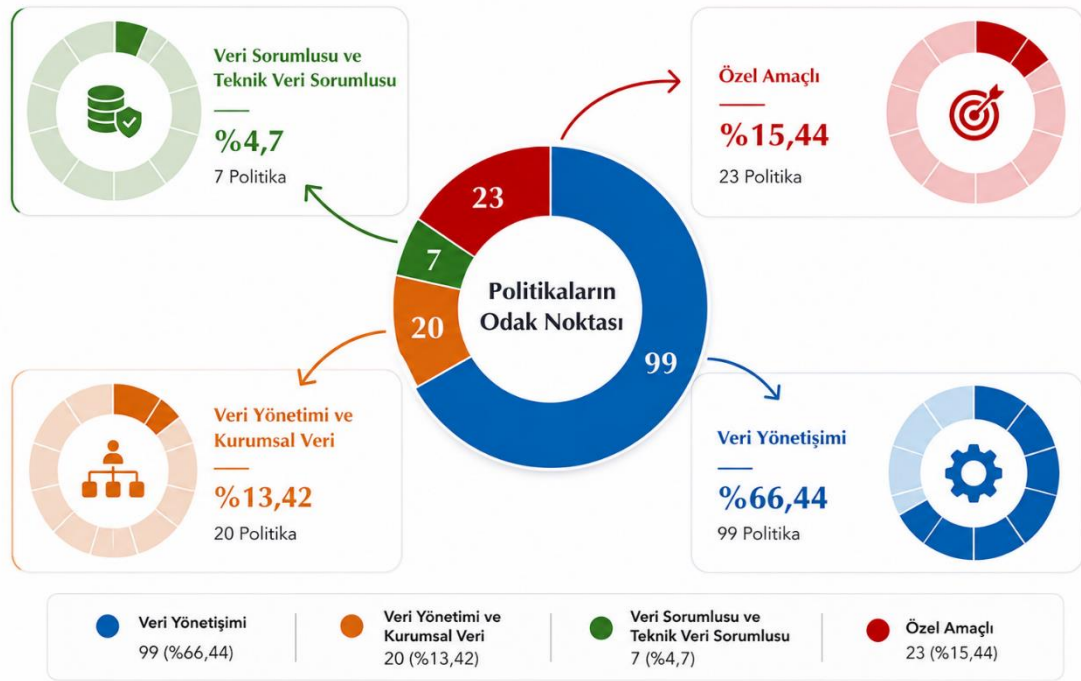
Grafik 2. Veri yönetiřimi politikalarının ülkelere göre dağılımı

Çalışma kapsamına alınan 1174 adet üniversitelerden 146 adedi erişilebilir politika belgesine sahiptir. İncelenen 146 üniversiteye ait veri yönetiřimi politika belgesinin büyük çoęunluęunun ABD kaynaklı olduęu görölmektedir (%89,7; n=131). BK (%5,5; n=8) ve Avustralya (%4,8; n=7) üniversiteleri daha sınırlı bir temsil düzeyine sahiptir. Bu dağılım, veri yönetiřimi politikalarının özellikle ABD üniversitelerinde kurumsal düzeyde yaygınlařtığını göstermektedir.



Grafik 3. Veri yönetiřimi politikalarının yıllara g re daėılımı

Grafik 3’te veri y netiřimi politikalarının  niversitelerde  zellikle 2020 sonrası d nemde hızla yaygınlařtıėını g stermektedir. ABD  niversiteleri erken adaptasyon ve s reklilik sergilerken, Avustralya ve BK  niversiteleri daha ge  bir politika  retim s reci yařamaktadır. Bu durum, veri y netiřiminin k resel  l ekte ortak bir ihtiya  haline geldiėini, kurumsal benimsenme hızının  lkelere g re farklılařtıėını ortaya koymaktadır.



Grafik 4. Veri yönetiřimi politikalarının bařlıklara g re daęılımı

Grafik 4'te incelenen üniversitelerin veri yönetiřimi politika bařlıklarının kavramsal odak noktalarına g re daęılımını ortaya koymaktadır. Bulgular, politika belgelerinin bařlık ve içeriklerinin deęerlendirilmesi sonucu oluřturulmuřtur. Büyük çoęunluęunun veri yönetiřimi kavramı etrafında toplanması veri yönetiřiminin baęımsız ve kurumsal alanı olarak tanımlandıęını ve terminolojik düzeyde güçlü biçimde benimsendięini g stermektedir (%66,44; n=99).

Özel amaçlı politikalar, komite t z kleri, özel amaçlı komiteler, ięg r ler ya da analitik bulgular ve belirli veri t rlerine (anket, sıralama, raporlama vb.) y nelik d zenlemeler gibi daha sınırlı ve baęlamsal amaçlara odaklanmaktadır. Bazı üniversitelerde veri yönetiřimi politika yerine, parçalı ve iřlevsel d zenlemeler  zerinden yapılandırıldıęını ortaya koymaktadır (%15,44; n=23)

Veri y netimi ve kurumsal veri  zerine odaklanan politikalar, veri y netiřimini daha çok veri y netimi s reçleri, kurumsal veri kullanımı ve operasyonel veri uygulamalarıyla iliřkilendirmektedir (%13,42; n=20).

Oldukça sınırlı olan veri sorumlusu ve teknik veri sorumlusu odaklı politikalarda kritik öneme sahip olan rollerin, başlık düzeyinde yeterince görünür kılınmadığını göstermektedir. Roller ve sorumlulukların çoğu zaman politika içeriğinde yer aldığı, başlık ve kavramsal çerçeve düzeyinde ikincil planda kaldığı söylenebilir (%4,7; n=7).

4.1.1. Veri Yönetişimi Birimleri ve Personeli

Uluslararası üniversitelerin veri yönetişimi politika metinleri, veri yönetişimi birimlerinin organizasyonel yapılanması, rol tanımları, yetki ve sorumluluk dağılımlarının benzerlik göstermektedir. Uluslararası üniversitelerin veri yönetişimi stratejik üst yönetim, bilgi teknolojileri ve hibrit yapılanma ekseninde şekillenmektedir (Bkz. Tablo 4). Bu yapılarda üst yönetim, yönetim kurulları, veri sahipleri, veri sorumluları ve teknik personelden oluşan bir organizasyon modelinin benimsendiğini ortaya koymaktadır. Üniversitelerin büyük çoğunluğunda veri yönetişimi, hiyerarşik rol dağılımları, açık görev tanımları ve uzmanlaşmış personel aracılığıyla kurumsallaştırılmaya çalışılmaktadır.

Tablo 4. Veri yönetiřimi birimlerinin yapılanması

Veri Yönetiřimi Birimi	Kurumsal Yapısı	Temel Özellikler
Stratejik Üst Yönetim Yapılanması	Rektörlük, Başkanlık Kabinesi/Konseysi ¹²⁰ , Baş Bilgi Yöneticisi ¹²¹ , Üniversite Sekreteri ¹²² , Mütevelli Heyeti ¹²³ gibi üst yönetim organlarının gözetimi altında	• Veri Sponsoru¹²⁴ ya da Veri sahibi¹²⁵ üst yönetim tarafından atanır. • Politika onayı ve kaynak planlaması üst yönetimde gerçekleşir. • Veri yönetiřimi kurum stratejisinin bir uzantısıdır. • Kurumsal düzeyde güçlü bir yönetim ve sahiplenme vardır.
BT Merkezli Yapılanma	Baş Bilgi Yöneticisi veya BT Direktörlüğü altında teknik ağırlıklı birim ¹²⁶	• Veri sınıflandırma, güvenlik, erişim kontrolü gibi teknik süreçler BT tarafından yönetilir. • Teknik Veri Sorumlusu¹²⁷ ve teknik personel belirleyicidir. • Risk azaltma, güvenlik ve teknik standartlara uyum odaktadır. • Yönetişim daha operasyonel-teknik bir yaklaşımla yürütölür.
Hibrit ya da Dağıtık Yapılanma	Hem akademik hem idari birimleri kapsayan, çok paydařlı ve çok katmanlı bir yaklaşım	• Veri Yönetişimi Konseyi¹²⁸ stratejik koordinasyonu sağlar. • Veri Sorumluluğu Konseyi¹²⁹ uygulama ve standartlaştırmadan sorumludur. • Komiteler arası hiyerarşı ve raporlama ilişkileri açık biçimde tanımlanmıştır. • Karar süreçleri katılımcı, yatay ve çok paydařlıdır.

¹²⁰ President's Cabinet/Council¹²¹ Chief Information Officer, CIO¹²² University Secretary¹²³ Board of Trustees¹²⁴ Data Sponsor: Kurumsal verilerin stratejik düzeyde yönetilmesini sağlayan, politika onayı ve kaynak planlamasının üst otoritesi olan, risk yönetimi ve kurumsal uyumluluğu garanti eden liderdir.¹²⁵ Data Owner: Belirli bir veri alanının mülkiyetinden, bütünlüğünden ve kullanım yetkilerinden en yüksek düzeyde sorumlu olan yöneticidir. Verinin nasıl tanımlanacağı, kimlerin erişebileceği, güvenlik seviyeleri, veri sınıflandırması ve kullanım politikaları üzerindeki nihai karar yetkisi vardır.¹²⁶ Veri yönetimini stratejik açıdan ele almaktan daha çok teknik operasyonlar (güvenlik, erişim, sistemler, altyapı) üzerinden yürüten BT merkezli yapı.¹²⁷ Data Custodian: Verinin teknik olarak saklanması, korunması ve sistemlerde güvenli şekilde işletilmesinden sorumlu teknik roldür. Veri altyapısını yönetir, erişim kontrollerini uygular ve güvenlik önlemlerini hayata geçirir.¹²⁸ Data Governance Council: Kurumun veriyle ilgili politika, standart ve stratejilerini belirleyen birimler arası koordinasyonu sağlayan, veri yönetiřimi kararlarını üst düzeyde yöneten çok paydařlı kuruldur.¹²⁹ Data Stewardship Council: Veri yönetiřimi politikalarının uygulanması, standartlaştırılması ve operasyonel seviyede yürütölmesi için Veri sorumluları arasında koordinasyon sağlayan veri kalitesi, erişim ve süreç yönetimini uygulama düzeyinde yöneten kurul.

Tablo 4'e göre üniversiteler stratejik üst yönetim yapılanmasında veri yönetişimini kurum stratejisiyle güçlü biçimde ilişkilendirerek net yetki dağılımı, hızlı politika onayı ve yüksek kurumsal meşruiyet sağlamaktadır. Ancak merkeziyetçi yapısı nedeniyle operasyonel ihtiyaçların yeterince temsil edilememesi ve karar süreçlerinin yavaşlaması riski bulunmaktadır.

BT merkezli yapılanma, veri güvenliği, teknik standartlar ve sistem entegrasyonu açısından etkinlik sağlamak ve operasyonel süreçleri hızlandırmaktadır. Buna karşın veri yönetişiminin stratejik ve kültürel boyutunun geri planda kalması sonucunda sorumluluğun BT birimlerine yüklenmesine yol açabilmektedir.

Hibrit ya da dağıtık yapılanma ise stratejik yönlendirme ile operasyonel uygulama arasında denge kurarak akademik ve idari birimlerin katılımını artırmakta ve veri odaklı kültürü güçlendirmektedir. Çok paydaşlı yapısı nedeniyle koordinasyon maliyetleri artabilmekte ve güçlü bir liderlik olmaksızın uygulamalar parçalı kalabilmektedir.

Veri yönetişimi birimleri ve rol dağılımları çok katmanlı, hiyerarşik ve paydaş temelli olarak yapılanmıştır. Rol dağılımları, çoğu kurumda benzer isimler taşımaktadır. Ancak rollerin sorumluluk alanları ve uygulama düzeyleri farklılaşmaktadır. Üniversitelerin politika metinlerinin neredeyse hepsinde Veri Sahibi, Veri Sorumlusu¹³⁰ ve Veri Kullanıcısı¹³¹ görev tanımları bulunmaktadır. Politikalarda aynı görev tanımının farklı üniversitelerde farklı işlevlerle tanımlanmakta olduğu görülmüştür (örneğin Veri Sorumlularının teknik ve/veya yönetsel görev tanımlarının bulunması).

¹³⁰ Data Steward: Belirli bir veri alanının günlük yönetimi, kalitesi, doğruluğu ve erişim süreçlerinden sorumlu olan operasyonel rol verinin doğru, tutarlı ve güvenli kullanılmasını sağlar.

¹³¹ Data User: Yetkilendirilmiş veriye erişen ve bu veriyi görevleri doğrultusunda kullanan kişi; veriyi doğru, güvenli ve etik şekilde kullanmakla yükümlüdür.



Şekil 20. Veri yönetimi birim personelinin yapılanması

Şekil 20’de üniversitelerde veri yönetim rollerinin hiyerarşik bir yapı içinde kurgulandığı görülmektedir. Stratejik üst düzey roller hiyerarşinin en üstünde yer alan, veri yönetiminin kurumsal sahipliğini ve stratejik yönünü belirleyen tanımlardan oluşmaktadır. Veri Sahibi, Veri Vekili¹³², Veri Sponsoru gibi roller öne çıkmaktadır. Bu roller veri politikalarının onaylanması, veri alanlarına ilişkin nihai yetki ve sorumluluğun üstlenilmesi, kaynak tahsisi ve kurumsal önceliklerin belirlenmesi gibi stratejik işlevleri yerine getirmektedir. Rektörlük, başkanlık veya yürütme kurulları tarafından atanan bu roller, veri yönetimini kurumun genel stratejik hedefleriyle ilişkilendiren temel aktörler olarak tanımlanmaktadır.

Yönetimsel ve koordinasyon düzeyindeki kurul ve konseyler veri yönetimi faaliyetlerinin kurumsal ölçekte koordine edilmesini sağlayan Veri Yönetimi Kurulu, Veri Sorumluluğu Konseyi ve benzeri komite yapıları yer almaktadır. Bu kurulların politika geliştirme, standart belirleme, veri kalitesi eşiklerinin tanımlanması ve birimler arası veri

¹³²Data Trustee: Belirli bir veri alanı için kurumsal çıkarları temsilen gözetim ve denetim sorumluluğu üstlenen, verinin politika ve mevzuata uygun biçimde kullanılmasını sağlayan yetkili roldür.

kullanımına ilişkin kararların uyumlaştırılması gibi yönetsel işlevler üstlendiğini göstermektedir. Çok paydaşlı yapıları sayesinde akademik ve idari birimler arasında temsil ve denge sağlayan bu konseyler, veri yönetişiminin kurum geneline yayılmasında kritik bir ara katman işlevi görmektedir.

Veri Sorumluları, Alan Bazlı Veri Sorumluları¹³³, Konu Bazlı Veri Alan Sorumluları¹³⁴ ve Veri Yöneticisi¹³⁵ gibi operasyonel bazlı roller ön plana çıkmaktadır. Belgelerde bu rollerin veri kalitesi, üst veri yönetimi, iş süreçlerine uygun veri tanımları ve günlük veri yönetişimi uygulamalarından sorumlu olduğu görülmektedir. Veri Sorumluları, stratejik düzeyde alınan kararların uygulamaya aktarılmasını sağlamakta ve veri yönetişimi ile iş süreçleri arasında köprü işlevi görmektedir.

Teknik ve altyapı odaklı roller, hiyerarşinin teknik katmanında Teknik Veri Sorumlusu¹³⁶, Teknoloji Altyapı Yöneticisi¹³⁷, BT Koordinatörü¹³⁸, Sistem Yöneticisi¹³⁹ rolleriyle temsil edilmektedir. Bu personel, veri altyapısının güvenliğini, erişilebilirliğini, sürekliliğini ve teknik bütünlüğünü sağlamaktan sorumludur. İçerik analizine göre bu roller veri yönetişiminin teknik omurgasını oluşturmaktadır. Stratejik karar alma yetkisinden ziyade, uygulama ve kontrol işlevleriyle sınırlandığını ortaya koymaktadır.

Hiyerarşinin en geniş tabanını Veri Kullanıcıları¹⁴⁰ grubu oluşturmaktadır. Akademik personel, idari personel, araştırmacılar ve yetkilendirilmiş diğer paydaşlardan oluşan bu grup, veri yönetişimi politikalarının günlük hayatta uygulanmasını sağlayan temel

¹³³ Domain Data Stewards: Belirli bir iş alanına veya kurumsal veri alanına ait verilerin kalitesi, tutarlılığı ve doğru kullanımından sorumlu operasyonel rollerdir.

¹³⁴ Subject Data Stewards: Belirli bir konu veya veri kümesine odaklanarak verinin doğruluğunu, anlam bütünlüğünü ve iş kurallarına uygunluğunu sağlayan operasyonel rollerdir.

¹³⁵ Data Manager: Belirli veri alanlarının günlük yönetimi, koordinasyonu ve iş süreçlerine uygun biçimde işletilmesinden sorumlu operasyonel roldür.

¹³⁶ Data Custodian: Verinin teknik altyapı, güvenlik, erişim ve sistem sürekliliğinden sorumlu olan veri yönetişimi politikalarının teknik düzeyde uygulanmasını sağlayan roldür.

¹³⁷ Technology Custodian: Veri ve bilgi sistemlerinin altyapı, sistem sürekliliği ve teknik işletiminden sorumlu, veri yönetişimini destekleyen teknolojik ortamın kesintisiz çalışmasını sağlayan roldür.

¹³⁸ IT Coordinator: BT birimleri ile iş birimleri arasında iletişimi ve koordinasyonu sağlayan, teknik süreçlerin planlandığı şekilde uygulanmasını takip eden roldür.

¹³⁹ System Administrator: Bilgi sistemlerinin kurulumu, işletimi, erişim yetkilendirmesi ve teknik sürekliliğinden sorumlu teknik roldür.

¹⁴⁰ Data Users: Yetkilendirildikleri verileri görevleri kapsamında kullanan, veri güvenliği, gizlilik ve etik kullanım kurallarına uymakla sorumlu kişilerdir.

aktörlerdir. Veri kullanıcıları hem veri tüketicisi hem de veri güvenliği, etik kullanım ve mevzuata uyum açısından sorumluluk taşıyan aktörler olarak tanımlandığı görülmektedir.

Bu bulgular, üniversitelerde veri yönetişiminin sürdürülebilir biçimde yürütülebilmesi için rol tanımları, yetki ve sorumluluk dağılımlarının açık biçimde tanımlanması gerektiğini göstermektedir. Bu nedenle geliştirilen modelin yönetim katmanında veri yönetişimi biriminin yapılanması ve personelinin hiyerarşisi temel bileşenler olarak yer almıştır.

4.1.2. Veri Standartları

Üniversitelerin veri yönetişimi politikaları, veri standartlarını veri yönetişiminin kurumsal olarak uygulanabilirliğini ve sürdürülebilirliğini sağlayan temel bileşenlerden biri olarak ele almaktadır. Politika metinlerinde verinin kurumsal karar alma süreçlerinde güvenilir, tutarlı ve yeniden kullanılabilir bir kaynak haline gelebilmesi için ortak veri tanımları, veri sınıflandırmaları, veri kalitesi ölçütleri ve teknik standartların oluşturulmasına öncelik verilmektedir.

Veri standartları, ağırlıklı olarak standartların uygulanması, izlenmesi ve sürdürülmesine yönelik süreçlerde çerçevelendirilmektedir. Standartların oluşturulması, uygulanması, izlenmesi ve güncellenmesine ilişkin sorumlulukların ise Veri Yönetişimi Kurulları, Veri Sahipleri ve Veri Sorumluları arasında paylaştırıldığı görülmektedir.

Tablo 5. Veri standardı uygulamaları

Veri Standartları	Uygulamalar	İlgili Roller
Veri Sınıflama	Veri sınıfları, erişim eşikleri	Veri Sahibi, Veri Sorumlusu
Üst veri ve Ortak Tanımlama	Veri sözlükleri, üst veri katalogları, SSR	Veri Sorumlusu, Veri Yönetişimi Kurulları
Veri Kalitesi	Doğruluk, tutarlılık, bütünlük, kalite ölçütleri	Veri Sahibi, Veri Sorumlusu
Veri Bütünlüğü ve Entegrasyon	Ortak veri modelleri, entegrasyon kuralları	Teknik Roller, Veri Sorumlusu
Veri Yaşam Döngüsü	Oluşturma, saklama, arşivleme, imha süreçleri	Veri Yöneticisi, Veri Sahibi
Veri Sahipliği ve Sorumluluğu	Veri Sahibi, Veri Sorumlusu, Teknik Veri Sorumlusu Roller	Tüm veri rolleri
Standartlara Uyum, İzleme ve Denetim	Uyum raporları, denetim süreçleri, düzeltici önlemler	Veri Yönetişimi Kurulları
Veri Standartlarının Sürekliliği ve Güncellenmesi	Revizyon takvimleri, eğitim, farkındalık	Üst Yönetim, Kurullar

Tablo 5’te görüldüğü gibi en yaygın ve ayrıntılı şekilde düzenlenen veri standardı alanı, veri sınıflamalarıdır. Üniversiteler, verinin gizlilik düzeyine göre farklı koruma ve erişim mekanizmalarının uygulanabilmesi amacıyla kurumsal veri varlıklarını sistematik biçimde sınıflandırmaktadır. İçerik analizine göre veri sınıflama uygulamaları şu ortak özellikleri taşımaktadır:

- Veri oluşturulduğu anda sınıflandırılmaktadır. Kullanım, saklama ve imha aşamalarında bu sınıflandırma esas alınmaktadır.
- Veriler genellikle kamuya açık (public), kurum içi (internal), korumalı (protected) ve kısıtlı/kritik (restricted/critical), hassas (sensitive) ve gizli (confidential) gibi kategorilere ayrılmaktadır.
- Bir veri kümesi, içerdiği en yüksek hassasiyet düzeyine göre sınıflandırılmaktadır. Veri sınıfının zaman içinde değişebileceği durumların (örneğin hassasiyetin azalması veya artması) tanımlandığı ve bu değişiklikleri yetkili rollerin onayladığı görülmektedir.
- Veri sınıflama, etiketleme faaliyeti ile birlikte yetki ve sorumluluk dağılımını şekillendiren bir kontrol mekanizması olduğunu ortaya koymaktadır.

- Korumalı ve kısıtlı veri sınıfları için şifreleme, erişim loglarının tutulması, veri paylaşımının sınırlandırılması ve veri ihlali durumlarında uygulanacak prosedürlerin önceden tanımlandığı görülmektedir.
- Veri sınıflamanın uygulanması, açık biçimde tanımlanmış rol ve sorumluluklara bağlanmıştır. Veri Sahipleri veri sınıfının belirlenmesinden nihai olarak sorumlu tutulurken, Veri Sorumluları sınıflamanın doğruluğunu ve tutarlılığını izlemektedir. Teknik roller ise sınıflamaya uygun güvenlik ve erişim kontrollerini uygulamaktadır.

Politikalarda öne çıkan bir diğer veri standardı alanı üst veri yönetimidir. Üst veri standartları, verinin anlamının kurumsal düzeyde ortak biçimde anlaşılmasını ve yorumlanmasını amaçlamaktadır. Politikalar doğrultusunda üst veri uygulamaları şu kurumsal tutarlılığı güçlendirmek için şu unsurları kapsamaktadır:

- Kurumsal veri varlıkları için standart veri tanımlarının oluşturulması,
- Veri sözlükleri ve üst veri katalogları aracılığıyla ortak terminolojinin sağlanması,
- Üst veri bilgilerinin veri sahipliği, sınıflama ve kullanım amacıyla ilişkilendirilmesi,
- Yeni veri setleri oluşturulurken üst veri girişinin zorunlu tutulması,
- Tanımların veri yönetişimi kurulları tarafından onaylanması şeklindedir.

İncelenen politikalarda veri kalitesi, veri yönetişiminin temel başarı kriterlerinden biri olarak tanımlanmaktadır. Veri kalitesi standartları, verinin doğru, zamanında, eksiksiz, tutarlı ve kullanılabilir olmasını hedeflemektedir. İçerik analizi sonucunda veri kalitesine ilişkin şu uygulamalar öne çıkmaktadır:

- Veri kalite boyutlarının (doğruluk, bütünlük, tutarlılık, güncellik) açık biçimde tanımlanması,
- Veri kalitesinin izlenmesi ve raporlanması sorumluluğu ile ilgili iş süreçlerinin oluşturulması,

- Düzenli denetim, kontrol ve düzeltme mekanizmalarının öngörülmesi,
- Analitik ve raporlama süreçlerinde standartlaştırılmış veri setlerinin kullanılması,
- Veri giriş ve güncelleme aşamalarında doğrulama kontrollerinin uygulanması,
- Veri Sorumluları aracılığıyla veri kalitesi iyileştirme çalışmalarının yürütülmesi.

Belgelerde veri bütünlüğü ve entegrasyonu, özellikle çoklu sistem kullanan üniversitelerde kritik bir standart alanı olarak ele alınmaktadır. Veri bütünlüğü, verinin doğruluğu ve güvenilirliğini, entegrasyon ise sistemler arası tutarlılığı sağlamayı amaçlamaktadır. Ortak uygulamalar şu şekilde özetlenebilir:

- Temel veri varlıkları için ortak tanımların kullanılması,
- Standart veri modelleri ve alanlarının merkezi olarak belirlenmesi,
- Entegrasyon süreçlerinin belgelenmesi,
- Veri akışlarının ve veri soy ağacının (data lineage) tanımlanması

Raporlama, analitik ve karar destek süreçlerinde veri tutarsızlıklarının azaltılması amaçlanmaktadır. Belgelerde entegrasyon süreçlerinin çoğunlukla teknik birimler tarafından yürütülmesine karşın, standartların belirlenmesi ve onaylanmasının veri yönetişimi kurulları tarafından yapıldığı görülmektedir.

Veri yaşam döngüsü standartlarının özellikle yasal uyum, kurumsal hafıza ve risk yönetimi ile ilişkilendirildiğini göstermektedir. Veri türlerine göre saklama sürelerinin belirlenmesi, tarihsel veya akademik değeri olan verilerin korunması ve kullanım süresi dolan verilerin güvenli biçimde imha edilmesi bu standartların temel uygulamaları arasında yer almaktadır.

Veri standartlarının güncelliğinin sağlanabilmesi için veri standartlarına uyumun periyodik olarak gözden geçirilmesi, standartlara aykırı veri kullanımının raporlanması ve düzeltilmesi, iç denetim ve uyum süreçleriyle veri yönetişimi uygulamalarının izlenmesi ve gerekli durumlarda politika ve standartların güncellenmesi gereklidir.

Üniversitelerin politika metinlerinde veri standartlarının kavramsal çerçevesi büyük ölçüde tanımlanmıştır. Elde edilen bulgular doğrultusunda geliştirilen modelin teknik katmanda bulunan veri mimarisi bileşeni veri standartlarına ilişkin bulgulardan; veri modelleme ve tasarımı bileşeni üst veri yönetimi, veri sözlüğü ve ortak veri tanımlarına ilişkin uygulamalardan; veri entegrasyonu ve uyumluluk, veri kalitesi ile üst veri yönetimi bileşenleri ise politika metinlerinde yer alan veri bütünlüğü, entegrasyon, kalite ve üst veri uygulamalarından oluşturulmuştur.

Süreç katmanında, veri standartlarının veri üretiminden arşivleme ve imhaya kadar tüm aşamalarda tutarlı biçimde uygulanmasını sağlamak amacıyla veri yaşam döngüsü temel süreçlerden biri olarak ele alınmıştır. Veri üretildiği andan itibaren sınıflandırılmaktadır. Yönetişim katmanda, veri standartlarının kurumsal düzeyde sahiplenilmesini ve stratejik hedeflerle uyumlu biçimde yönetilmesini sağlamak amacıyla veri sahipliği ve sorumluluğu bileşeni, veri standartlarının kurumsal ölçekte uygulanabilirliğinin güvence altına alınması amacıyla standartlara uyum, izleme ve denetim ile veri standartlarının sürekliliği ve güncellenmesi yönetim mekanizmalarının temel bileşenleri olarak yapılandırılmıştır.

4.1.3. Veri Erişimi ve Paylaşımı

Politikalardaki veri erişimi ve paylaşımı teması, açıklık ile güvenlik arasında denge kurmayı amaçlamaktadır. Politika metinlerinde veri erişimi ve paylaşımı, verinin sınıflandırma düzeyine, kullanım amacına ve kullanıcı rolüne bağlı olarak sınırlandırılmaktadır. Erişim yetkilerinin bireysel talepler yerine rol temelli ve görev odaklı bir yaklaşımla verilmesi öngörülmektedir.

Tablo 6. Veri erişimi ve paylaşımı uygulamaları

Veri Erişimi ve Paylaşımı	Uygulamalar	İlgili Roller
Rol Temelli Veri Erişimi	Erişim yetkilerinin görev ve rol tanımlarına göre verilmesi	Veri Sahibi, Veri Sorumlusu, Veri Kullanıcıları
Veri Sınıflamasına Dayalı Erişim	Veri sınıfına göre erişim düzeyi ve paylaşım sınırlarının belirlenmesi	Veri Sahibi, Veri Sorumlusu
Yetkilendirme ve Onay Süreçleri	Erişim taleplerinin resmi başvuru ve onay süreçlerine bağlanması	Veri Sahibi, Yönetişim Kurulları
Kurum İçi Veri Paylaşımı	Birimler arası veri paylaşımının iş gereksinimi esaslı yürütülmesi	Akademik ve İdari Birimler
Kurum Dışı Veri Paylaşımı	Paylaşımın yasal çerçeve, sözleşme ve üst yönetim onayına bağlanması	Üst Yönetim, Hukuk Birimi
Etik İlkelerine Dayalı Kullanım	Verinin meşru ve kurumsal amaçlarla kullanılması	Veri Kullanıcıları
Kayıt Altına Alma (Logging)	Erişim ve paylaşım işlemlerinin kayıt altına alınması	Teknik Veri Sorumluları
İhlal ve Uyumsuzluk Yönetimi	Yetkisiz erişimlerin raporlanması ve değerlendirilmesi	Yönetişim Kurulları
Rehberlik ve Farkındalık	Politika ve prosedürlerin kullanıcılarla paylaşılması	Veri Yönetişimi Birimi

Tablo 6’da sunulan veri erişimi ve paylaşımı konularında temel referans verilerin gizlilik ve risk düzeylerine göre sınıflandırılmasından geçmektedir. Her veri sınıfı için farklı erişim, paylaşım ve koruma kurallarının uygulanması, hassas/kısıtlı veriler için ek onay ve kayıt altına alma süreçleri geliştirilmiştir. Veri sınıflandırmasına bağlı olarak rol temelli veri erişim uygulamaları, bireysel talepler yerine görev ve sorumluluk esaslı erişim modeli sunmaktır. Veri erişim yetkilerinin kurumsal rol tanımlarına göre belirlenmesi, görev değişikliği veya kurumdan ayrılma durumlarında erişim haklarının güncellenmesi uygulamaları ile karşılaşılmıştır.

Veri erişim ve paylaşımının izlenebilir ve gerekçelendirilmiş bir süreç olarak işleyebilmesi için yetkilendirme ve onay mekanizmaları oluşturulmuştur. Veri erişim taleplerinin resmi başvuru süreçlerine bağlanması, Veri Sahibi veya yetkili birimler tarafından onay zorunluluğu ve geçici veya süreli erişim izinlerinin tanımlanması sıklıkla uygulanmaktadır.

Kurum içinde verimlilik ve tutarlılık sağlayabilmek amacıyla akademik ve idari birimler arasında veri paylaşımının iş gereksinimi temelli olması kullanılması, merkezi sistemler üzerinden veri paylaşımının teşvik edilmesi ve ortak veri tanımları ve standart raporlama yapıları geliştirilmiştir. Kurum dışı veri paylaşımının üst yönetim veya yetkili kurulların onayına tabi tutularak istisnai ve kontrollü bir şekilde yasal düzenlemeler, sözleşmeler ve mutabakat metinleri ile sınırlandırılmış olduğu gözlemlenmiştir.

Veri erişimi ve paylaşımı süreçleri, etik ilkelere dayalı veri kullanımı çerçevesinde ele alınmaktadır. Verinin meşru, kurumsal ve görevle ilişkili amaçlar doğrultusunda kullanılmasının zorunlu olduğu vurgulanmaktadır. Yetkisiz, kişisel veya etik dışı veri kullanımının açık biçimde yasaklandığı görülmektedir. Politika metinlerinde veri kullanıcılarının etik sorumlulukları tanımlanarak, veri erişimi ve paylaşımının bireysel takdir alanı olmaktan çıkarılıp kurumsal etik yönetişimin bir parçası haline getirildiği anlaşılmaktadır. Bu yaklaşım politika belgelerinin etik, sorumluluk ve kurumsal güven ilişkisi içinde yapılandırıldığını göstermektedir.

Veri erişimi ve paylaşımına ilişkin bir diğer önemli uygulama alanı, kayıt altına alma ve izleme (logging) mekanizmalarıdır. Belgelerde, veri erişim ve paylaşım işlemlerinin sistematik biçimde kayıt altına alınması, yetkisiz erişimlerin ve olası ihlallerin izlenmesi gerektiği belirtilmektedir. Gerektiğinde denetim ve soruşturma süreçlerinin işletilmesine olanak tanıyan bu kayıt mekanizmaları, veri yönetişiminin izlenebilirlik ve hesap verebilirlik boyutunu güçlendirmektedir.

İhlal ve uyumsuzluk durumlarına yönelik uygulamaların çoğu politikalarda daha çok ilkesel düzeyde tanımlandığı görülmektedir. Veri erişimi ve paylaşım ihlallerinin raporlanması ve bu ihlallere karşı disiplin veya düzeltici önlemlere yer verilmiştir. Ancak bu süreçlerin nasıl işletileceğine ilişkin operasyonel ayrıntılar sınırlı kalmaktadır. İhlallerin veri yönetişimi kurulları veya yetkili yapılar tarafından değerlendirilmesi öngörülmüştür. Uygulamaya dönük net iş akışlarının eksikliği, bu alanın yönetim olgunluğu açısından geliştirilmesi gereken bir boyut olduğunu göstermektedir.

Son olarak, veri erişimi ve paylaşımına ilişkin rehber dokümanların yayımlanması, kullanıcıların politika ve prosedürler hakkında bilgilendirilmesi ve standartların

erişilebilir biçimde sunulması veri yönetişiminin kurumsal düzeyde benimsenmesini destekleyen uygulamalar olarak öne çıkmaktadır.

Bu doğrultuda yönetişim katmanı, veri sahibi, veri sorumlusu, veri kullanıcıları ve yönetişim kurullarının erişim yetkileri, rol temelli veri erişimi, yetkilendirme ve onay süreçleri temel alınarak yapılandırılmıştır. Teknik katmanda, veri güvenliği bileşeninde veri sınıflandırmasına dayalı yetkilendirme, kurum içi ve kurum dışı veri paylaşımı, ihlal ve uyumsuzluk yönetimi teknik mekanizmalarına yer verilmiştir. Kültür katmanda ise etik ilkelere dayalı veri kullanımı, etik ve sorumlu kullanım anlayışının kurumsallaştırılmasını destekleyen bir bileşen olarak ele alınmıştır. Rehberlik ve farkındalık uygulamaları ise eğitim ve farkındalık bileşeninin oluşturulmasına temel sağlamıştır.

4.1.4. Veri Depolama, Yedekleme, Güvenlik ve Gizlilik

Üniversitelerin veri depolama ve koruma uygulamalarının büyük ölçüde veri sınıflandırması temelinde yapılandırıldığı anlaşılmıştır. Politikaların çoğunda veriler *genel/kamuya açık, korunan, gizli ve özel* gibi kategorilere ayrılmaktadır. Bu sınıflar doğrudan depolama ortamı seçimini, erişim kısıtlarını ve imha gerekliliklerini belirlemektedir. Üniversitelerde veri depolama, verinin nerede, nasıl ve hangi koşullarda saklanacağına ilişkin kararların, kurumsal politikalarla belirlenmesi gerektiği vurgulanmaktadır. Veri depolamanın büyük ölçüde merkezi ve denetimli sistemler üzerine kurgulandığını göstermektedir. Hassas ve kısıtlı verilerin, üniversite tarafından yönetilen sunucular veya onaylı bulut hizmetleri dışında saklanması çoğu politikada açık biçimde yasaklanmaktadır. Kişisel cihazlar, taşınabilir bellekler ve kontrolsüz depolama ortamları yüksek riskli alanlar olarak tanımlanmaktadır. Bu tür ortamlarda veri saklanması istisnai durumlarda ve ek güvenlik önlemleriyle mümkün kılınmaktadır. Bu yaklaşım, veri güvenliğinin bireysel sorumluluktan çıkarılarak kurumsal kontrol altına alındığını göstermektedir.

Veri yedekleme ise politika metinlerinde iş sürekliliği ve veri kurtarma perspektifiyle ele alınmaktadır. Üniversitelerin, düzenli yedekleme süreçleri oluşturması, yedeklerin fiziksel veya mantıksal olarak ana sistemlerden ayrılmış ortamlarda saklanması ve yedekleme–geri yükleme süreçlerinin periyodik olarak test edilmesi gerektiği

vurgulanmaktadır. Yedekleme sorumluluğu çoğunlukla teknik veri sorumluları ve veri vekilleriyle ilişkilendirilmektedir. Ancak yedekleme gereksinimlerinin belirlenmesinde Veri Sahibi ve Veri Sorumluları rollerinin de karar süreçlerine dahil olduğu görülmektedir. Böylece yedekleme, yönetim kapsamında paylaşılan bir sorumluluk alanı haline gelmektedir.

Veri güvenliği boyutunda, politika metinlerinde çok katmanlı güvenlik yaklaşımının benimsendiği dikkat çekmektedir. Yetkilendirme, şifreleme, iki faktörlü kimlik doğrulama, uzaktan bağlantı güvenliği (ör. VPN zorunluluğu) ve erişim kayıtlarının tutulması (loglama) politikaların ortak unsurlarıdır. Özellikle hassas ve kişisel verilerin hem aktarım sırasında hem de depolama ortamında korunması gerektiği belirtilmektedir. Yetkisiz erişimlerin önlenmesi, erişim faaliyetlerinin kayıt altına alınması ve güvenlik ihlallerinin izlenmesi, veri güvenliğinin temel unsurları arasında yer almaktadır. Bu durum, veri güvenliğinin önleyici kontrol mekanizmalarına dayandığını göstermektedir.

Gizlilik uygulamaları ise özellikle kişisel veriler ve hassas veri alanlarında yasal uyum ve etik sorumluluk çerçevesine dayandırılmaktadır. Politika metinlerinde FERPA, HIPAA, GDPR, GLBA, FISMA gibi düzenlemelere uyum vurgusu belirgin olup, bazı kurumların GDPR'ye tam uyum politikası geliştirdiği (ör. North Kentucky ve Suffolk) görülmektedir. Bu kapsamda veri öznesi hakları (erişim, düzeltme, silme), şeffaflık ve otomatik karar süreçlerinde etki analizi gibi unsurlar öne çıkmaktadır.

Üniversitelerin dış paydaşlarla veri paylaşımını güvenlik ve gizlilik açısından sıkı koşullara bağladığı görülmektedir. Montana Eyalet Üniversitesi e-posta ile veri gönderimini yasaklamakta, hassas verilerin şifreli dosya transferi veya güvenli web servisleri aracılığıyla paylaşılmasına izin vermektedir. Saint Thomas Üniversitesi, ülke dışına veri aktarımı ve yabancı uyruklu bireylerle paylaşım durumlarında ihracat kontrol düzenlemelerine dikkat çekerek ön onay mekanizması öngörmektedir. Bu uygulamalar, veri depolama–yedekleme–güvenlik–gizlilik ekseninin dış kaynak kullanımı ve veri aktarımı gibi alanlarda da yönetim kapasitesini gerektirdiğini göstermektedir.

Politika metinlerinde ayrıca veri saklama süreleri ve imha süreçleri, veri güvenliğinin tamamlayıcı bir boyutu olarak ele alınmaktadır. Verinin gereğinden uzun süre saklanması güvenlik riski oluşturabileceği vurgulanmaktadır. Yasal, idari ve

akademik gereklilikler doğrultusunda saklama sürelerinin tanımlanması önerilmektedir. Saklama süresi dolan verilerin güvenli biçimde imha edilmesi hem dijital hem de fiziksel ortamlarda uygulanması gereken zorunlu bir uygulama olarak sunulmaktadır. Bu çerçevede veri güvenliği, verinin yaşam döngüsünün tamamını kapsamaktadır. Aynı zamanda veri depolama ve imha standartları, yasal yükümlülükler ve kurumsal risk yönetimiyle ilişkilendirilmektedir. Bu kapsamda öne çıkan uygulamalar şunlardır:

- Veri türlerine göre saklama sürelerinin tanımlanması
- Tarihsel değeri olan verilerin korunması
- Kullanım süresi dolan verilerin güvenli biçimde imha edilmesi
- Kayıt yönetimi ve veri yönetişimi politikalarının uyumlu biçimde ele alınması

Genel olarak bulgular, üniversitelerde veri depolama, yedekleme, güvenlik ve gizlilik uygulamalarının veri sınıflandırması, rol temelli yetkilendirme, teknik kontrol ve yasal/etik uyum bileşenleri üzerinden bütünselik biçimde yapılandırıldığını ortaya koymaktadır. Bununla birlikte, bazı politikaların operasyonel iş akışlarını ayrıntılandırmak yerine ilkesel düzeyde kalmaktadır. Buna karşılık belirli kurumların (ör. Indiana, Bucknell, Maryland, GDPR uyumlu üniversiteler) daha sistematik ve denetlenebilir güvenlik–gizlilik modelleri geliştirdiği dikkat çekmektedir.

Teknik katmanda yer alan veri depolama ve operasyonlar, veri güvenliği, veri ambarı ve iş zekası bileşenleri politika metinlerinde tanımlanan veri depolama, koruma, yedekleme, erişim kontrolü ve merkezi veri yönetimi uygulamaları temel alınarak yapılandırılmıştır. Ayrıca politika belgelerinde yer verilen veri güvenliği, gizlilik, veri saklama ve imhaya ilişkin yasal düzenlemeler ile kurumsal politika hükümleri, modelin yasal ve etik katmanında yer alan düzenleyici çerçeveler ve stratejik politika çerçeveleri bileşenlerinin oluşturulmasına katkı sağlamıştır.

4.1.5. Veri Kültürü

Üniversitelerin politikaları, veri yönetişimini kurumsal değerler, davranış normları ve yönetim anlayışıyla bütünleşik bir kurum kültürü inşa etme aracı olarak konumlandırmaktadır. Bu bağlamda veri, üniversitelerin stratejik hedeflerine yön veren, karar alma süreçlerini besleyen ve kurumsal sorumluluk anlayışını şekillendiren temel bir varlık olarak ele alınmaktadır. Politikaların amaç, arka plan ve politika ilkeleri bölümleri, verinin kurumsal değer sisteminin merkezine yerleştirildiğini ve tüm paydaşların bu ortak anlayış etrafında yönlendirildiğini göstermektedir.

Üniversitelerde veri temelli düşünme biçiminin kurumsal davranışa dönüştürülmesi için güçlü bir etik ve normatif çerçevenin oluşturulduğunu ortaya koymaktadır. Etik kullanım ilkeleri, gizlilik, şeffaflık, hesap verebilirlik gibi kavramlar veriyle temas eden tüm aktörler için bağlayıcı davranış kuralları haline getirilmiştir. Özellikle veriyi kötüye kullanımının hukuki ve bireysel sorumluluk doğuran bir eylem olarak tanımlanması, kurum kültürünün disiplin ve etik boyutunu güçlendirmektedir.

Kurum kültürünün sürdürülebilirliği açısından eğitim ve farkındalık mekanizmaları merkezi bir rol oynamaktadır. Üniversiteler, veri yönetişimi eğitimlerini işe alım sürecinden başlayarak periyodik biçimde tüm personel ve paydaşlara sunmaktadır. Eğitimlerin tamamlanması kurumsal sistemlerde izlenmekte ve üst yönetime raporlanmaktadır. Hassas veriyle çalışan personel için özel eğitimler zorunlu tutulmaktadır. Böylece bilgi güvenliği ve etik farkındalık kurumsal refleks haline getirilmektedir.

Ayrıca politikalar, veri yönetişimini kurumsal öğrenme ve iş birliği kültürüyle bütünleştirmektedir. Üst veri yönetimi, veri sözlükleri, ortak veri dili oluşturma girişimleri ve komiteler arası koordinasyon mekanizmaları, üniversitelerde paylaşılan anlam üretimini ve kolektif sorumluluk anlayışını güçlendirmektedir. Karar süreçlerinin çok paydaşlı komiteler aracılığıyla yürütülmesi, katılımcı yönetim kültürünün kurumsallaşmasını sağlamaktadır.

Sonuç olarak üniversitelerde veri yönetişimi, etik davranış, kurumsal sorumluluk, katılımcı yönetim ve sürekli öğrenmeye dayalı bir kurum kültürü üretmektedir. Bu kültür,

üniversitelerin akademik, idari ve stratejik kimliğini şekillendiren temel bir unsur haline getirmektedir.

Tablo 7. Veri kültürü uygulamaları

Kültürel Boyut	Politika ve Uygulama Unsurları	Kurumsal Etki
Stratejik Sahiplik Kültürü	Verinin <i>kurumsal varlık</i> olarak tanımlanması, üst yönetim onayı ve politika sahipliği, stratejik hedeflerle uyum	Veriye dayalı karar alma ve yönetsel bütünlük
Etik ve Sorumluluk Kültürü	Etik kullanım ilkeleri gizlilik ve şeffaflık, bireysel ve kurumsal sorumluluk vurgusu, ihlal yaptırımları	Güven temelli kurumsal davranış
Eğitim ve Farkındalık Kültürü	Zorunlu veri koruma ve gizlilik eğitimleri rol bazlı eğitim programları, düzenli güncelleme	Sürdürülebilir bilgi güvenliği
Katılımcı Yönetişim Kültürü	Çok paydaşlı komiteler, veri yönetim konseyleri, rol ve görev tanımları	Kurumsal iş birliği ve sahiplenme
Standartlaşma ve Öğrenme Kültürü	Üst veri yönetimi, veri sözlükleri, ortak veri dili, sürekli iyileştirme	Kurumsal öğrenme ve veri kalitesi
Hesap Verebilirlik Kültürü	Loglama, ihlal bildirimi, denetim süreçleri, revizyon ve izleme mekanizmaları	Kurumsal şeffaflık ve güvenilirlik
Uyum ve Sürdürülebilirlik Kültürü	Yasal düzenlemelere uyum politika güncellemeleri, sürekli gözden geçirme	Kurumsal dirençlilik ve uzun vadeli yönetim

Tablo 7’de, üniversitelerde veri yönetişiminin kurumsal kültürün yapılandırılması göstermektedir. Tablo 7’de yer alan katmanlar, verinin stratejik bir kurumsal varlık olarak sahiplenilmesinden başlayarak etik sorumluluk, eğitim ve farkındalık, katılımcı yönetim, standartlaşma ve kurumsal öğrenme ile hesap verebilirlik ilkelerine uzanan çok boyutlu bir kültürel dönüşümü temsil etmektedir. Veri yönetişiminin üniversitelerde ortak değerler, davranış normları ve sürdürülebilir yönetim anlayışı üreten bir kurum kültürü inşa ettiğini ortaya koymaktadır.

Bu bölümden elde edilen bulgular, geliştirilen modelin kültür katmanının oluşturulmasına da katkı sağlamıştır. Bu doğrultuda politika metinlerinde vurgulanan stratejik sahiplik, liderlik desteği bileşenine temel oluşturmuştur. Verinin etik ilkelere uygun, yalnızca kurumsal amaçlar doğrultusunda kullanılmasına yönelik düzenlemeler, etik ve sorumlu

kullanım bileşeninin geliştirilmesini desteklemiştir. Politika ve prosedürlerin çalışanlarla paylaşılması, rehberlik faaliyetleri ve farkındalık uygulamaları ise veri okuryazarlığı, veri güveni, eğitim ve farkındalık bileşenlerinin oluşturulmasına katkı sağlamıştır. Kurum içi veri paylaşımı ve katılımcı yönetim, iş birliği bileşenine temel oluştururken, veri standartlarının ortak biçimde uygulanmasına yönelik standartlaşma ve kurumsal öğrenme ise veri kalitesi boyutlarının bu bölümde yer almasını sağlamıştır.

4.2. ULUSAL ÜNİVERSİTELERİN MEVCUT DURUMLARI

Bu bölümde, ulusal ölçekte karşılaştırmalı bir değerlendirme yapabilmek amacıyla YÖK'ün ve Türkiye'deki 23 üniversitenin kurumsal veri yönetişimine yönelik yapılandırılmış birimleri incelenmiştir. Bu kapsamda, ilgili birimlerle doğrudan görüşmeler gerçekleştirilmiş ve ayrıca 24 farklı birime ait resmî web sitesi sistematik olarak analiz edilmiştir.

YÖK'ün ve üniversitelerin veri yönetişimi alanında faaliyet gösteren birimlerinin resmî web siteleri incelenerek, birimlerin kurumsal yapılanmaları ve idari düzenlemeleri hakkında veri toplanmıştır. Elde edilen bulgular şekil ve tablolar aracılığıyla sunulmuştur. Bunun yanı sıra, kurumların web sitelerinde erişime açık olan politika, yönerge ve yönetmelik gibi idari düzenlemeler içerik analiz yöntemi kullanılarak değerlendirilmiştir.

Üniversiteler içinde sadece Hacettepe Üniversitesi, Kurumsal Veri Yönetişimi Politikası geliştirmiştir. Politika, veri yönetişiminin temel bileşenleri olan veri kalitesi, veri sahipliği, veri sınıflandırma, veri paylaşımı, veri güvenliği ve rol temelli yönetim yapılarını kapsayan bir kurumsal çerçeve sunmaktadır. Diğer üniversitelerin yönerge ve yönetmeliklerinde veri yönetişimi birimi çoğunlukla ilkesel ve yönetsel bir yapı olarak tanımlanmaktadır. Birimlerin günlük operasyonları, iş yükü, süreç sahipliği ve uygulama sorumlulukları ayrıntılandırılmamaktadır. Hacettepe Üniversitesinin politikasında ise yönetim ve destek seviyelerinden oluşan bir model tanımlanmıştır. Bu durumla beraber veri sahipliği, veri sorumluluğu ve operasyonel roller açık biçimde belirlenmiştir. Özellikle üç seviyeli yapı (politika, yönetim, destek), veri yönetişimi literatürü ile uyumludur.

Politikanın misyon ve vizyon ifadelerinde verinin stratejik bir varlık olarak konumlandırıldığı ve karar alma süreçlerinin veri temelli yürütülmesinin hedeflendiği

açık biçimde ortaya konmuştur. Veri kalitesi yönetimi doğruluk, bütünlük, tutarlılık ve güncellik gibi boyutlar açıkça tanımlanmış ve bu yönüyle literatürdeki veri kalite standartlarıyla uyum sağlanmıştır.

Politika ve standartlar açısından veri sınıflandırma, erişim, güvenlik, paylaşım ve hukuki uyum konuları ayrıntılı biçimde ele alınmıştır. Özellikle KVKK ve ISO 27001 gibi düzenlemelerle uyumlu bir yapı kurulması önemli bir güçlü yön olarak öne çıkmaktadır.

Veri kültürü ve organizasyonel dönüşüm açısından politika olumlu bir yaklaşım sergilemektedir. Eğitim, farkındalık ve kurumsal benimseme vurgulanmış ve veri yönetişiminin tüm paydaşları kapsayan bir yapı olması gerektiği belirtilmiştir.

Teknoloji ve veri altyapısı boyutunda veri katalogları, üst veri yönetimi, veri entegrasyonu, veri mimarisi veya analitik platformlara ilişkin geliştirilmesi gereken noktalar göze çarpmaktadır.

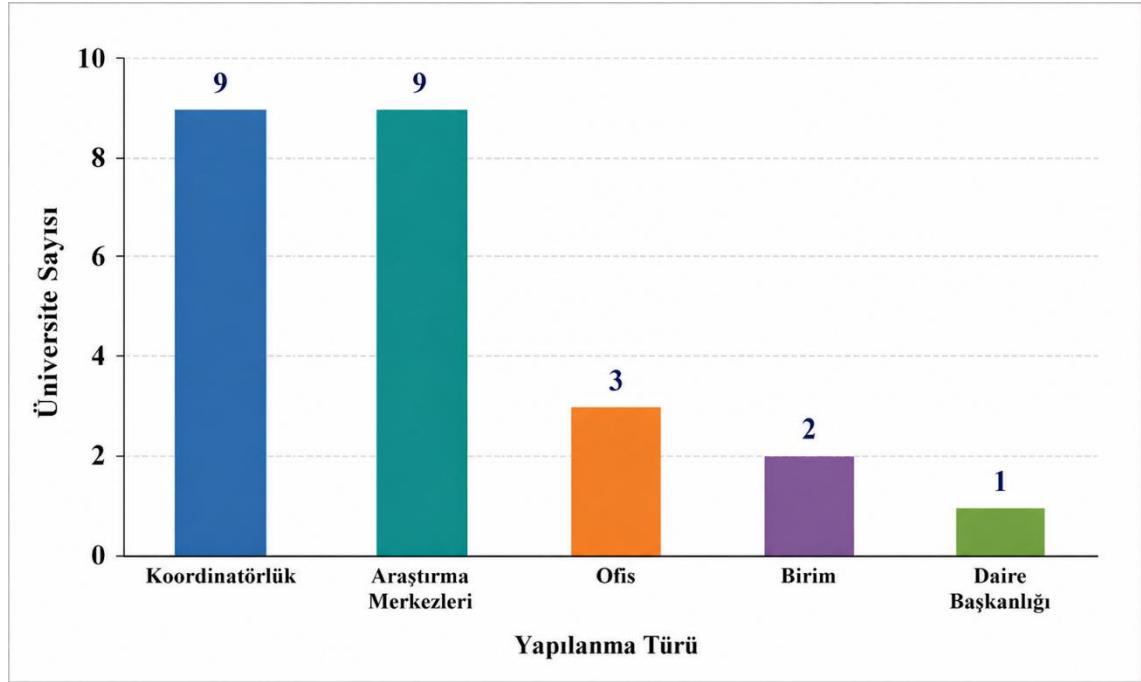
Aynı zamanda politikanın izleme, değerlendirme ve sürekli iyileştirme boyutunda politika sınırlı kalmaktadır. Yıllık gözden geçirme ifadesi bulunmakla birlikte, veri yönetişimi performansının nasıl ölçüleceği, hangi göstergelerin kullanılacağı ve geri bildirim mekanizmalarının nasıl işleyeceği tanımlanmamıştır. Bu durum, veri yönetişimi olgunluğunun sürdürülebilir şekilde geliştirilmesini zorlaştırabilir.

Geliştirilmesi gereken yönler bir tarafa politika, Türkiye'deki üniversitelerde veri yönetişiminin kurumsallaşmasına yönelik olgunlaşmış bir model örneği olarak değerlendirilebilir niteliktedir.

4.2.1. Veri Yönetişimi Birimleri ve Personeli

Üniversitelerdeki veri yönetişimi birimleri, kuruluş amaçları, kurumsal konumları ve dayandıkları idari düzenlemeler bakımından birbirinden farklılık göstermektedir. Koordinatörlük veya ofis türü yapılanmalarda kurumsal veri varlıklarının yönetimi, raporlama ve karar destek vurgusu yapılmıştır. Uygulama ve araştırma merkezlerinde veri bilimi, büyük veri, yapay zeka ve Ar-Ge kapasitesi ön plana çıkmaktadır. Ayrıca bazı örneklerde veri yönetişimi yapılanmalarının zaman içinde dijital dönüşüm ve bilişim çerçevesiyle birleşerek yeniden konumlandığı görülmektedir. Yasal dayanak türlerindeki çeşitlilik (KHK/kurul kararı-senato/yönetim kurulu-Resmî Gazete yönetmeliği-

yönerge) ise veri yönetişiminin yükseköğretimde henüz standartlaşma sürecinde olduğuna işaret etmektedir.



Grafik 5. Veri yönetişimi birimlerinin yapılanma türü

Grafik 5'te üniversitelerin kurumsal veri yönetişimine yönelik yapılanma türlerinin dağılımını göstermektedir. Daire Başkanlığı yapılanması YÖK'e aittir ve üniversitelerde bu yapılanma türü görülmemektedir. Veri yönetişimi alanında en yaygın yapılanma biçiminin koordinatörlük olduğu görülmektedir. Veri bilimi, büyük veri ve yapay zeka odaklı araştırma merkezleri, üniversitelerin analitik kapasite geliştirme yönündeki eğilimlerini yansıtmaktadır. Buna karşılık, ofis ve birim düzeyindeki yapılanmaların sınırlı sayıda olduğu görülmektedir. Üniversitelerde veri yönetişiminin büyük ölçüde esnek, proje ve koordinasyon odaklı yapılanmalar aracılığıyla yürütüldüğünü ortaya koymaktadır. Bu bulgu, üniversitelerde veri yönetişiminin halen gelişim ve olgunlaşma sürecinde olduğunu, kurumsal yapıların standartlaşma ihtiyacı taşıdığını göstermektedir.

Yönetmelikler ve yönergeler incelendiğinde araştırma merkezlerinin ve koordinatörlükleri amaçları, faaliyet alanları, organizasyon yapıları, görev dağılımları ve veriyle ilgili süreç tanımları bulunmaktadır. Araştırma merkezlerinin temel amaçlarında veri analizi yapmak, istatistiksel değerlendirme ve danışmanlık sağlamak, eğitim ve

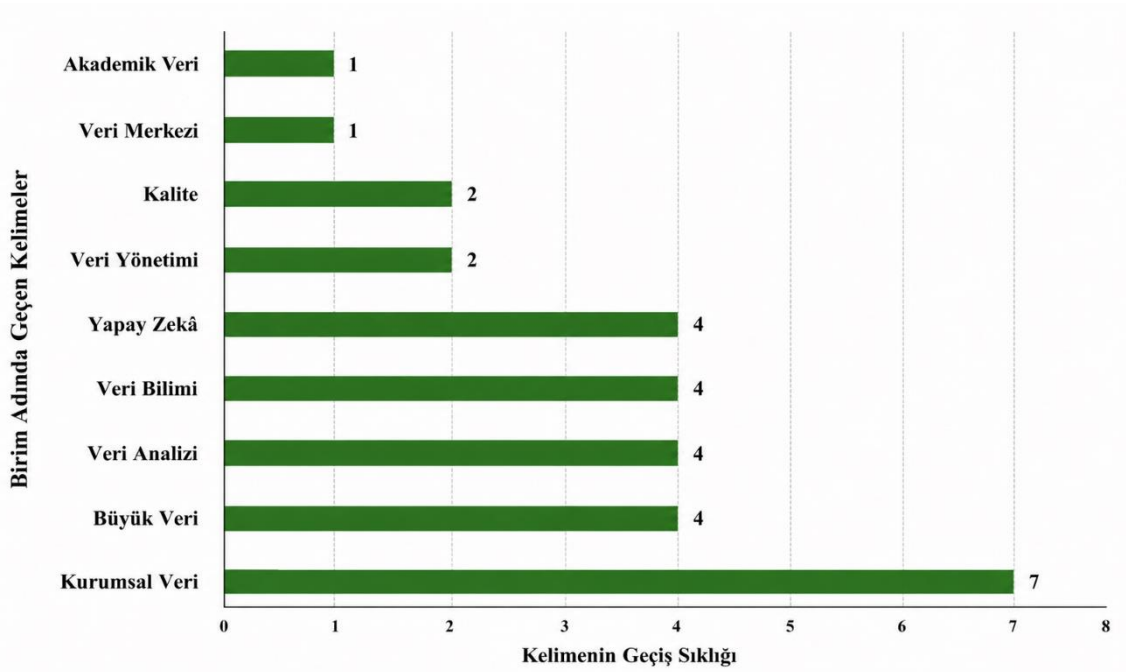
sertifika programları düzenlemek, araştırma ve inovasyon odaklı, teknoloji geliştirme ve veri üretimi, disiplinler arası iş birlikleri yaklaşımlarının öne çıktığı görülmektedir.

Yönergelerle düzenlenen koordinatörlüklerin ve ofislerin amaçları, kurumsal verilerin merkezi yönetimi, veri kalitesi ve bütünlüğünün sağlanması, veriye dayalı karar alma süreçlerinin desteklenmesi, kurumsal performans izleme ve raporlama, dijital dönüşüm ve veri odaklı yönetim olarak tanımlanmıştır. Bu bulgular, araştırma merkezlerinden farklı olarak koordinatörlüklerin doğrudan kurumsal veri yönetişimi amacıyla kurulduğunu göstermektedir.

Görüşme bulgularına göre tüm üniversitelerde veri yönetişimi birimlerinin üst yönetime doğrudan bağlı olarak yapılandırılmıştır. Birimler çoğunlukla rektörlük veya araştırmadan sorumlu rektör yardımcılığı bünyesinde konumlandırılmıştır:

Doğrudan rektörlük çatısı altında... rektör ve rektör yardımcılarına raporlama yapıyoruz (K15).

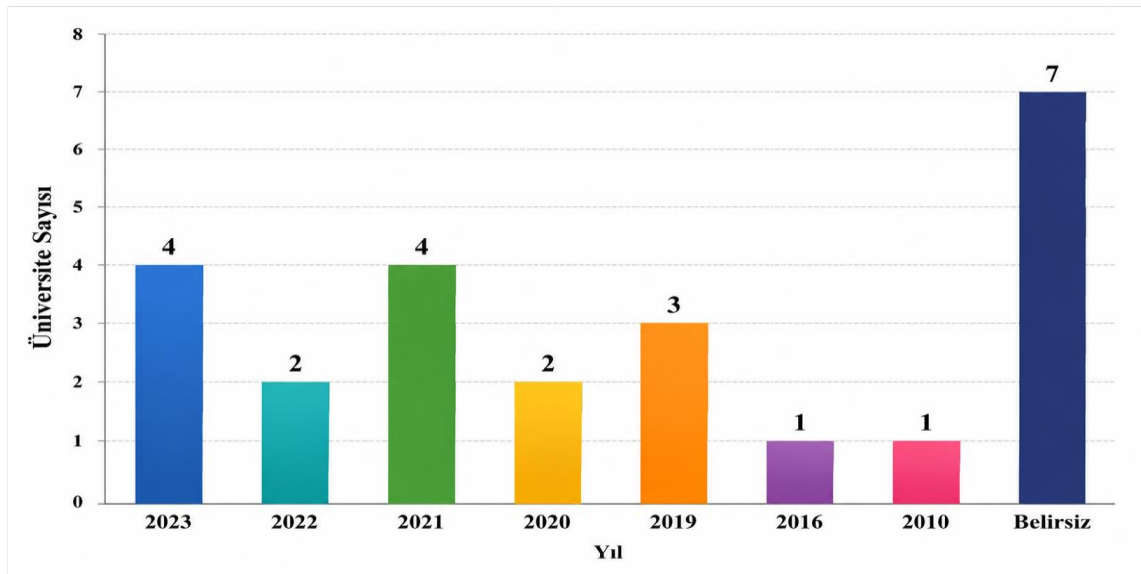
Biz şu anda araştırmadan sorumlu rektörlüğe bağlıyız, onun vasıtasıyla doğrudan rektörle irtibattayız (K16).



Grafik 6. Veri yönetişimi birim adında geçen kelime dağılımı

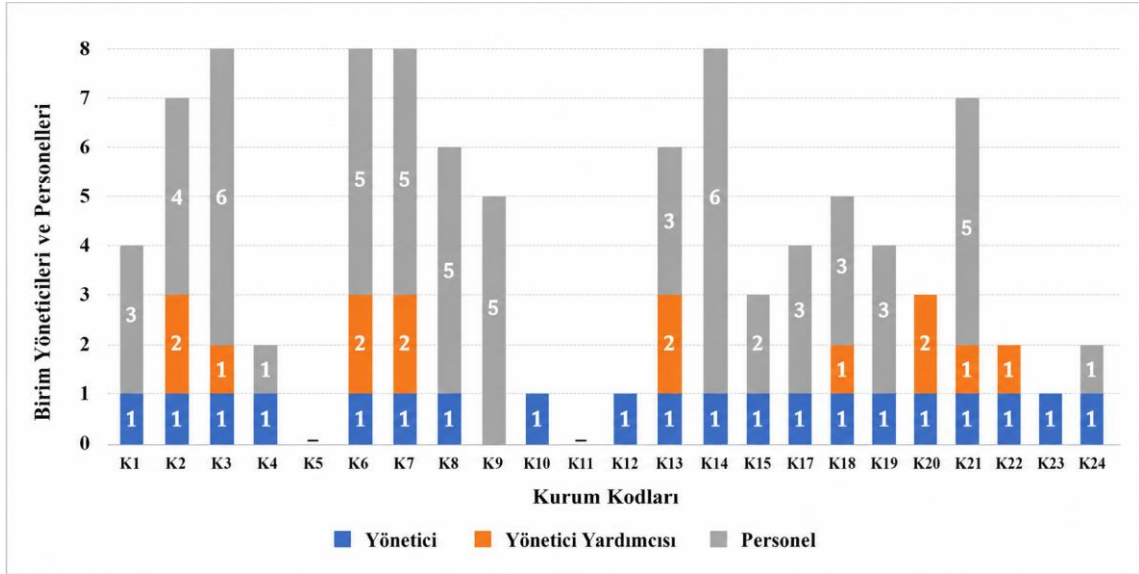
Grafik 6, üniversitelerde kurumsal veri yönetiřimi kapsamında faaliyet gösteren birimlerin adlandırılmasında kullanılan anahtar kelimelerin daęılımını göstermektedir. Birim adlarında en sık geen ifadenin *kurumsal veri* olduęu grlmektedir. niversiteler veri ynetiřiminin kurum geneline yayılan ve merkezi olarak ele alınan bir ynetsel alan olarak konumlandırıldığını ortaya koymaktadır.

Birim adlarında *byk veri*, *veri analizi*, *veri bilimi*, *yapay zeka*, *veri ynetimi akademik veri*, *veri merkezi* ve *kalite* gibi farklı ifadelerinin kullanılması, veri ynetiřimi birimlerinin yapılanması ile ilgili belirsizliklerin ve karmařanın olduęunun bir gstergesi olabilir.



Grafik 7. Veri ynetiřimi birimlerinin kuruluř yılları daęılımı

Grafik 7, niversitelerin veri ynetiřimi birimlerinin kuruluř yıllarına gre daęılımını gstermektedir. řekil incelendiğinde, zellikle 2021 ve 2023 yıllarında kurulan birimlerin sayısındaki artıř gstermektedir. te yandan, kuruluř yılı belirtilmeyen veri ynetiřimi birimlerinin sayısının grece yksek olması dikkat ekicidir.



Grafik 8. Veri yönetiřimi birimi yönetici ve personel daęılımı

Grafik 8’de veri yönetiřimi kapsamında oluřturulan birimlerde görev yapan yönetici, yönetici yardımcısı ve personel sayılarını kurum bazında göstermektedir. Birimlerin tamamına yakınında en az bir yönetici bulunduęu, buna karřılık yönetici yardımcısı pozisyonunun bir veya iki ile sınırlı olduęu, bazı kurumlarda ise bu pozisyonun hiç yer almadıęı görölmektedir. Personel sayıları açısından deęerlendirildięinde, kurumlar arasında farklılıklar bulunduęu bazı üniversitelerde veri yönetiřimi birimlerinin bir veya iki personel ile faaliyet gösterdięi, bazı üniversitelerde ise personel sayısının beř ve üzeri olduęu tespit edilmiřtir. Aynı zamanda veri yönetiřimi birimlerindeki personelin rolleri ve sorumluluk alanları tamamen tanımsız olarak yürütölmektedir. Yönetici ve personeli olmayan birimlerin web sitelerinde konu ile ilgili herhangi bir paylařımda bulunulmamıřtır.

Personel sayısı yüksek olan birimlerin, genellikle veri analizi, büyük veri ve yapay zeka gibi teknik ve analitik iřlevleri de üstlendięi, daha az personelle çalışan birimlerin ise aęırlıklı olarak koordinasyon ve idari iřlevlere odaklandıęı anlařılmaktadır.

Yönetmelikler incelendięinde arařtırma merkezlerinin organizasyon yapısının büyük ölçüde benzer olduęu görölmektedir. İncelenen arařtırma merkezlerin tamamında ortak yönetim yapısı (müdür, yönetim kurulu, danıřma kurulu) dikkat çekmektedir. Tüm

merkezlerde merkezin temsilcisi olan müdür yönetim kurulunun başkanı, faaliyetlerin koordinatörü ve yıllık raporları hazırlayan kişi olarak tanımlanmıştır.

Yine yönetmeliklerde personel ihtiyacının Rektörlük tarafından görevlendirilen personel, proje bazlı görevlendirmeler yoluyla karşılanacağı belirtilmektedir. Ancak hiçbir yönetmelikte veri yönetişimi sorumlusu, veri sahibi, veri sorumlusu, veri kalite yöneticisi gibi veri yönetişimine özgü roller açık şekilde tanımlanmamıştır.

İncelenen yönergelerle göre koordinatörlük yapılarında genel olarak koordinatör (birim yöneticisi), koordinatör yardımcısı, yönetim kurulu, danışma kurulu, koordinasyon kurulu, çalışma grupları veya veri birimleri organizasyon modeli görülmektedir. Örneğin K1’de yönetim kurulunda rektör, rektör yardımcısı, genel sekreter ve bilgi işlem daire başkanı yer almaktadır. K2 örneğinde:

Danışma kurulumuzda Rektör, Rektör Yardımcısı, Strateji Daire Başkanı, Bilgi İşlem Daire Başkanı ve Kalite Komisyonu Temsilcisi var (K2).

Bazı üniversitelerin yönergelerinde kısıtlı da olsa veri yönetişimi rollerine yer verilmiştir. Örneğin K23 yönergelerinde her birimde “Birim Veri Sorumlusu” atanması öngörülmüştür. K1 yönergelerinde veri sahipleri, veri kullanıcıları ve veri sorumlularına ilişkin süreçlerin yönetilmesi belirtilmiştir. K21 yönergelerinde de veri sahipleri ve veri sorumlularına ilişkin süreçlerin yönetimi yer almaktadır. Görüşme metinlerinde de yönergelerdeki uygulamadan bahsedilmektedir:

Her akademik ve idari birime birer veri yöneticisi ve veri sorumlusu atadık, bu kişilerin yetki ve sorumlulukları resmi çalışma esaslarıyla tanımlandı (K2).

Veri giriş sorumlusu ve veri onay sorumlusu belirtiyoruz (K1).

Her birimden veri yöneticisi ve veri sorumlusu görevlendirdik, bunların yetkilerini ve iş akışlarını resmi olarak belirledik (K21).

Görüşme yapılan üniversitelerin tamamında veri yönetişimi birimleri, bir öğretim üyesinin yönetici olarak görevlendirilmesi ve bu yöneticinin altında yer alan yönetici yardımcısı ile çeşitli idari personelden oluşan bir yapı göstermektedir. Ancak bu birimlerde görev yapan personelin çoğunlukla veri yönetimi veya veri yönetişimi alanında uzmanlaşmış kişilerden oluşmadığı görülmektedir. K1 kodlu birim yöneticisi, kendisinin de bu alanın uzmanı olmadığını ifade ederek kurumsal yetkinlik boşluğuna

dikkat çekmiştir. Birimin geçmişte “veri toplama birimi” olarak daha operasyonel bir rol üstlendiği, yaklaşık iki yıl önce veri koordinatörlüğüne dönüştürüldüğü anlaşılmaktadır.

Personel sorunu üniversiteler tarafından şu şekilde vurgulanmıştır:

Personel sorunu büyük bir sorun. Bu kadar büyük bir üniversite yapılanması içerisinde bu kadar az kişinin olması olumsuz tarafı (K2).

Personel eksikliği! Bu bir sıkıntı (K1).

Görüşmelerde, veri yönetişimi birimlerinin başında yer alan öğretim üyelerinin esas görevlerinin eğitim-öğretim ve akademik araştırma faaliyetleri olduğu, veri yönetişimi ile ilgili görevleri ise bu asli sorumluluklarından arta kalan zaman dilimlerinde yürüttükleri ifade edilmiştir. Bu durum, veri yönetişimi süreçlerinin kurumsal düzeyde stratejik ve sürekli bir faaliyet yerine ek görev niteliğinde yürütüldüğünü göstermektedir. Görüşme metinlerindeki şu ifade anlatılan durumu desteklemektedir:

Benim de kısıtlı zamanım var. Çünkü ben burada tek işim bu değil. Akademisyenim, derslerim var (K23).

Birimlerin faaliyetlerinin büyük ölçüde gönüllülük ve ek görev mantığıyla yürütülmesi önemli bir yapısal risk olarak ortaya çıkmaktadır. Katılımcı, akademik görev yükü nedeniyle koordinatörlük çalışmalarının artan zamanlarda yürütülebildiğini belirtmiştir. Bu bulgu, veri yönetişiminin kurumsal sürdürülebilirliği açısından insan kaynağı tahsisi ve rol netliği ihtiyacına işaret etmektedir.

Bazı üniversitelerde veri yönetişimi konusunda sınırlı uzmanlığa sahip personel bulunduğu, hatta bir yönetici tarafından açıkça “Bu alanın uzmanı değilim” ifadesinin kullanıldığı belirtilmiştir (K1). Bu tür ifadeler, veri yönetişimi görevlerinin çoğu kurumda alan uzmanlığına dayalı profesyonel kadrolar yerine, mevcut personelin görevlendirilmesi yoluyla yürütüldüğünü şu ifadeler ortaya koymaktadır:

Veri bilimi uzmanı yok. Biz direkt dışarıdan destek alıyoruz (K9).

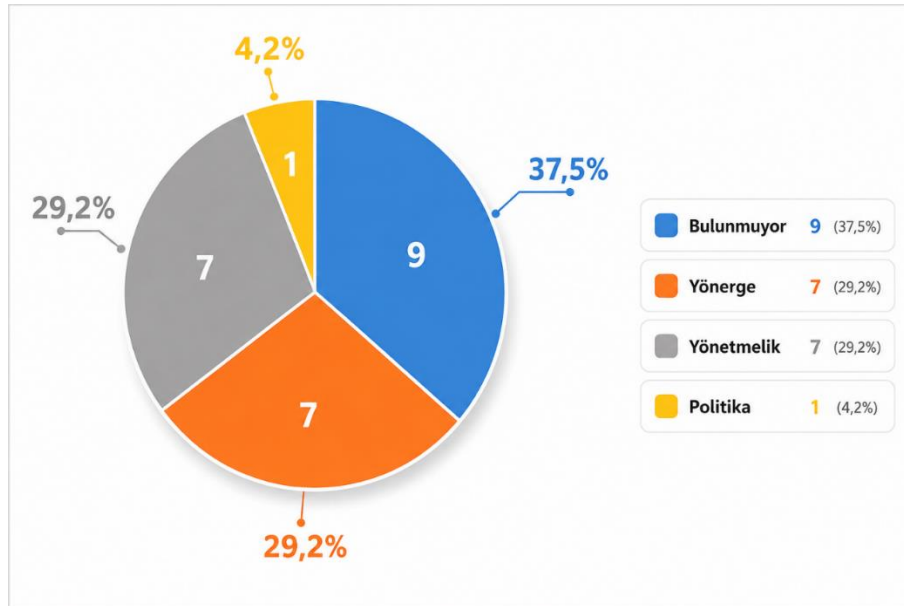
Veri yönetimi başlı başına bir uzmanlık alanı artık (K17).

Bu birim çok büyük bir iş yapıyor. Veri bilimi elemanı bu işin lisans eğitimini almış insanların burada bulunmasının daha doğru olduğunu düşünüyorum (K2).

Buna karşın, az sayıda üniversitede veri bilimi geçmişine sahip personelin bulunduğu görülmektedir. Örneğin, K6 ve K21 kodlu üniversitelerde veri bilimi alanında uzman iki personelin görev yaptığı ifade edilmiştir. K10 kodlu üniversitede ise veri bilimi ve analitik ekibinin bulunduğu, veri ambarı altyapısının geliştirilmesine ihtiyaç duyulduğu vurgulanmıştır. Öte yandan, K9 kodlu üniversitede veri bilimi uzmanının bulunmadığı ve bu tür ihtiyaçlar için dış destek alındığı belirtilmiştir.

Veri yönetişimi birimlerinde görev yapan personelin büyük ölçüde akademik kökenli olduğunu ve profesyonel veri yönetişimi veya veri bilimi uzmanlığının sınırlı olduğunu ortaya koymaktadır. Birçok üniversitede yöneticilik görevleri, yazılım mühendisliği, işletme, istatistik veya mühendislik alanlarından gelen akademisyenler tarafından yürütülmektedir.

Bu durum, Türkiye üniversitelerinde veri yönetişimi alanının kurumsal profesyonelleşme sürecinin henüz erken bir aşamasında olduğunu göstermektedir.



Grafik 9. Veri yönetişimi birimlerinin idari düzenlemeleri

Grafik 9, üniversitelerde kurumsal veri yönetişimi kapsamında faaliyet gösteren birimlerin yasal ve idari düzenleme türlerine göre dağılımını göstermektedir. Veri yönetişimi birimlerinin önemli bir bölümünde (%37,5; n=9) bu alana ilişkin herhangi bir resmî düzenlemenin bulunmadığı görülmektedir. Veri yönetişimi birimlerinin yaklaşık

üçte birinde (%29,2; n=7) faaliyetlerin yönerge ile düzenlendiği, benzer oranda birimde (%29,2; n=7) ise yönetmelik düzeyinde bir idari düzenlemenin bulunduğu görülmektedir.

Buna karşın, bir üniversitede (%4,2; n=1) veri yönetişimine ilişkin politika belgesinin bulunması, politika düzeyinde stratejik yönlendirme araçlarının üniversitelerde henüz yaygınlaşmadığını ortaya koymaktadır. Oysa politika belgeleri, veri yönetişiminin uzun vadeli hedeflerini, ilkelerini ve kurumsal sorumluluklarını tanımlayan temel araçlar arasında yer almaktadır. Üniversitelerde veri yönetişiminin sürdürülebilirliği ve hesap verebilirliğinin sağlanabilmesi için, yönerge ve yönetmeliklerin politika belgeleriyle desteklendiği bir düzenleyici çerçeveye ihtiyaç duyulmaktadır.

Birimler, ihtiyaç duyulan verinin niteliğine göre kurum içindeki farklı birimlerle iletişim kurmaktadır. Bu süreçte en yoğun iş birliği yapılan birimin, veri altyapısının yönetiminden sorumlu olması nedeniyle Bilgi İşlem Daire Başkanlığı olduğu ifade edilmiştir. Bunun yanı sıra Kalite Koordinatörlüğü, BAP Koordinatörlüğü ve Kütüphane ve Dokümantasyon Daire Başkanlığı gibi birimler de veri üretimi ve raporlama süreçlerinde önemli paydaşlar arasında yer almaktadır:

Belirli birimlerden örneğin Strateji Daire Başkanlığından, BAP Koordinatörlüğünden ve bir ya da iki diğer birimden daha kısmi zamanlı olarak görevlendirilmiş (personel) yani, mevcut görevlerine ek olarak gerektiğinde destek olan arkadaşlar var. Bilgi İşlem Daire Başkanlığından çok daha geniş bir grupta da farklı amaçlarla çalışıyorum. Hani ben onlara destek oluyorum, onlar bana destek oluyor (K9).

Koordinatörlükler, bu birimlerin yürüttüğü raporlama faaliyetlerinde kimi zaman destekleyici, kimi zaman ise süreci yönlendiren merkezi bir rol üstlenmektedir. Veri yönetişimi birimlerinin stratejik veri yönetişimi süreçlerinden ziyade, kurumsal veri talebini karşılayan ve farklı birimler arasında veri akışını sağlayan operasyonel bir işlev gördüğünü ortaya koymaktadır:

Görüşme yapılan üniversitelerin büyük çoğunluğunda veri yönetişimi birimlerine tahsis edilmiş bağımsız bir bütçe bulunmamaktadır. Birimler genellikle ihtiyaç duydukları mali kaynakları rektörlük üzerinden talep etmekte ve harcamalar merkezi bütçeden karşılanmaktadır (K1, K2, K9, K15, K16, K17).

Birime ait bütçe yok, üniversitenin uygun gördüğü yapıda bütçe sağlanıyor (K2).

Birimimize ait bütçemiz yok (K1).

K10 ise veri yönetişimi faaliyetleri için proje bazlı bütçeler oluşturulmakta, dijitalleşme ve açık kaynak yazılım geliştirme çalışmaları bu bütçelerle desteklenmektedir.

4.2.2. Veri Standartları

Yönetmelikler incelendiğinde veri yönetişiminin teknik süreçlerine ilişkin tanımların sınırlı olduğu görülmektedir. Merkezlerin çoğunda veri kalitesi, veri sınıflandırma, veri sahipliği, veri standartları, veri sözlükleri, üst veri yönetimi gibi veri yönetişiminin temel bileşenlerine açık ve sistematik biçimde yer verilmemektedir. Merkezlerin daha çok araştırma, analiz, danışmanlık ve eğitim fonksiyonları üzerine kurulduğu anlaşılmıştır. Bu birimler, üniversitelerin akademik ve idari süreçlerinde büyük veri teknolojileri, istatistiksel yöntemler ve yapay zeka uygulamalarının kullanılmasını hedeflemektedir.

İncelenen yönergelerde ise veri kalitesi ve standartlaşmaya ilişkin birkaç düzenleme bulunmaktadır. Örneğin K23 veri sözlüğü, veri haritası ve veri katalogları oluşturulmasını faaliyet alanları arasında saymıştır. K16 yönergesinde veri yönetişimi politikaları, prosedürleri ve standartlarının oluşturulması belirtilmiştir. K21 yönergesinde veri kalitesi doğruluk, bütünlük, güncellik, geçerlilik, gizlilik, erişilebilirlik alt boyutlarıyla tanımlanmıştır. Bu tanımlama, veri kalitesinin çok boyutlu bir kavram olarak ele alındığını göstermektedir.

Üniversitelerde veri standartlaştırma çalışmaları parçalı ve büyük ölçüde uygulama temelli ilerlemektedir. Akademik verilerin toplanmasında ağırlıklı olarak ticari yazılım olan Avesis kullanılmaktadır. Üniversitelerde veri standardizasyonu büyük ölçüde Avesis altyapısı üzerinden yürütülmektedir. Akademik personelin sisteme kurumsal e-posta uzantısı ile tanımlanması zorunluluğu, veri bütünlüğünü sağlamaya yönelik temel bir kontrol olarak uygulanmaktadır. Bu sistem üzerinden akademik personelin yayın ve faaliyet verileri girilmektedir. Aynı sistem üzerinden veri doğruluğunu artırmak amacıyla çok katmanlı bir doğrulama yaklaşımı uygulanmaktadır: Avesis'e veri girişi, Atosis'e akademik teşvik doğrulaması ve Apsis'e ek doğrulama ve ödül süreçleri girilerek veri doğrulaması sağlanmaktadır:

Biz de bu şekilde elimizde Avesis'teki akademik verilerin doğruluğunu %90–%95 oranında sağlamış oluyoruz (K1).

Görüşme bulgularında üniversitelerin verinin kurumsal bir varlık olarak tanımlanması gerekliliğinin farkında olmaları ve bu doğrultuda çalışmalara başlamaları önemli bir gelişme olarak görülebilir:

Kurumsal işleyiş içerisinde iş süreçlerini ilgilendiren herhangi bir veriyi biz kurumsal veri olarak tanımlıyoruz (K2).

Görüşme bulgularına göre üniversitelerde verilerin fiili olarak farklı erişim düzeylerine göre sınıflandırıldığı ve bu sınıflandırmanın çoğu kurumda henüz yazılı bir veri sınıflama politikası haline getirilmediği anlaşılmıştır:

Verileri özel veri, kısıtlanmış veri, kamu verisi, dahili veri gibi ayırıyoruz ama bunu belirleyen yazılı bir veri yönetimi politikası yok (K6).

Kurumsal verileri tanımlamak, sınıflamak... bizim görevimiz (K9).

Verilerin sınıflandırmasını belirleyen yazılı bir belge yok (K21).

Öğrenci verileri, akademik veriler, araştırma verileri, yine bunların içerisinde onun dışında yönetimle ilgili veriler gibi birçok başlığımız var. 7 tane başlık altında toplamıştık. O verileri kurumsal veri olarak tanımlıyoruz ama biz veri toplamıyoruz (K2).

Veri sözlüğü maalesef başlayıp sonuçlanmamış bir çalışma. Üniversite içerisinde çok fazla veri var. Bir ağız birliği, bir ortak dil geliştirebilmek adına böyle bir çalışma (veri sözlüğü) yapılmış (K1).

K2 kodlu üniversitenin öncelikli hedeflerinden biri üniversite genelinde bir veri envanteri oluşturulmasıdır. Bu amaçla her birimde veri temsilcileri belirlenmiş ve bu temsilciler aracılığıyla üst verisi toplanmaktadır.

Biz veri toplamıyoruz, bu verileri konsolide etme ve onlarla ilgili standartlar ve kuralların belirlenmesini sağlıyoruz (K2).

Bu yaklaşım, modern veri yönetişimi literatüründe önerilen federatif veri yönetişimi modeli ile uyumludur.

Üniversitelerde veri erişimi ve paylaşımının rol tabanlı yetkilendirme modeliyle yürütüldüğünü göstermektedir. Her birimde tanımlanan veri yöneticileri ve veri sorumluları sistem üzerinden veri girişini gerçekleştirmektedir. Benzer biçimde, bazı

üniversitelerde erişim yetkileri görev tanımlarına göre belirlenmektedir. Ancak bu yapı henüz yayımlanmış kurumsal bir sınıflama politikası ile desteklenmemektedir:

Dekanın, rektör yardımcısının, kütüphane daire başkanının görebileceği veriler farklı... herkes kendi yetki alanına göre verileri görebiliyor (K21).

Bu bulgular, veri sınıflamasının üniversitelerde uygulama düzeyinde kullanıldığını ancak yönetim düzeyinde henüz kurumsallaşmadığını göstermektedir.

Üniversiteler, verilerin anlamlandırılabilmesi için üst veri ve ortak tanımların kritik önemde olduğunu farkındadır. Hedef metinlerinde en sık karşılaşılan temalardan biri, kurumsal veri yönetişimi politika ve prosedürlerinin geliştirilmesi, güncellenmesi ve uygulanmasıdır. Veri ambarı tasarımı, veri sözlüğü çalışmaları, veri yaşam döngüsünün yönetimi ve veri entegrasyonu bu kapsamda öne çıkmaktadır. Özellikle kurumsal olarak aynı dili konuşur hale gelinmesini hedeflemektedirler:

Göstergelerin meta verilerinin ve tanımlarının çok düzgün yapılması gerektiğini tespit ettik. Üniversite genelinde veri sözlüğü çalışması yaptık (K2).

Hangi veri hangi birimde vardır, göstergelerin meta verileri nelerdir? bunların standardını oluşturduk ve yazılımımıza entegre ettik (K17).

Birim veri temsilcileri bize ‘bizim şu verilerimiz var’ diye üst verilerini sağlıyor (K2).

Üniversitelerin web siteleri incelendiğinde veri bütünlüğü, doğruluk, tutarlılık, güncellik, gizlilik ve erişilebilirlik gibi veri kalitesi boyutları güçlü biçimde vurgulanmaktadır. Tutarsızlıkların tespiti, güvenilirliğin sağlanması ve kalite sürdürülebilirliği bu tema altında yer almaktadır. Görüşme bulgularında veri kalitesinin özellikle sıralama, performans ve kalite süreçleri açısından bir gereklilik olarak ele alınmaktadır. Üniversiteler veri kalitesinin sistematik biçimde izlenilmesi ve yönetilmesi gerekliliğinin farkındadırlar:

Veri tabanlarından gelen veriler doğrulanmış veri ancak manuel olarak eklediği veri doğrulanmış veri değil. Bunları biz tekrar kontrol ediyoruz. Bu verilerinde doğrulanmasını istiyoruz. Çeşitli komisyonlar tarafından (veriler) kontrol ediliyor. (K1).

Web of Science’tan geliyorsa doğrulanmış veri. Manuel girilen veri doğrulanmış veri değil (K16).

Verinin doğruluğunu da ben kontrol ediyorum (K9).

Verileri topluyoruz, hataları ayıkliyoruz, doğruluyoruz. Sonra analiz ediyoruz (K10).

Üniversitelerde verilerin doğrulanması konusunda herhangi bir yazılı belge ya da standart kullanımına rastlanmamıştır. Kurum içinde yazılı olmayan şekilde belirledikleri standartlar veri kalitesini belirlemektedir. Bu durum standart eksikliğinden kaynaklanan veri tutarsızlığına işaret etmektedir. Bu nedenle veri yönetişimi birimleri veri sahipliğinin belirlenmesi, veri formatlarının standardizasyonu, veri sorumluluklarının tanımlanması, mükerrer veri üretiminin önlenmesi gibi alanlarda kural koyucu rol üstlenmektedir. Bu durumu şu şekilde açıklayabiliriz:

Veri standartlarını oluşturacağız, veri formatlarına karar vereceğiz, veri sorumluluklarını belirleyeceğiz. Öğrenci sayısı bir yerde 500 çıkıyor, başka yerde 600 çıkıyor. Çünkü veriler belli bir standartta tutulmuyor (K2).

Veri yönetişimi birimleri düzenli izleme ve raporlama faaliyetleri yürütmektedir. Veri yönetişimi, üst yönetime akademik verilerin rapor halinde sunulması gerekliliği ile bağdaştırılmıştır:

Haftalık yayın verilerini, aylık araştırma göstergelerini izliyoruz. Raporları üst yönetime sunuyoruz (K15).

Altı ayda bir akademik performans raporları hazırlıyoruz (K9).

6 ayda bir kontrol sağliyoruz. Verileri raporlama işlemleri sonucunda yayınlıyoruz (K23).

Üniversitelerde çok sayıda farklı sistem bulunmakta ve bu sistemlerin entegrasyonu Avesis ve Bilgi İşlem Daire Başkanlığı sağlamaktadır. Aynı zamanda bu sistemlerin entegrasyonu veri yönetişiminin temel zorluk alanlarından biri olarak ortaya çıkmaktadır. Üniversiteler aşağıdaki ifadelerle bu zorluğun farkında olduklarını dile getirmişlerdir:

Avesis, Atosis, Apsis... hepsi farklı sistemler, bunları entegre etmeye çalışıyoruz (K23).

Bu yazılımların (32'den fazla kendi geliştirdikleri yazılımdan bahsediyor) en üstünde bir varlık yönetim sistemi var, veriler burada beraber görünüyor (K6).

İncelenen yönergelerde özellikle K1 ve K21 üniversitelerinde veri yaşam döngüsü açık biçimde tanımlanmıştır. Bu süreçler verinin tanımlanması, üretilmesi, bütünleştirilmesi,

yaşam döngüsü boyunca kalite ve güvenliğinin sağlanması şeklinde ifade edilmiştir. Bu yaklaşım, veri yönetişimi literatüründe yer alan veri yaşam döngüsü modeline doğrudan karşılık gelmektedir. Veri, üniversitelerde üretim, doğrulama, kullanım, arşivleme ve raporlama aşamalarını içeren bir yaşam döngüsü içerisinde yönetilmektedir. Görüşme metinlerindeki şu ifadeler bu durumu desteklemektedir:

Her hafta üretilmiş verilerin arşivlenmesi söz konusu (K9).

Topladık, ayıkladık, doğruladık, analiz ettik... sonra kurumsal politikalara dönüştürdük (K10).

Veri yönetişimi süreçleri, kalite, akreditasyon ve denetim mekanizmalarıyla doğrudan ilişkilidir. Bu bağlantı şöyle açıklamaktadır:

Akreditasyon sürecinde verilerin sunulması ve denetimlere hazırlıkta aktif rol alıyoruz (K16).

4.2.3. Veri Erişimi ve Paylaşımı

Yönetmelikler incelendiğinde veri erişimi ve paylaşımı faaliyet alanı olarak büyük veri setlerinin toplanması, işlenmesi ve görselleştirilmesi belirtilmiştir. Veri kümelerinin kişisel verilerden arındırılarak araştırmacıların kullanımına sunulması sağlanmaktadır. Verilerin paylaşılabileceği fiziksel veya sanal ortamların oluşturulması öngörülmektedir. Bu ifadeler, veri yönetişimi açısından veri erişimi, veri paylaşımı, veri anonimleştirme başlıklarının sınırlı düzeyde yer aldığını göstermektedir.

Akademik veri erişiminin büyük ölçüde Avesis ve ilişkili sistemler üzerinden yürütüldüğü görülmektedir. Görüşme bulgularına göre kurumlarda kurumsal veri erişimi henüz merkezi bir platform üzerinden yürütülmemektedir. Uzun vadede tüm kurumsal verilerin tek bir gösterge paneli (dashboard) üzerinden izlenmesine yönelik bir yazılım projesi planlanmaktadır. Üniversitelerin veri erişimi ve paylaşımı konusunda daha başlangıç seviyesinde olduğunu aşağıdaki cümleler net bir şekilde ortaya koymaktadır:

Biz veri istemiyoruz, sadece üst verilerini istiyoruz. Bu veriler kimlerin erişebildiğinin bilgilerine ihtiyacımız var. Bundan sonra şu veriler şu formatlarda tutulacak diye direktifleri temsilciler aracılığıyla göndereceğiz. İstedğimiz zaman sorumluluk dahilinde raporlayacak bir sistem kurgulamaya çalışıyoruz. Şu anda daha envanter aşamasındayız (K2).

Her birimde birim veri yöneticisi ve sorumlusu olmak üzere en az iki kişi tanımladık. Veri girişini sağlıyorlar. Veri göstergeleri ilgili tanımlar yapılıyor ve bizim onayımıza sunuluyor. Biz de bunu kontrol ediyoruz, uygun ise onayını veriyoruz. Geçmiş yılda girmiş olduğu veri ile bu yıl arasında büyük sapma var mı diye bakıyoruz. Grafik yönetim modülüyle web sayfası olarak yayınlatabiliyoruz. E-posta listesini sisteme eklediğinde o göstergeyle ilgili veriyi kişilerden talep edebiliyoruz (K21).

Üniversitelerin web sayfalarında ise doğru, güvenilir, tutarlı ve erişilebilir veri kavramlarının özellikle vurgulandığı görülmektedir. Veri kalitesinin güvence altına alınması, veri bütünlüğünün korunması ve veriye erişimin kolaylaştırılması, veri yönetişimi birimlerinin temel sorumluluk alanları arasında yer almaktadır. Aynı zamanda veri erişimi ve paylaşımının üniversitelerde kurumsal görev tanımlarına bağlı biçimde belirlendiği ama yazılı bir belgelerinin olmadığı anlaşılmıştır. Görüşme bulgularına göre veri erişimi ve paylaşımı rol ve yetki temelli olarak kurgulandığını şu ifade açıklamaktadır:

Dekanın, rektör yardımcısının, kütüphane daire başkanının görebileceği veriler var. Herkes kendi yetki alanına göre verileri görebiliyor. Üst yönetim bütün verileri görebiliyor ama verilerin ham halini değil, özet halini (K6).

Bu yaklaşım, veri erişiminin en az yetki ilkesiyle sınırlandırıldığını ve yönetici seviyesindeki rollerin daha geniş, operasyonel seviyelerde ise daha kontrollü erişim uygulandığını göstermektedir. Veri erişimi ve paylaşımı, veri yönetiminden sorumlu birim tarafından belirlenen çerçeve doğrultusunda birim temsilcileri üzerinden yürütülmektedir:

Kurumsal veri yönetim koordinatörlüğünün görevi, hangi veri tabanlarında tutulduğu, bu verilerin kimlerin erişebildiği ve veri sorumluluklarının kimlerde olduğu bilgilerini belirlemek (K2).

Üniversitelerin web sitelerinde araştırma performansı, ulusal ve uluslararası sıralamalar, kalite güvence sistemleri ve Yükseköğretim Kalite Kurulu (YÖKAK) süreçleri ile doğrudan ilişkili görevler öne çıkmaktadır. Kurum içi değerlendirme raporlarının hazırlanması, performans göstergelerine ilişkin verilerin toplanması ve analiz edilmesi gibi faaliyetler bu kapsamda vurgulanmaktadır. Görüşme verilerinde benzer şekilde üniversitelerde veri paylaşımı büyük ölçüde kurum içi karar alma ve performans izleme amaçlarına yöneliktir. Veriler, rektörlük, rektör yardımcıları, genel sekreterlik, strateji

daire başkanlığı ve kalite birimleri arasında düzenli olarak paylaşılmaktadır. Bu süreç şöyle tanımlanmaktadır:

Haftalık yayın sayılarını, aylık araştırma üniversitesi göstergelerini izliyoruz. Ana raporları rektör yardımcılığına ve araştırma üniversitesi yürütme kuruluna veriyoruz, genel sekreterlik ve strateji daire başkanlığına da bilgi geçiyoruz (K15).

Akreditasyon sürecindeki adımlar doğrultusunda verilerin erişilebilmesi için idari ve akademik taraftaki yayın süreçlerine ilişkin verilerin paylaşılması gerekiyor. Bu aşamada ben yardımcı oluyorum (K17).

K17'deki durum, veri paylaşımının üniversitelerde süreç odaklı ve yönetsel gereksinimlere bağlı biçimde gerçekleştiğini göstermektedir.

Üniversitelerin web sitelerindeki bilgiler değerlendirildiğinde, ulusal ve uluslararası üniversite sıralama sistemleri, YÖK, TÜBİTAK ve benzeri kurumların değerlendirme süreçleri için veri üretimi ve analiz faaliyetleri önemli bir yer tutmaktadır. Akademik performans, araştırma çıktıları ve kurumsal göstergeler gibi başlıklara rapor hazırlama amacı yoğunlaşmaktadır. Görüşme verilerinde benzer şekilde üniversiteler, kurum içi ve kurum dışı veri erişim ve paylaşımı yaptıklarını söylemişlerdir. YÖK, TÜBİTAK, sıralama kuruluşları (THE, QS, URAP vb.) ve diğer kamu kurumlarıyla sürekli veri alışverişi yürütmektedir.

YÖK izleme ve değerlendirme, sıralamalar. Üniversiteden izlenen her şeyin içindeyiz (K1).

Orcid, YÖKSİS, PubMed, Web of Science, Scopus üzerinden verileri çekebiliyoruz (K9).

Üniversitelerden temel verileri alıyoruz. Yayınları uluslararası veri tabanlarından çekiyoruz. TÜBİTAK'tan veri alıyoruz (K10).

Veri erişim ve paylaşımının çok aktörlü bir yönetim mimarisi içinde işlediğini ortaya koymaktadır.

Avesis sistemi üzerinden yapılan veri erişimi ve paylaşımlarında yetkilendirme ve loglama süreçlerinin bulunduğu ifade edilmektedir:

Avesis açık arşivine yetkilendirme doğrultusunda erişiyoruz. Verilerin çekimini gerçekleştiriyoruz. Bilgi işlem tarafından IP blokları uygulanıyor (K16).

4.2.4. Veri Depolama, Yedekleme, Güvenlik ve Gizlilik

Veri güvenliği ve mevzuat uyumu, incelenen yönergelerin çoğunda temel amaçlar arasında yer almaktadır. K7 koordinatörlüğünde veri etiği ve güvenliği ayrı bir birim olarak yapılandırılmıştır. K23 yönergesinde KVKK'ya uyum ve veri mahremiyeti temel amaçlardan biri olarak tanımlanmıştır. K16 yönergesinde veri yönetişimi çerçevesi içinde veri kullanım politikalarının oluşturulması öngörülmektedir.

Özellikle K1 kodlu üniversitenin yönergesinde veri entegrasyonunu sağlanabilmesi için tekrarlı veri girişinin önlenmesi, veriye kaynağından erişim, sistemler arası birlikte çalışabilirlik, verilerin tek merkezde toplanması gibi ilkeler açık biçimde yer almaktadır. Bu yaklaşım, kurumsal veri ambarı ve tekil veri kaynağı prensiplerine karşılık gelmektedir.

Kurumsal veri yönetimi koordinatörlüğü ve ofis türündeki birimlerin web sitelerinde de veri güvenliği, gizliliği, bütünlüğü ve erişilebilirliği kavramlarının belirgin biçimde öne çıktığı görülmektedir. Veri depolama, yedekleme ve güvenlik konularında veri yönetişimi, stratejik ve operasyonel sorumluluklar olmak üzere ayrılmaktadır. Stratejik veya kural koyucu rol koordinatörlük bünyesinde operasyonel uygulama ise Bilgi İşlem Daire Başkanlığı tarafından yürütülmektedir. Güvenlik altyapısının Bilgi İşlem tarafından yürütüldüğü ve ISO 27001 gibi standartlara uyum sağlandığı ifade edilmiştir:

Bilgi işlemde bilgi güvenliğiyle ilgili bazı standartlara uyuluyor, işte 27001 vesaire (K2).

Veriyle ilgilenen birimin Bilgi İşlem Daire Başkanlığıyla çok yakın çalışması gerekiyor (K1).

Politikamızın içerisinde veri güvenliğini Bilgi İşlem Dairesi Başkanlığı sağlar diye belirleyeceğiz (K2).

Koordinatörlüğün bu alandaki rolü güvenlik politikalarını tanımlamak, sorumlulukları belirlemek, standartlara atıf yapmak şeklinde konumlanmaktadır. KVKK uyumuna yönelik yerleşik bir uygulama örneği şu şekildedir:

Veri gizliliği ile ilgili gizlilik butonu var. Kişisel verileri kapsıyorsa kişiler hiçbir şekilde sorgulama yapamıyorlar. Yetkisi varsa verileri görebiliyor fakat indiremiyor. Eğer kişisel bilgi içeriyorsa ona hiçbir şekilde erişemiyor. Gösterge rapor yönetimi modülünden ilgili veriler görülebiliyor (K21).

Görüşme metinleri analizlerinde üniversitelerde verinin çok sayıda farklı bilgi sistemi üzerinde tutulduğunu ve bu sistemlerin giderek daha bütünleşik bir mimariye dönüştürülmeye çalışıldığı sonucuna varılmıştır. Bu yapı şu şekilde tanımlanmaktadır:

Avesis, Atosis, Apsis, Verisis... bunların hepsi farklı amaçlar için kullanılan yazılımlar. Şu anda bunları entegre etmeye çalışıyoruz. Bu yazılımlar üniversitemizin Bilgi İşlem Daire Başkanlığı sunucularında tutuluyor. (K1).

Bu yazılımların en üstünde bir varlık yönetim sistemi var. Bütün veriler burada beraber görünebiliyor. Herkese açık bir sistem değil, veri yöneticileri ve üst yöneticiler görebiliyor (K21).

Bu ifadelerle üniversitelerde verinin dağıtık sistemlerde tutulduğunu, yönetsel bütünlüğün merkezî platformlar aracılığıyla sağlanmaya çalışıldığını göstermektedir.

Veri güvenliğinin en kritik bileşenlerinden biri düzenli yedekleme ve arşivleme süreçleridir. Bu süreç şu şekilde açıklamaktadır:

Her hafta üniversitemiz tarafından üretilmiş verilerin arşivlenmesi söz konusu (K23).

Avesis dışarıdan bir sistem. Tüm arşivleme işlemleri Avesis gerçekleştiriyor (K9).

Verilerin yedeklenmesi ve depolanması ile ilgili açıkçası teknik kısımda çok bir bilgim yok. Ama bu verilerin kendi sunucularımızda tutulması, felaket senaryosuna karşı da yedeklerinin farklı bir yerde tutulması gerekiyor. (K1).

Depolama ve yedekleme süreçleri dış sistemlerle birlikte yürütülmektedir. Verilerin kurum içinde, ticari yazılım sağlayıcılarının altyapılarında eş zamanlı olarak güvence altına alındığını göstermektedir. Bu durumu şu ifade açıklamaktadır:

Avesis, depolama ve yedekleme için Bilgi İşlem Daire Başkanlığı'ndaki sunucularda tamamen otomatik şekilde kendi sistemini kullanıyor. Bizde bu sistemlere erişim sağlayabiliyoruz (K9).

Depolama, yedekleme ve güvenlik için kullanılacak yazılımın ticari bir yazılım olmaması gerekiyor (K1).

Veriye erişim, çok katmanlı güvenlik önlemleriyle korunmaktadır. Veri erişimi, güvenlik ve gizlilik mekanizmalarıyla sıkı biçimde sınırlandırılmaktadır. Erişimin kullanıcı adı/şifre üzerinden ve ağ güvenliği, IP kısıtları ve yetkilendirme süreçleriyle kontrol edildiğini göstermektedir. Bu mekanizma şu şekilde tanımlanmaktadır:

Veri gizliliği ve veri politikası yönünden çift aşamalı girişler var. IP blokları tanımlanıyor. Sadece benim ve Bilgi İşlem izniyle erişim sağlanabiliyor (K9).

Bu uygulamalar, üniversitelerde veri depolama, yedekleme ve güvenliği işlemlerinin Avesis ticari yazılım bünyesinde gerçekleştiği, Bilgi İşlem sunucularında depolandığını izleyici ve denetleyici mekanizmalarla sürekli olarak yönetildiğini göstermektedir.

4.2.5. Veri Kültürü

Görüşme bulguları, kurumda veri yönetişiminin önündeki en kritik zorluklardan birinin kurum kültürü dönüşümü olduğunu açık biçimde ortaya koymaktadır. Veri yönetişimi biriminin görevleri veri farkındalığı oluşturma, birim temsilcilerini eğitme, tüm çalışanlara yönelik bilinçlendirme, veri kültürü geliştirme faaliyetleri yer almaktadır. Bu faaliyetleri gerçekleştirme anlamında birimlerin yeni süreçleri iş yükü olarak görmesi, veri temsilcilerinin rolü yanlış anlaması, yeniliğe kapalı organizasyonel yapı, büyük ve köklü üniversite olmanın getirdiği sistem mirası ya da küçük ve yeni üniversite olmanın tecrübesizliği kültürel engeller olarak karşımıza çıkmaktadır. Buna karşılık en önemli kolaylaştırıcı unsur olarak üst yönetim desteği ve rektör düzeyinde sahiplenme öne çıkmaktadır:

Üst yönetimin desteği önemli. Rektör hocanın birebir ilgilendiği bir konu (K17).

Aslında bir kurum kültürü yaratmak bu konuyla ilgili. Birim temsilcilerini sonra tüm kurum çalışanlarını veri konularında aydınlatmak bizim görevimiz. Bu verileri neden tutmalıyız? veri yönetimi nedir? bunlarla ilgili farkındalık yapmak da bizim görevimiz. Ama kurum kültürünü değiştirmek özellikle eski üniversitelerde zor (K2).

Üst yönetimlerin değişimi veri yönetişimi ile ilgili tüm tercihleri ve teknik stratejileri etkileyebilmektedir:

Üniversitenin kendi geliştirdiği yazılım vardı ama yönetim değişince vazgeçildi, Avesis satın alındı (K1).

Yazılım yoktu, kendim geliştirdim (K10).

Yönetim değişince yapılanlar çöpe atıldı. İnsanlar demoralize oldu (K16).

Yönetim değiştikçe stratejilerin değişmesi en büyük sıkıntımız (K17).

Kuruluş aşamasında yaşanan en önemli sorunlardan biri üniversitelerin birimlerinin direnci olmuştur. Özellikle faaliyet temelli verilerin akademik birimler tarafından tutulması gerektiğinde başlangıçta zorluk yaşandığı ifade edilmiştir. İdari birimlerde de ek iş yükü olarak bakılarak belirli bir direnç yaşanmıştır:

En büyük sorun, kendimizi ne düzeyde anlatabildiğimiz (K2).

Birim veri temsilcisi seçtik, sordukları ilk soru ‘biz nereye ne kadar veri gireceğiz’ oldu (K1).

İlk göreve geldiğimizde veri toplamada çok büyük sıkıntı yaşamıştık. Kurumsal hafızanın olmadığını ilk etapta gözlemledik. Dirençle karşılaşıyorsunuz. Faaliyet temelli verilerin bir şekilde ilgili birimlerde tutulması gerekiyor. Bu sistemle ilgili bir kullanım kılavuzu da var. Temel fonksiyonların nasıl idame ettirileceğine ilişkin videolar var. İş yükünün fazla olması nedeniyle herkesin arta kalan vakitlerinde yapabildiği bir iş (K21).

Üniversitelerde veriye dayalı karar alma kültürünün henüz tam olarak yerleşmediğini, güçlü bir farkındalık sürecinin yaşandığını ortaya koymaktadır. Üniversitelerin veri yönetişimi politikaları olmamalarına rağmen veri politikası ihtiyaçlarının farkına varmaktadırlar:

Ölçemezseniz yönetemezsiniz... Veriye dayalı stratejiler ve politikalar geliştirmemiz gerekiyor (K10).

Politika kesinlikle olması gereken bir şey (K1).

Politika geliştirilmeli. Üniversitenin veri politikasına ihtiyacı olduğunu düşünüyorum (K9).

Politikamız var, yayınlanması bekleniyor (K21).

Henüz belge haline gelmedi açıkçası (K15).

Veri yönetimine dair bir politika. Maalesef yok (K6).

Kurumlarda veri farkındalığı oluşturma yönünde çabalar bulunmaktadır. Akademik personele yönelik sistem kullanım eğitimleri düzenli aralıklarla fakülte bazında verilmektedir. Bu eğitimler çevrim içi veya yüz yüze gerçekleştirilmektedir. Eğitimlerde

özellikle kurumsal ID sorunları, profil doldurma sistem kullanım hataları üzerine odaklanıldığı ifade edilmiştir.

Biz bunu (eğitimi) belli aralıklarla akademik kadroya yapıyoruz. Fakülte sistemi (Avesis) kullanma eğitimleri veriyoruz (K16).

(Eğitim) Bazen online oluyor, bazen fiziksel oluyor. Eğitim sırasında yaşanan problemleri değerlendiriyoruz (K9).

Görüşmeler, veri yönetişiminin akademik ve idari kültür arasında yeni bir etkileşim alanı oluşturduğunu göstermektedir:

Akademik ve idari birimler bir arada çalışıyor. Bu sürecin kurumsal yürütülmesi gerektiğini fark ettik (K2).

Veri yönetişimi uygulamalarının kurumsal sürdürülebilirliği, çalışanların bu süreçleri sahiplenmesine bağlıdır. Birçok kurumda yönerge, yönetmelik bulunurken kapsamlı veri yönetişimi politikası henüz oluşturulmamıştır.

5. BÖLÜM

ÜNİVERSİTELERE YÖNELİK VERİ YÖNETİŞİMİ MODEL ÖNERİSİ

Araştırmanın bu bölümünde Türkiye’deki üniversitelerde veri yönetişimine yönelik süreçleri katmanlar halinde sunan bir kavramsal model önerisinde bulunmaktadır. Model önerisinin geliştirilmesi için veri yönetişimi ile ilgili literatür incelenmiş ve ulusal ve uluslararası uygulama örnekleri ile geliştirilen farklı modeller değerlendirilmiştir. Aynı zamanda üçüncü bölümde verilen araştırmanın sınırlılıkları kapsamında ulusal ve uluslararası yasal düzenlemeler dikkate alınmıştır. Araştırma için toplanan dördüncü bölümde sunulan Türkiye’deki üniversiteler ile yapılan yarı yapılandırılmış görüşme veriler ve araştırma sınırlılıkları içinde belirlenen ABD, AB, Avustralya, BK kapsayan veri yönetişimi politika belgeleri verilerinde de yararlanılmıştır.

Bu bölümün içeriğinde ilk olarak Türkiye’de üniversitelerin nasıl bir model izlemesi gerektiği ve bu doğrultuda önerilen modelin amacı, dayandığı ilkeler ve genel bir açıklaması yapılmıştır. Ardından modelde yer alan katmanlar ilgili literatür, ulusal ve uluslararası mevzuat, politika belgeleri, üniversite çerçeveleri ve kurum görüşmeleri ile ilişkilendirilerek sunulmuştur. Bölümün sonunda ise önerilen modele ilişkin bir tartışmaya yer verilmiştir.

5.1. ÜNİVERSİTELER İÇİN VERİ YÖNETİŞİMİ MODELİ

Günümüzde üniversiteler, eğitim, araştırma, toplumsal katkı ve idari faaliyetler kapsamında çok çeşitli veri türlerini üretmekte ve kullanmaktadır. Ancak bu veriler çoğunlukla farklı birimlerde, farklı sistemlerde ve standartlardan yoksun biçimde yönetilmektedir. Bu durum, veri kalitesinin düşmesine, veri bütünlüğünün sağlanamamasına ve veri temelli karar alma süreçlerinin zayıflamasına yol açmaktadır.

Bunun yanı sıra üniversitelerde veri yönetişimi uygulamaları çoğu zaman parçalı, teknik odaklı ve kurumsal stratejilerle yeterince bütünleşmemiş durumdadır. Özellikle veri sahipliği, karar hakları, veri paylaşımı ve veri güvenliği konularında kurumsal düzeyde tanımlanmış politika eksiklikleri dikkat çekmektedir. Ayrıca mevcut veri yönetişimi

yaklaşımları, üniversitelerin federatif yapısını, akademik özgürlük ilkesini ve araştırma verisi yönetimi gereksinimlerini yeterince dikkate almamaktadır.

Üniversitelerdeki verinin, tek merkezden üretilmesi ve yönetilmesi mümkün değildir. Çünkü eğitim, araştırma, insan kaynakları, kalite, idare, öğrenci işleri, kütüphane, uzaktan eğitim, bilimsel üretim ve dış paydaş ilişkileri farklı iş mantıklarına sahiptir. Buna karşılık kurumsal düzeyde ortak standartlar, ortak roller, ortak veri dili ve ortak güvenlik-etik ilkeleri olmadan da sürdürülebilir bir veri yönetişimi kurulamaz. En uygun merkezî ilke ve standartlarla yönlendirilen, uygulamada birim temelli sorumluluğu koruyan federatif bir modeldir.

Literatürde veri yönetişimi alanında DAMA, DCAM ve Veri Yönetişimi Enstitüsü gibi kapsamlı çerçeveler geliştirilmiş olmakla birlikte, bu modellerin büyük ölçüde genel organizasyon yapıları için tasarlandığı görülmektedir. Aynı zamanda her ülkenin kurumsal yapısı, veri kültürü farklı olduğu için çerçeveler Türkiye için uygunluk göstermeyebilir. Üniversiteler özelinde geliştirilen veri yönetişimi çerçeveleri ise genellikle belirli bileşenlere odaklanmaktadır.

Bu bağlamda, üniversitelere özgü ihtiyaçları karşılayan, veri yönetişimi yapısı ile veri yönetişimi politikalarının geliştirilmesini bütünselik biçimde ele alan, uygulanabilir ve sürdürülebilir bir modele ihtiyaç duyulmaktadır. Veri yönetişimi ile ilgili mevcut çalışmalar incelendiğinde üniversiteler için veri yönetişimi süreçlerinde aşağıdaki boşlukların olduğu düşünülmüştür:

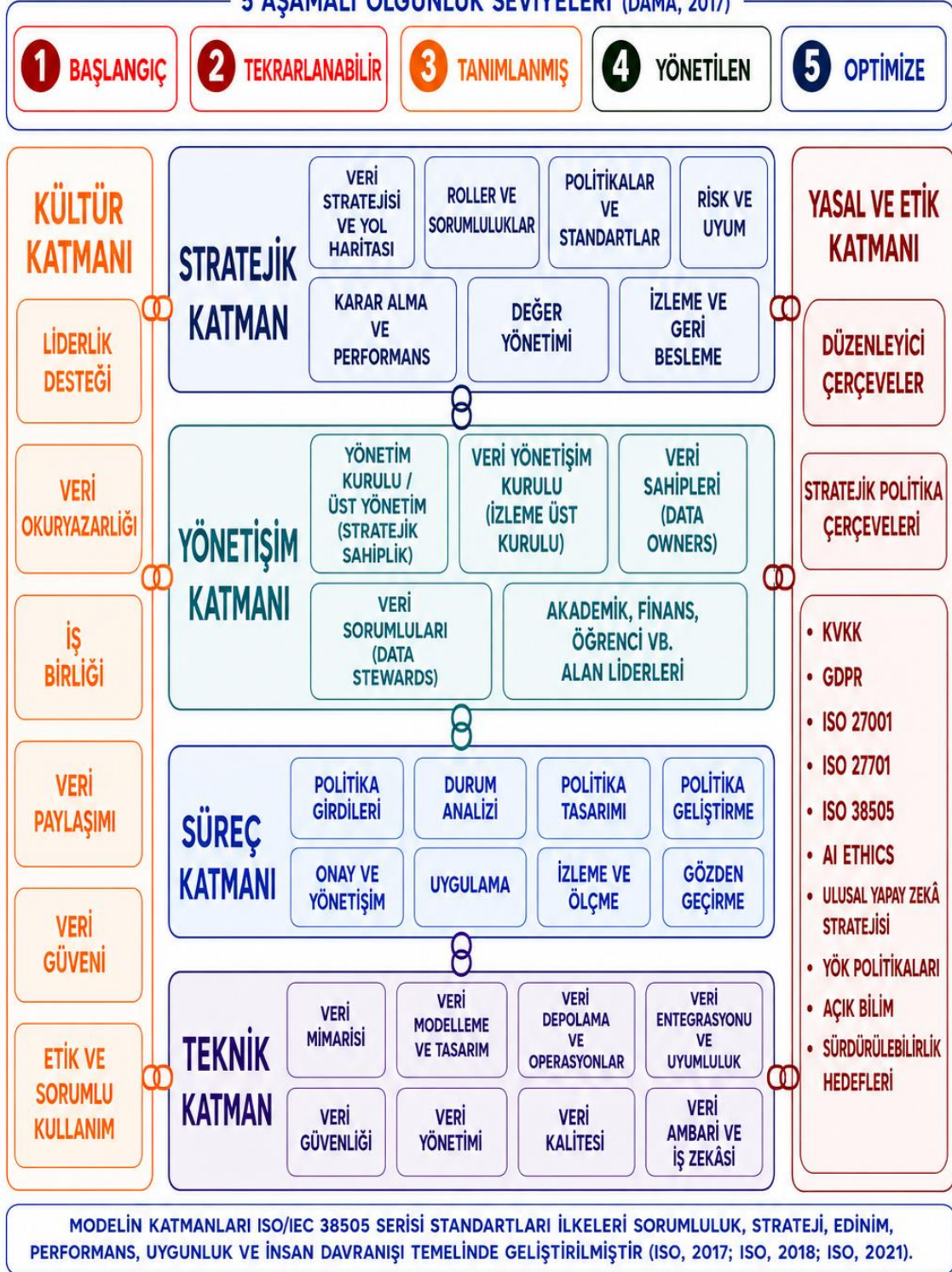
1. Yapı ve süreç entegrasyonu eksikliği: Çoğu model ya organizasyonel yapıya ya da süreçlere odaklanmaktadır.
2. Politika geliştirme sürecinin yetersiz ele alınması: Veri yönetişimi politikalarının nasıl geliştirileceğine ilişkin sistematik bir model bulunmamaktadır.
3. Üniversiteye özgü veri yapısının dikkate alınmaması: Eğitim, araştırma ve idari veri vb. ayrımı çoğu modelde yer almamaktadır.
4. Federatif yönetim eksikliği: Üniversitelerdeki merkezi olmayan yapı yeterince modellenmemiştir.

5. Kltrel ve akademik boyutun ihmal edilmesi: Veri okuryazarlıęı, akademik zgrlk ve veri etięi gibi unsurlar sınırlı ele alınmaktadır.

Bu durumlarla birlikte YK’te niversitelere zg bir veri ynetiřimi modeli ihtiyacının farkındadır (YK, 2025). Bu bořluklar, niversitelere zg, ok boyutlu ve btnleřmiř bir veri ynetiřimi modelinin geliřtirilmesini gerekli kılmaktadır.

ÜNİVERSİTELER İÇİN KATMANLI VERİ YÖNETİŞİMİ MODELİ

5 AŞAMALI OLGUNLUK SEVİYELERİ (DAMA, 2017)



Şekil 21. Üniversiteler için katmanlı veri yönetiřimi modeli

Bu gereklilik doğrultusunda Şekil 21’de önerilen modelin amacı, Türkiye’deki üniversitelerde veriyi kurumsal bir varlık olarak konumlandırmak ve uygulanabilir bir veri yönetişimi modeli tasarlamaktır. Model aşağıdaki temel ilkelere dayanmaktadır:

1. **Verinin Kurumsal Varlık Olarak Kabul Edilmesi:** Bu ilke doğrultusunda veri sahipliği tanımlanmakta, veri yaşam döngüsü yönetilmekte, veri kalitesi ölçülmekte, veri yönetişimi kurumsal stratejiyle ilişkilendirilmektedir (DAMA, 2017; Fisher, 2009; ISO, 2017; ISO, 2023a; Khatri ve Brown, 2010; Otto, 2011; World Bank, 2020). Bu ilke doğrultusunda modeldeki stratejik katman ve süreç katmanı oluşturulmuştur.
2. **Stratejik Uyum İlkesi:** Model, veri yönetişiminin üniversitenin misyon, vizyon ve stratejik hedefleriyle uyumlu olması gerektiği ilkesine dayanmaktadır. Bu kapsamda model veri stratejisini kurumsal stratejiye bağlamakta, performans ve KPI temelli yönetimi desteklemekte, karar alma süreçlerini veri odaklı hale getirmektedir (ISO, 2017). Bu ilke sayesinde stratejik, teknik, süreç ve kültür katmanı geliştirilmiştir.
3. **Hesap Verebilirlik ve Rol Açıklığı İlkesi:** Modelde yönetim katmanı karar hakları, roller ve sorumlulukların açık biçimde tanımlanmasına dayanmaktadır (DAMA, 2017; ISO, 2017; Otto, 2011; Weber vd., 2009). Bu ilke kapsamında senato, veri yönetim kurulu, veri ofisi, veri sahipleri, veri sorumluları, veri domain liderleri gibi roller tanımlanmış ve aralarındaki ilişki mekanizmaları kurulmuştur. Bu yapı sayesinde hesap verebilirlik, denetlenebilirlik, yönetsel şeffaflık, veri sahipliği kurumsallaştırılmaktadır. Bu ilke stratejik ve yönetim katmanları ile doğrudan ilişkilidir.
4. **Veri Yaşam Döngüsü Yönetimi İlkesi:** Modelde veri yaşam döngüsü veri üretimi, veri işleme, veri depolama, veri analizi, veri kullanımı, veri paylaşımı ile yayınlama, arşivleme veya imha aşamalarından oluşmaktadır (DAMA, 2017; ISO, 2017). Bu ilke sayesinde süreç katmanı geliştirilmiştir.
5. **Veri Kalitesi ve Standartlaşma İlkesi:** Bu ilkeye göre ortak veri sözlüğü, üst veri yönetimi, veri modelleme, kalite kriterleri, entegrasyon standartları, referans

veri yönetimi kurumsal veri ekosisteminin temel bileşenleridir (DAMA, 2017; ISO, 2017; ISO, 2023a; ISO, 2023b). Bu ilke teknik katmanla doğrudan ilişki içindedir.

6. **Güvenlik, Gizlilik ve Etik Kullanım İlkesi:** Modelin temel taşı olan yasal ve etik katman KVKK, GDPR, ISO 27001, ISO 27701, UNESCO AI Etik, Açık Bilim ilkeleri ile ilişkilidir. Bu ilke kapsamında kişisel veri koruma, etik veri kullanımı, yapay zeka etiği, açıklanabilirlik, hesap verebilirlik, siber güvenlik ön plana çıkarılmıştır (ISO, 2017).
7. **Veri Odaklı Kurumsal Kültür İlkesi:** Kültür katmanını geliştiren bu ilke veri okuryazarlığı, farkındalık, eğitim, veri paylaşım kültürü, etik farkındalık, iş birliği kurumsal dönüşümün temel unsurları olarak ele alınmaktadır (ISO, 2017; Klievink vd., 2017; Koltay, 2016; Kremser ve Brunauer, 2019).
8. **Sürekli İyileştirme ve Olgunluk Yaklaşımı:** Model olgunlaşan ve gelişen bir yapı olarak tasarlanmıştır. Bu yaklaşım ISO yönetim sistemi mantığı ve veri yönetişimi olgunluk modelleriyle ilişkilidir. Bu nedenle modelde KPI ölçümü, EDM modeli performans izleme, geri bildirim, politika güncelleme, denetim, olgunluk seviyeleri yer almaktadır (ISO, 2018; Verdi vd., 2024).
9. **Katmanlı Yönetim İlkesi:** Veri yönetişimi, yükseköğretim kurumunun yapısına uygun yapılmalıdır. Türkiye'deki üniversitelerin mevcut durumu tek seferde tam kurulum yerine aşamalı geçiş gerektirmektedir. Modelin en özgün yönlerinden biri, veri yönetişimini birbirinden bağımsız olarak tasarlamak yerine katmanlar arası ilişkiler üzerinden ele almasıdır. Bu nedenle model stratejik, yönetsel, süreç, teknik, kültürel, yasal/etik katmanların birbirini beslediği bütünlük bir zincir mimarisi üzerine kurulmuştur. Önerilen model, herkese uyan tek bir çözüm yaklaşımı mantığında geliştirilmemiştir (Brous vd., 2016b).

Önerilen model, üniversitelerde veri yönetişimi yapısı ile veri yönetişimi politikalarının geliştirilme sürecini bütünlük bir çerçevede ele almak amacıyla tasarlanmıştır. Model, stratejik, yönetim, süreç, kültür ve teknoloji katmanlarından oluşan çok katmanlı bir

yapı üzerine kurulmuştur. Literatürde benzer şekilde kurumsal, organizasyonel ve teknik düzeyde yapılandırılan veri yönetişimi çerçeveleri bulunmaktadır (Wu, 2023).

Stratejik katman, üniversitenin misyonu, vizyonu, hedefleri ile uyumlu veri stratejisi, politika ve standartların belirlenmesini kapsarken yönetim katmanı veri sahipliği, karar hakları ve federatif yönetim yapısını içermektedir. Süreç katmanı, veri erişim, paylaşım, kalite ve yaşam döngüsü süreçlerini tanımlarken, kültür katmanı veri okuryazarlığı, açık bilim, veri etiği ve akademik özgürlük gibi unsurları içermektedir. Teknik katman ise veri altyapısı, sistemler, entegrasyon ve güvenlik bileşenlerinden oluşmaktadır. Her katman birbirlerine bağlı ve ilişki içindedir.

Önerilen model, katmanlı veri yönetişimi yapısını olgunluk seviyeleri ile entegre ederek literatürde yer alan mevcut yaklaşımları bütünleştirmektedir. DAMA (2017) tarafından önerilen olgunluk modeli, veri yönetişimi bileşenlerinin gelişim düzeylerini değerlendirmeye olanak tanırken, bu çalışma kapsamında geliştirilen katmanlı yapı söz konusu bileşenlerin organizasyonel konumlandırmasını sağlamaktadır. Bu entegrasyon, modelin hem değerlendirme hem de uygulama aracı olarak kullanılabilmesine imkan tanımaktadır.

5.2. MODELİN KATMANLARI

Modelde yer alan stratejik, yönetim, süreç, teknik, kültür, yasal ve etik katman ile bu katmanlar kapsamında yer alan unsurlar bu bölümde ayrıntılı olarak ele alınmaktadır.

5.2.1. Stratejik Katman

Stratejik katman, veri yönetişimi modelinin en üst düzeyini oluşturan ve tüm diğer katmanlara yön veren temel bileşendir (ISO, 2017). Bu katman, verinin kurumsal bir varlık olarak konumlandırıldığı, veri ile ilgili karar haklarının tanımlandığı ve veri kullanımının kurumsal hedeflerle hizalandığı yönetsel çerçeveyi ifade etmektedir (ISO, 2017; OECD, 2020; OECD, 2022). Stratejik katman altında yer alan veri stratejisinin oluşturulmasından başlayarak politika geliştirme, standart belirleme, risk ve uyum yönetimi, karar alma, değer üretimi ve performans izleme aşamalarını bütünsel bir yapı içerisinde sunmaktadır (ISO, 2018; ISO, 2023a).

Şekil 22’de stratejik katmanın iş akışında gösterildiği üzere başlangıç noktası kurumsal yön belirleme aşamasıdır. Bu aşamada üniversitenin misyonu, vizyonu, stratejik hedefleri ve kurumsal öncelikleri belirlenmektedir. Başka bir deyişle veri yönetişiminin hangi kurumsal önceliklere hizmet edeceği ortaya konmaktadır (ISO, 2025a). Veri stratejisi, kurumsal hedeflerle uyumlu olarak planlanmalı ve bu doğrultuda önceliklendirilmelidir (Bhansali, 2014; DAMA, 2017; Karkošková 2023; Ladley, 2020). Veri yönetişimini kamu ve kurumsal değer üretiminin temel aracı olarak değerlendiren yaklaşımı ile örtüşmektedir (OECD, 2020). Aynı zamanda Weber vd. (2009)’un veri yönetiminin stratejik iş hedefleri ile hizalanması gerektiğini savunan yaklaşımıyla da uyumludur.



Şekil 22. Stratejik katman iş akışı

Üniversitelerde veri yönetişimi yapılandırması için üniversitenin akademik ve idari hedefleri birbirleri ile uyumlu olmalıdır (Jim ve Chang, 2018). Mevcut veri problemleri, stratejik veri gereksinimleri değerlendirilmeli ve üniversite neye ihtiyaç duyuyorsa veri stratejisi bu yönde oluşturulmalıdır. Üniversitenin veri çıktılarıyla ulaşmak istediği stratejik sonuçlar tanımlanmalıdır. Örneğin öğrenci başarısı, araştırma performansı, idari verimlilik, açık bilim kapasitesi gibi alanlar önceliklendirilmelidir. Önceliklerin tespit edilmesi için veri kaynakları, veri kalitesi, sistemler arası entegrasyon, veri sahipliği durumu, yasal riskler ve yönetim boşlukları analiz edilmelidir. Aynı zamanda veri envanterini çıkarma, sorunlu alanları belirleme, riskleri ve eksiklikleri analiz etme, mevcut olgunluk seviyesi değerlendirilmelidir. Belirlenen kurumsal öncelikler doğrultusunda veri stratejisi hazırlanmalıdır. Bu strateji, verinin nasıl yönetileceği, hangi alanlarda değer üretilmesi ve hangi yönetim mekanizmalarının kurulacağına dair yol haritasını içermelidir (DAMA, 2017; ISO, 2017).

Khatri ve Brown (2010), veri yönetişiminin temelini karar haklarının dağılımına dayandırmıştır. Karar hakları dağılımı veri ile ilgili kimlerin karar alacağı, kimlerin uygulamadan sorumlu olacağı ve kimlerin teknik koruma işlevi göreceğinin belirlenmesidir (Khatri ve Brown 2010). Bu doğrultuda modelde karar haklarını dağıtmak, veri sahipliği yapısını belirlemek, rol çatışmalarını önlemek, hesap verebilirliği kurmak amacıyla veri sahipleri (data owners), veri sorumluları (data stewards), veri yönetişimi kurulu gibi rolleri stratejik katman tarafından açık biçimde tanımlanmalıdır

RACI¹⁴¹ çerçevesi, veri yönetişimi süreçlerinde rol ve sorumlulukların açık biçimde tanımlanmasını sağlayan önemli bir yönetim aracıdır. Belirli bir süreç veya faaliyet kapsamında kimin sorumlu, kimin hesap verebilir, kimlere danışılması gerektiği ve kimlerin süreç hakkında bilgilendirileceği konularını sistematik biçimde belirlemeye yardımcı olmaktadır. Böylece veri yönetişimi süreçlerinde görev çakışmalarının önüne geçilmekte, karar alma mekanizmaları netleştirilmekte ve kurumsal koordinasyon güçlendirilmektedir (Eryurek vd., 2021, s. 104). Üniversitelerde roller sorumlulukların

¹⁴¹ 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)

tanımlanması farklı fakülteler, enstitüler ve idari birimler tarafından veri üretildiği ve kullanıldığı için önemlidir.

Veri yönetişimi uygulanabilir politikalar ve standartlar geliştirildiğinde sürdürülebilirliği sağlanmaktadır (Dismute, 2009; Weber vd., 2009). Politika kapsamı belirleme, öncelikli politika alanları tanımlama, farklı veri türleri için gerekli yönetim başlıkları netleştirilmelidir. Bu kapsamda veri erişimi, veri paylaşımı, veri güvenliği, veri kalitesi, üst veri, veri sınıflanması, veri ihlali, saklama-imha gibi konularda politikalar, prosedürler veya standartlar tanımlanmalıdır. Veri Ofisi, Veri Sahipleri, Veri Sorumluları, Hukuk Müsteşarlığı, Bilgi İşlem Daire Başkanlığı, Kalite Koordinatörlüğü öncülüğünde politika metinlerini hazırlamak, standart veri tanımlarını oluşturmak, veri kalite kriterleri belirlenmelidir.

Veri yönetişiminin stratejik boyutunda, veri ile ilgili risklerin yönetimi ve yasal uyumun sağlanması kritik bir rol oynamaktadır. Özellikle kişisel verilerin korunması (KVKK), araştırma verisi etik ilkeleri ve uluslararası veri paylaşım standartları bu kapsamda değerlendirilmelidir. Otto (2011), veri yönetişiminin temel amaçlarından birinin veri ile ilgili riskleri minimize etmek olduğunu belirtmektedir. Bu bağlamda stratejik katman veri güvenliği riskleri, gizlilik ihlalleri, yasal uyumsuzluklar gibi unsurların yönetilmesini sağlamaktadır.

Verinin ekonomik niteliğinin sabit olmadığı, veri yaşam döngüsü boyunca değişmektedir. Ham veri başlangıçta kamusal ya da ortak mal niteliği taşıırken, işlenmiş veri ve veri tabanları özel mülkiyet kapsamında değerlendirilebilmektedir. Üniversiteler açısından veri yönetişiminin veri koruma veya mahremiyet meselesi olmadığı, veriye değer kazandırılması gerekmektedir (Savona, 2026). Bu nedenle veriden değer üretmeyi merkeze alan bir yaklaşım benimsemektedir.

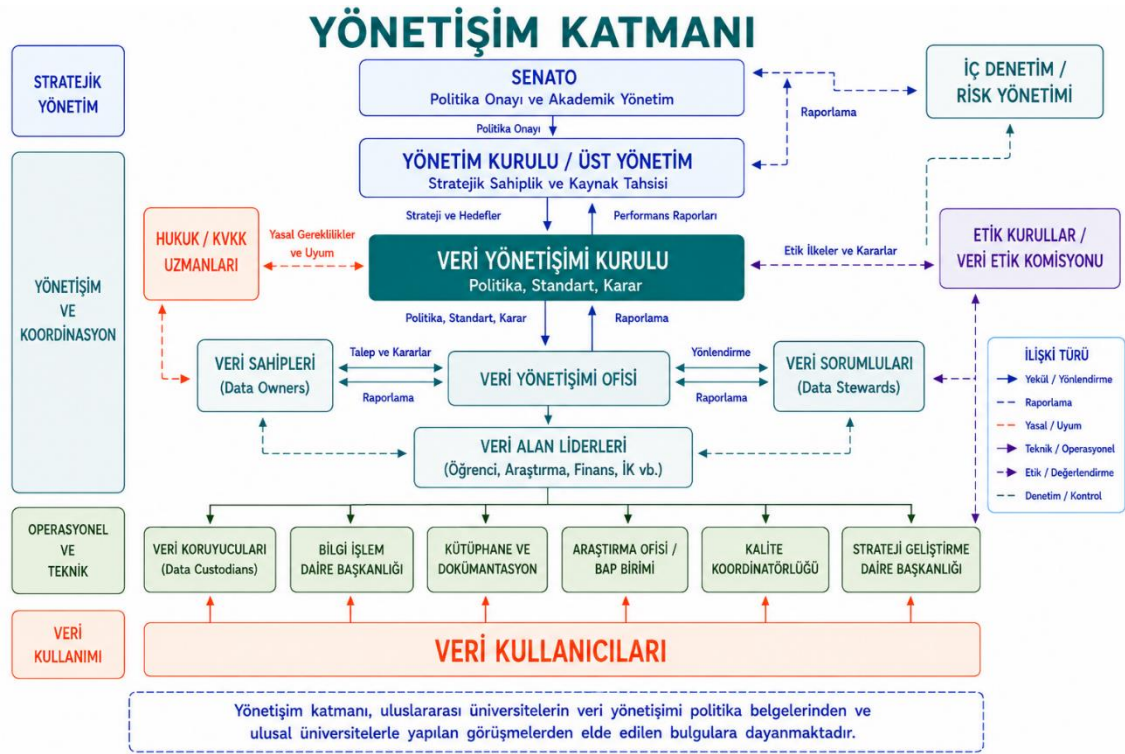
İzleme ve geri besleme, sürdürülebilirliği sağlamak için birçok veri yönetişimi modelinde (Abraham vd., 2019; Al-Badi vd., 2018; Hanisch vd., 2023; Jang ve Kim, 2021; Khatrı ve Brown, 2010 Wende ve Otto, 2007) yer almaktadır. Bu aşamada ISO/IEC 38505-2'de yer alan kademeli aktarım mekanizması ile veri stratejinin operasyonel süreçlere aktarılması kontrol edilir ve strateji, politika, süreç, kontrolü sayesinde üniversite genelinde stratejinin güncellenmesi öngörülmektedir (ISO, 2018).

Stratejik katman, ulusal görüşmelerde veri yönetiřimi birimlerinin doęrudan rektörlüęe veya ilgili rektör yardımcılıęına baęlı olarak yapılandırılması, üst yönetime düzenli raporlama yapılması ve veri yönetimi faaliyetlerinin aęırlıklı olarak raporlama ile karar destek işlevleri etrafında yürütölmesi bulgularına dayanmaktadır. Uluslararası politika belgelerinde de üst yönetimin politika onayı, kaynak tahsisi ve yönetsel gözetim rolünün vurgulanması, stratejik katmanın modeldeki yerini desteklemektedir. Görüşme ve politika bulgularının stratejik katmanla ilişkisi Ek 7 ve Ek 8’de ayrıntılı olarak sunulmuştur.

5.2.2. Yönetişim Katmanı

Yönetişim katmanı, veri yönetiřimi süreçlerinin kurumsal yapı içerisinde nasıl organize edildiğini belirleyen ve karar alma yetkileri ile sorumlulukların dağıtımını düzenleyen temel bileşendir. Bu katman, veri ile ilgili kararların kim tarafından, hangi yetkiyle ve hangi sorumluluk çerçevesinde alınacağını belirleyerek veri yönetişiminin uygulamaya aktarılmasını sağlamaktadır.

Literatürde veri yönetişimi, organizasyonel veri varlıklarının yönetimi için karar haklarının, sorumlulukların ve rollerin tanımlanmasıdır (Alhassan vd., 2016; Brous vd., 2016b; Cheong ve Chang, 2007; DAMA, 2017; DGI, t.y.; El Abed ve Njonko, 2014; European Commission, 2020a; ISO, 2017; Jang ve Kim, 2021; Khatri ve Brown, 2010; Smith, 2025; Wende ve Otto, 2007; World Bank, 2020). Veri yönetişimi süreçlerinin etkin yürütöllebilmesi için veri yönetişimi kurulu, veri ofisi, veri sorumluları ve veri koruyucuları arasında koordinasyon gerekmektedir (Korhonen vd., 2013).



Şekil 23. Yönetişim katmanı iş akışı

Khatri ve Brown'a (2010) göre veri yönetişimi, hangi kararların alınacağı ve bu kararları kimin alacağı sorularına odaklanmalıdır. Şekilde 23'te sunulan üniversite veri yönetişimi yapısı, stratejik yönetim, yönetim koordinasyonu, operasyonel ve teknik yönetim ile veri kullanımı boyutlarını bütünsel biçimde ele alan çok katmanlı bir organizasyon modeli ortaya koymaktadır (Bkz. Şekil 20). Modelde yer alan yapılar veri ile ilgili karar alma, koordinasyon, uygulama, denetim ve geri besleme mekanizmalarının nasıl işlediğini göstermektedir. Veri yönetişiminin kurumsal strateji, süreç yönetimi, teknik altyapı ve veri kullanımı arasında koordinasyon gerektiren disiplinler arası bir alan olduğunu ortaya koymaktadır.

Modelin en üst düzeyinde yer alan Senato ve üst yönetim, veri yönetişiminin stratejik sahipliğini temsil etmektedir. Senato, veri yönetişimi politikalarının oluşumunu sağlayan en üst karar organı olarak konumlandırılmıştır. Üst yönetim ise veri stratejisinin kurumsal hedeflerle uyumlu hale getirilmesi, kaynak tahsis ve yönetim mekanizmalarının desteklenmesinden sorumludur. Literatürde DAMA (2017), DCAM (EDM Association, 2025), ve OECD (2020, 200) veri yönetişimi yaklaşımları, üst yönetim desteğini veri yönetişiminin temel başarı faktörlerinden biri olarak değerlendirmektedir (ISO, 2017).

Stratejik yönetim ile operasyonel veri yönetimi arasındaki koordinasyonu sağlayan temel yapı ise Veri Yönetişimi Kuruludur (Jim ve Chang, 2018). Bu kurul, veri politikalarının geliştirilmesi, veri standartlarının belirlenmesi, veri kalite kriterlerinin tanımlanması ve veri paylaşım kararlarının yönetilmesi gibi görevleri yürütmektedir. Aynı zamanda veri ile ilgili çatışmaların çözülmesi ve veri yönetişimi önceliklerinin belirlenmesi süreçlerinde merkezi koordinasyon görevi üstlenmektedir. Veri yönetişimi kurulunun hem üst yönetime hem de operasyonel veri yönetimi birimlerine bağlı çalışması, modelde stratejik kararlar ile operasyonel süreçler arasında çift yönlü bir ilişki kurulduğunu göstermektedir.

Modelde veri sahipleri, belirli veri alanlarının stratejik sorumluluğunu üstlenen yönetsel roller olarak konumlandırılmıştır. Veri sahipleri, veri erişim ve paylaşım kararlarını vermektedir. Veri kalite hedeflerini ve veri kullanımına ilişkin onay mekanizmalarını yürütmektedir. Buna karşılık veri sorumluları, veri süreçlerinin günlük operasyonel yönetiminden sorumludur. Veri kalite kontrolü, metadata yönetimi, veri sözlüğü güncellemeleri ve veri standartlarının uygulanması veri sorumlularının temel görevleri arasında yer almaktadır. Veri sahipliği ile operasyonel veri yönetimi arasında açık bir görev ayrımı oluşturarak hesap verebilirlik mekanizmasını güçlendirmektedir.

Veri alan (domain) liderleri ise öğrenci, araştırma, finans ve insan kaynakları gibi alan bazlı veri süreçlerinin koordinasyonundan sorumlu yapı olarak konumlandırılmıştır. Bu rol, özellikle modern veri yönetişimi yaklaşımlarında öne çıkan alan bazlı veri yönetimi anlayışını desteklemektedir. Veri alan liderleri, veri ihtiyaçlarının belirlenmesi, süreç iyileştirme faaliyetlerinin yürütülmesi ve farklı veri alanları arasındaki koordinasyonun sağlanması görevlerini üstlenmektedir.

Operasyonel ve teknik katmanda yer alan veri koruyucuları ile Bilgi İşlem Daire Başkanlığı, veri yönetişiminin teknik altyapısını oluşturmaktadır. Bu yapı veri güvenliği, sistem yönetimi, veri entegrasyonu, erişim kontrolü ve yedekleme süreçlerini yürütmektedir. Böylece veri yönetişiminin teknik sürdürülebilirliği sağlanmaktadır. Teknik yapı ile veri yönetişimi kurulu arasındaki ilişki, veri politikalarının teknik altyapıya entegre edilmesini mümkün kılmaktadır.

Kütüphane ve Dokümantasyon Birimi ile Araştırma Ofisi/BAP birimi, modelde özellikle akademik veri yönetimi açısından kritik role sahiptir. Kütüphane birimi üst veri yönetimi, açık veri ve açık bilim süreçlerini desteklerken araştırma ofisi araştırma verilerinin yönetimi, proje verisi süreçleri ve araştırma uyum faaliyetlerini yürütmektedir. Üniversitelerde veri yönetişiminin araştırma ekosistemi ile bütünleşik çalıştığını göstermektedir.

Kalite Koordinatörlüğü ve Strateji Geliştirme Daire Başkanlığı ise performans yönetimi ve kurumsal izleme boyutunu temsil etmektedir. Kalite Koordinatörlüğü veri kalite standartlarını, KPI'ları ve sürekli iyileştirme faaliyetlerini yürütürken, Strateji Geliştirme daire Başkanlığı performans raporlama ve stratejik veri analizlerini gerçekleştirmektedir. Bu ilişki, veri yönetişiminin performans ve kalite yönetimi sistemi ile bütünleşik olduğunu göstermektedir.

Modelde Hukuk Müşavirliği/KVKK uzmanları ile etik kurullar da önemli bir bileşen olarak konumlandırılmıştır. Hukuk Müşavirliği ve KVKK uzmanları yasal uyum, veri paylaşım protokolleri ve sözleşme süreçlerini yürütürken etik kurullar araştırma verileri, kişisel veri kullanımı ve yapay zeka uygulamalarına ilişkin etik değerlendirme süreçlerini yönetmektedir. Böylece veri yönetişimi modeli etik ve hukuki boyutları da kapsamalıdır.

Modelin en altında yer alan veri kullanıcıları ise yönetim yapısının nihai kullanım boyutunu temsil etmektedir. Akademisyenler, idari personeller, yöneticiler, araştırmacılar, analistler ve öğrenciler veriyi karar alma, analiz ve akademik üretim süreçlerinde kullanmaktadır. Veri kullanıcıları aynı zamanda veri kalite sorunlarının bildirilmesi ve veri kullanım politikalarına uyum sağlanması süreçlerinde aktif rol almaktadır. Veri yönetişiminin kullanıcı katılımına dayalı sürdürülebilir bir sistem olduğunu göstermektedir.

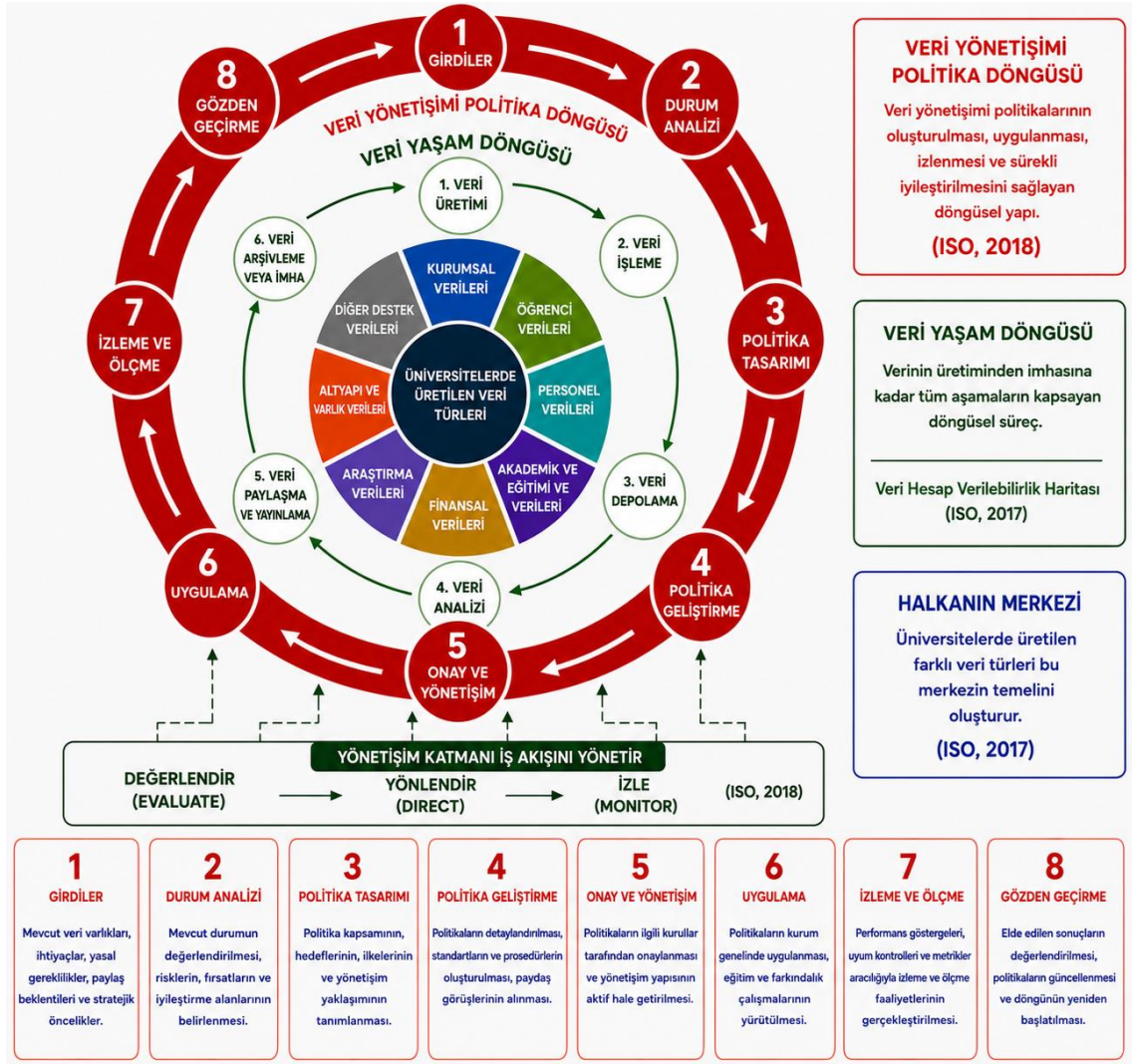
Böylece yönetim katmanı, veri yönetişimi modelinde karar alma, sorumluluk dağılımı ve hesap verebilirlik mekanizmalarının bütünleşik bir şekilde yönetilmesini sağlayan temel bileşen olarak konumlandırılmaktadır (Khatri ve Brown, 2010).

Yönetişim katmanı, üniversitelerde veri yönetişimi birimlerinin koordinatörlük, ofis, merkez ve farklı birim biçimlerinde yapılandırılması, rol ve sorumlulukların her kurumda

aynı açıklıkta tanımlanmamış olması ve akademik, idari ve teknik birimler arasında koordinasyon ihtiyacının bulunması bulgularıyla ilişkilidir. Bu durum, modelde Veri Yönetişimi Kurulu, Veri Yönetişimi Ofisi, veri sahipleri, veri sorumluları, teknik veri sorumluları, veri alan liderleri ve veri kullanıcılarından oluşan federatif bir rol yapısının oluşturulmasına temel sağlamıştır. Uluslararası politika belgelerinde görülen rol temelli yönetim, veri sahibi onayı ve çok paydaşlı koordinasyon uygulamaları da bu yapıyı desteklemektedir. İlgili eşleştirmeler Ek 7 ve Ek 8’de gösterilmiştir.

5.2.3. Süreç Katmanı

Süreç katmanı, üniversitelerde üretilen verilerin yaşam döngüsü boyunca nasıl yönetileceğini ve veri yönetişimi politikalarının operasyonel düzeyde nasıl uygulanacağını tanımlayan temel yapıyı oluşturmaktadır. Bu katman, veriyle ilgili tüm faaliyetlerin standartlaştırılmış, tekrarlanabilir, ölçülebilir ve sürdürülebilir süreçler aracılığıyla yürütülmesini sağlamaktadır (ISO, 2017). Süreç katmanı veri yönetişimi politikalarının uygulamaya dönüştürüldüğü, veri yaşam döngüsünün işletildiği ve veriyle ilişkili yönetsel faaliyetlerin kurumsal iş süreçlerine entegre edildiği operasyonel yönetim alanını temsil etmektedir. Model kapsamında süreç katmanı, yönetim mekanizmaları ile teknik altyapı arasında köprü görevi görmektedir.



Şekil 24. Süreç katman iş akışı

Şekil 24'te gösterilen süreç katmanı, birbiriyle ilişkili üç temel yapıdan oluşmaktadır. Bunlar üniversitelerde üretilen veri alanlarını temsil eden merkez yapı, veri yaşam döngüsünü temsil eden iç halka ve veri yönetimi politika döngüsünü temsil eden dış halkadır. Modelin merkezinde yer alan kurumsal veriler, öğrenci verileri, personel verileri, akademik ve eğitim verileri, finansal veriler, araştırma verileri, altyapı ve varlık verileri ile diğer destek verileri gibi üniversitelerde farklı kaynaklardan üretilen veri alanlarını göstermektedir. Üniversitelerde veri kaynaklarının çeşitliliği ve farklı sistemler arasında dağınık biçimde bulunması, veri yönetimi süreçlerini zorunlu hale getirmektedir (Aisyah ve Ruldeviyani, 2018; DAMA, 2017).

Merkezi çevreleyen yeşil halka, veri yaşam döngüsünü temsil etmektedir. Veri yaşam döngüsü, verinin üretilmesinden arşivlenmesine veya imha edilmesine kadar geçen tüm süreçleri kapsamaktadır (DAMA, 2017; ISO, 2017; ISO, 2017). Şekilde bu süreçler veri üretimi, veri işleme, veri depolama, veri analizi, veri paylaşımı ve yayınlama ile veri arşivleme veya imha aşamalarından oluşmaktadır. Döngüsel yapının tercih edilmesi, veri yönetiminin süreklilik esasına dayalı olduğunu ve her aşamanın bir sonraki aşama ile doğrudan ilişkili olduğunu göstermektedir. Aynı zamanda veri yaşam döngüsünün kesintisiz devam eden bir süreç olduğu ve verinin her aşamada yeniden değer üretebildiği vurgulanmaktadır.

Veri yaşam döngüsünün ilk aşaması olan veri üretimi öğrenci bilgi sistemleri, öğrenme yönetim sistemleri, araştırma projeleri, insan kaynakları süreçleri, finansal işlemler ve yönetsel faaliyetler sonucunda oluşan verileri kapsamaktadır. Üniversitelerde verinin çok sayıda kaynaktan üretilmesi, ortak veri tanımlarının, üst veri standartlarının ve veri kalite kriterlerinin oluşturulmasını zorunlu hale getirmektedir (ISO, 2022). Bir sonraki aşama olan veri işleme süreci ise üretilen verilerin temizlenmesi, doğrulanması, dönüştürülmesi ve kullanılabilir hale getirilmesini kapsamaktadır. Bu aşamada veri kalite kontrolleri, veri doğrulama mekanizmaları ve standartlaştırma faaliyetleri yürütülmektedir (ISO, 2023b). Literatürde veri yönetişiminin temel amaçlarından biri yüksek kaliteli veri üretmek olarak değerlendirildiğinden, veri işleme süreci veri doğruluğu ve veri bütünlüğü açısından kritik bir aşama olarak kabul edilmektedir (Askham, 2014; Li vd., 2026).

Veri depolama sürecinde veriler veri tabanları, veri ambarları veya kurumsal depolama sistemleri içerisinde saklanmaktadır (Eryurek vd., 2021, s. 88). Bu sebeple veri depolama süreci, veri güvenliği, erişim kontrolü ve veri bütünlüğü açısından teknik katman ile doğrudan ilişkilidir. Bu bağlamda süreç katmanı veri akışlarını tanımlarken teknik katman bu süreçlerin çalışmasını sağlayan altyapıyı desteklemektedir.

Üniversitelerde veri temelli karar alma mekanizmalarının temelini veri analizi oluşturmaktadır (Eryurek vd., 2021, s. 88). Bu süreçte analitik yöntemler, iş zekası uygulamaları, performans analizleri ve raporlama faaliyetleri yürütülmektedir. Akademik performans ölçümü, öğrenci başarıları analizi, araştırma çıktılarının değerlendirilmesi ve stratejik planlama süreçleri veri analizi aşamasının temel kullanım alanlarıdır.

Veri paylaşımı ve yayınlama, verinin kurum içi veya kurum dışı paydaşlarla kontrollü biçimde paylaşılmasını kapsamaktadır (Eryurek vd., 2021, s. 88). Veri paylaşımı süreçlerinde erişim yetkileri, veri gizliliği ve etik kullanım ilkeleri kritik önem taşımaktadır. Bu nedenle süreç katmanı, yönetim ve yasal/etik katmanlarla doğrudan ilişkili kurgulanmıştır.

Son aşama olan veri arşivleme veya imha, verinin yaşam döngüsünün tamamlandığı aşamayı temsil etmektedir. Bu süreçte verilerin saklama politikalarına uygun biçimde arşivlenmesi veya yasal düzenlemeler doğrultusunda güvenli şekilde imha edilmesi sağlanmaktadır (Eryurek vd., 2021, s. 89).

Şekilde kırmızı renk ile gösterilen dış halka ise veri yönetişimi politika döngüsünü temsil etmektedir. Politika döngüsü, veri yaşam döngüsünün hangi ilke, standart ve yönetim mekanizmaları doğrultusunda işletileceğini belirlemektedir (Eryurek vd., 2021, s. 101; ISO, 2023a).

Politika döngüsünün ilk aşaması olan girdiler bölümünde kurumsal ihtiyaçlar, stratejik hedefler, yasal gereklilikler ve paydaş beklentileri belirlenmektedir. Durum analizi aşamasında mevcut veri yönetimi yapısı, riskler ve iyileştirme alanları değerlendirilmektedir (Eryurek vd., 2021). Politika tasarımı ve politika geliştirme aşamalarında veri yönetimine ilişkin kurumsal politika, standart ve süreçler oluşturulmaktadır (Korhonen vd., 2013). Onay ve yönetim aşamasında ise geliştirilen politikalar senato, veri yönetişimi kurulu veya üst yönetim tarafından onaylanarak kurumsal yönetim yapısına entegre edilmektedir.

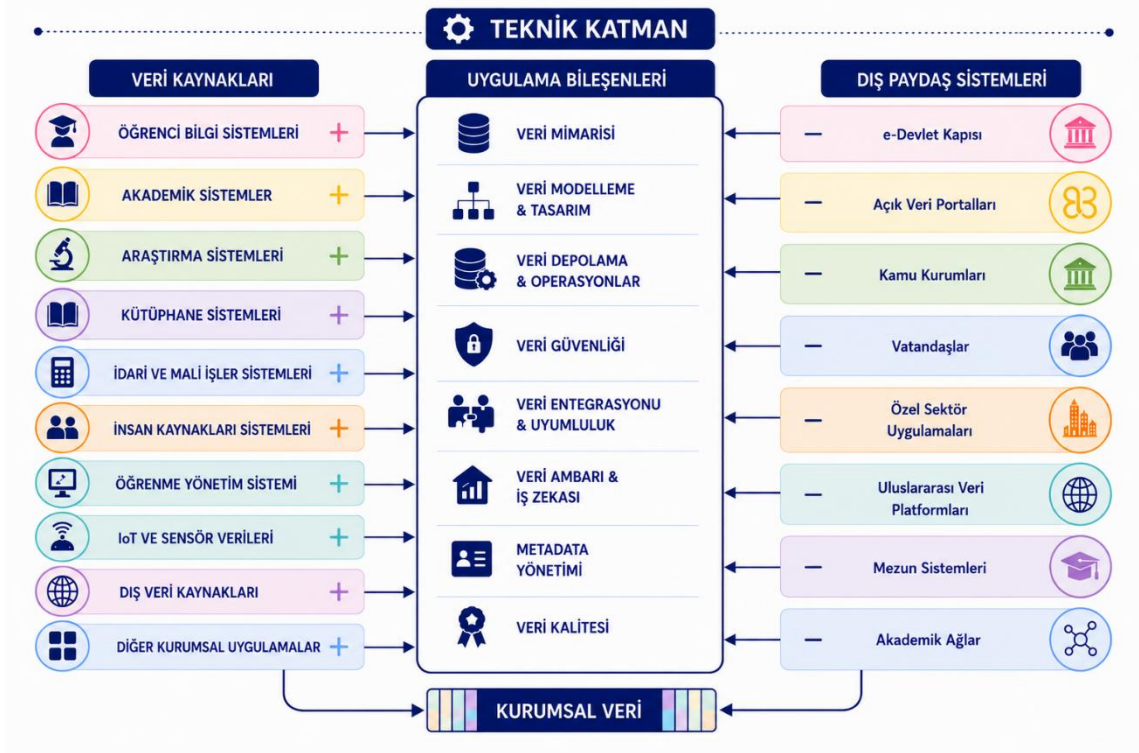
Uygulama aşamasında veri yönetişimi politikaları kurum genelinde yürürlüğe alınmaktadır. Veri erişim süreçleri, veri kalite uygulamaları ve farkındalık çalışmaları gerçekleştirilmektedir. İzleme ve ölçme aşamasında KPI'lar, veri kalite göstergeleri ve uyum kontrolleri aracılığıyla süreç performansı değerlendirilmektedir. Son aşama olan gözden geçirme süreci ise elde edilen sonuçların yeniden değerlendirilmesini, politika ve standartların güncellenmesini ve veri yönetişimi yapısının sürekli iyileştirilmesini sağlamaktadır (Eryurek vd., 2021; ISO, 2023a). Böylece politika döngüsü sürekli geri besleme ile çalışan bir sistem haline gelmektedir.

Şeklin alt bölümünde yer alan EDM modeli ise ISO/IEC 38505-2:2018 standardından uyarlanmaktadır. Buna göre süreç katmanını stratejik katmandan gelen hedefler doğrultusunda çalışmakta, yönetim katmanını tarafından kontrol edilmekte, teknik katman tarafından desteklenmekte, kültür katmanını tarafından benimsenmekte ve yasal/etik katman tarafından sınırları belirlenen bir yapı haline dönüşmektedir (ISO, 2018).

Süreç katmanını, görüşmelerde belirlenen veri envanteri oluşturma, veri girişi ve doğrulama sorumluluklarının ayrıştırılması, veri taleplerinin değerlendirilmesi, veri göstergelerinin onaylanması, kurum içi ve dışı veri paylaşımı ile arşivleme gereksinimleri temelinde geliştirilmiştir. Bulgular, üniversitelerde veriyle ilgili uygulamaların çoğu zaman standartlaşmış iş akışlarına dayanmadığını; erişim, paylaşım, doğrulama, saklama ve imha süreçlerinin açık biçimde tanımlanmasına ihtiyaç duyulduğunu göstermektedir. Uluslararası politika belgelerinde verinin oluşturulmasından imhasına kadar yaşam döngüsü boyunca yönetilmesine yönelik hükümler de süreç katmanını desteklemektedir. Bu ilişkiler Ek 7 ve Ek 8’de ayrıntılandırılmıştır.

5.2.4. Teknik Katman

Bu çalışma kapsamında geliştirilen veri yönetimi modelinde teknik katman, üniversitelerde üretilen verilerin güvenli, entegre, sürdürülebilir ve değer üretecek biçimde yönetilmesini sağlayan teknolojik altyapıyı temsil etmektedir (DAMA, 2017; EDM Association, 2025; ISO, 2017; PwC, 2019; Wu, 2023). Bu katman verinin farklı kaynaklardan toplanması, işlenmesi, depolanması, entegrasyonu, analiz edilmesi ve paylaşılması süreçlerinde kullanılan teknik mimariyi kapsamaktadır. Bu katman Bilgi İşlem Daire Başkanlığı altyapısında ve veri yaşam döngüsünün sürdürülebilirliğini sağlayan kurumsal veri ekosistemidir.



Şekil 25. Teknik katman iş akışı

Şekil 25'te gösterilen teknik katman, üniversitelerde dağınık halde bulunan veri kaynaklarının ortak bir kurumsal veri yapısı içerisinde bütünleştirilmesini sağlayan teknolojik çerçeveyi ortaya koymaktadır. Literatürde veri yönetişiminin sürdürülebilir biçimde uygulanabilmesi için güçlü bir teknik altyapının gerekli olduğu vurgulanmaktadır (DAMA, 2017; Eryurek vd., 2021). Özellikle yükseköğretim kurumlarında öğrenci bilgi sistemleri, akademik sistemler, araştırma yönetim sistemleri, insan kaynakları uygulamaları, öğrenme yönetim sistemleri ve finansal sistemler gibi çok sayıda veri kaynağının bulunması, teknik entegrasyon ihtiyacını artırmaktadır. Bu nedenle teknik katman, farklı veri kaynaklarını ortak veri standartları ve entegrasyon mekanizmaları çerçevesinde bir araya getiren merkezi bir yapı olarak tasarlanmıştır.

Şeklin sol bölümünde yer alan Veri Kaynakları, üniversitelerde veri üreten temel sistemleri göstermektedir. Öğrenci bilgi sistemleri, akademik sistemler, araştırma sistemleri, kütüphane sistemleri, idari ve mali işler sistemleri, insan kaynakları sistemleri, öğrenme yönetim sistemleri, IoT ve sensör verileri, dış veri kaynakları ve diğer kurumsal uygulamalar bu yapının temel bileşenlerini oluşturmaktadır. Üniversitelerde verinin farklı sistemlerde parçalı biçimde bulunması, veri silolarının oluşmasına neden olmaktadır. Bu

durum veri bütünlüğü, veri paylaşımı ve kurumsal analiz süreçlerini zorlaştırmaktadır. Teknik katman bu dağınık yapıyı veri politikalarıyla entegre edilmiş veri mimarisi altında birleştirmeyi amaçlamaktadır (ISO, 2022; ISO, 2025a; ISO, 2025b).

Şeklin merkezinde yer alan Uygulama Bileşenleri bölümü, teknik katmanın temel operasyonel yapılarını temsil etmektedir (DAMA, 2017). Veri mimarisi bileşeni, kurumsal verinin nasıl yapılandırılacağını, veri varlıklarının nasıl ilişkilendirileceğini ve veri akışlarının nasıl yönetileceğini belirlemektedir. Veri modelleme ve tasarım süreci ise ortak veri tanımlarının, veri ilişkilerinin ve üst veri yapılarının oluşturulmasını kapsamaktadır. Özellikle ISO/IEC 11179 üst veri standardı ile ilişkili olup kurum genelinde ortak veri dili oluşturulmasını desteklemektedir (ISO, 2023b).

Veri depolama ve operasyonlar bileşeni veri tabanları, veri ambarları, bulut sistemleri ve operasyonel depolama altyapılarının yönetimini kapsamaktadır. Üniversitelerde büyük hacimli verilerin güvenli biçimde saklanabilmesi için ölçeklenebilir ve sürdürülebilir depolama altyapılarının oluşturulması kritik önem taşımaktadır (Eryurek vd., 2021). Veri güvenliği bileşeni ise erişim kontrolü, kimlik doğrulama, loglama, veri gizliliği ve güvenlik politikalarının uygulanmasını kapsamaktadır. ISO/IEC 27001 ve ISO/IEC 27701 standartlarıyla doğrudan ilişkilidir (ISO, 2022; ISO, 2025b).

Teknik katmanın önemli bileşenlerinden biri olan veri entegrasyonu ve uyumluluk alanı, farklı sistemler arasında veri paylaşımının standartlaştırılmış biçimde gerçekleştirilmesini sağlamaktadır. Üniversitelerde farklı yazılım altyapılarının kullanılması veri bütünleşmesini zorlaştırdığından, entegrasyon süreçleri veri yönetişiminin temel gereksinimlerinden biri haline gelmektedir (ISO, 2025c).

Veri ambarı ve iş zekası bileşeni, kurumsal verilerin analiz edilmesini ve karar alma süreçlerinde kullanılabilir bilgiye dönüştürülmesini sağlamaktadır. Bu bölümde performans analizleri, raporlama süreçleri, gösterge panelleri ve analitik uygulamalar yer almaktadır. Üniversitelerde akademik performans ölçümü, öğrenci başarısı analizi, araştırma çıktılarının değerlendirilmesi ve stratejik planlama süreçleri bu yapının temel kullanım alanlarıdır.

Üst veri yönetimi bileşeni, verilerin tanımlanması, sınıflandırılması ve veri sözlüğü yapılarının oluşturulmasını kapsamaktadır. Üst veri yönetimi sayesinde kurum genelinde ortak veri anlamı oluşturulmakta, veri bütünlüğü korunmakta ve veri paylaşım süreçleri kolaylaştırılmaktadır. Veri kalitesi bileşeni ise veri doğruluğu, tutarlılığı, bütünlüğü ve güncelliğinin izlenmesini sağlamaktadır. Veri kalite yönetimi, ISO 8000-51:2023, ISO/IEC 5259-5:2025 ve ISO/IEC 25642:2025 standartlarıyla ilişkili biçimde değerlendirilmektedir.

Şeklin sağ bölümünde yer alan Dış Paydaş Sistemleri üniversitelerin dış veri ekosistemleriyle de etkileşim içerisinde olduğunu göstermektedir. E-Devlet Kapısı, açık veri portalları, kamu kurumları, vatandaşlar, özel sektör uygulamaları, uluslararası veri platformları, mezun sistemleri ve akademik ağlar bu yapının temel bileşenlerini oluşturmaktadır. Teknik katman, üniversitelerin dış paydaşlarla güvenli veri paylaşımı gerçekleştirebilmesini sağlayan birlikte çalışabilirlik altyapısını temsil etmektedir.

Şeklin alt bölümünde yer alan Kurumsal Veri alanı ise tüm veri kaynakları, uygulama bileşenleri ve dış sistemlerin ortak çıktısını temsil etmektedir. Teknik katmanın temel amacının kurumsal düzeyde bütünlük, güvenilir ve yönetilebilir veri üretmek olduğunu göstermektedir. Böylece teknik katman, stratejik katmanın veri odaklı karar alma süreçlerini, yönetim katmanının politika ve standartlarını, süreç katmanının operasyonel işleyişini, kültür katmanının veri kullanım alışkanlıklarını ve yasal-etik katmanın güvenlik ile uyum gereksinimlerini destekleyen teknolojik altyapıyı oluşturmaktadır.

Teknik katman veri mimarisi, veri modelleme, veri depolama, veri güvenliği, entegrasyon, veri ambarı, iş zekası, üst veri yönetimi ve veri kalite süreçleri aracılığıyla kurumsal veri ekosisteminin sürdürülebilirliğini desteklemektedir. Teknik katmanda teknolojik altyapı kurumsal hedefler doğrultusunda yönlendirilmesi stratejik katmanda alınan kararlara dayanmaktadır. (DAMA, 2017; ISO, 2017). Bununla birlikte teknik katman bağımsız çalışmamaktadır. Stratejik katman, yönetim katmanı, süreç katmanı ve kültür, yasal ve etik katmanlarla sürekli etkileşim içerisinde.

Şekil 25'te teknik katman ile yönetim katmanı arasındaki ilişki, rol ve sorumlulukların teknik süreçlere entegre edilmesi biçiminde gösterilmektedir. Veri yönetimi kurulu, veri ofisi, veri sahipleri ve veri sorumluları tarafından belirlenen politika, standart ve karar

mekanizmaları teknik altyapı aracılığıyla uygulanmaktadır. Örneğin veri erişim yetkileri, kimlik doğrulama süreçleri, veri paylaşım kuralları ve veri kalite kriterleri teknik sistemler içerisinde uygulanabilir hale getirilmektedir. Böylece teknik katman yönetim kararlarının operasyonel düzeye aktarılmasını sağlamaktadır (Wu, 2023).

Teknik katman veri yaşam döngüsü süreçlerinin teknik olarak desteklemektedir. Süreç katmanında tanımlanan veri üretimi, işleme, depolama, analiz, paylaşım ve arşivleme süreçleri teknik katman tarafından yürütülmektedir. Teknik katmanda yer alan veri depolama sistemleri, entegrasyon altyapıları, veri ambarı çözümleri ve analitik platformlar süreç katmanının operasyonel uygulanabilirliğini sağlamaktadır. Bu nedenle süreç katmanı veri yönetişiminin operasyonel akışını tanımlarken teknik katman bu süreçlerin çalışmasını sağlayan altyapıyı temsil etmektedir.

Üniversitelerde ISO/IEC 27001 ve 27701 standartları veri kaynakları bileşeninde yer alan sistemlerin birçok hassas veri alanının güvenliği bu standartlarla güçlendirilebilir. Yükseköğretim kurumları içinde risk temelli veri yönetimi¹⁴², veri güvenliği politikalarının kurumsallaşması¹⁴³, kişisel veri işleme süreçlerinin standardizasyonu¹⁴⁴, veri ihlallerine hızlı ve sistematik müdahale¹⁴⁵, dijital dönüşüm projelerinde güvenli bir temel oluşturulması gibi alanlara katkı sağlaması¹⁴⁶ beklenebilir (ISO, 2022; ISO, 2025b).

Teknik katmanın kültür, yasal ve etik katmanlarla ilişkisi ise veri güvenliği, etik kullanım ve uyum süreçleri üzerinden açıklanmaktadır. Teknik katman KVKK, bilgi güvenliği standartları, erişim kontrolleri, loglama mekanizmaları, veri gizliliği uygulamaları ve güvenlik politikaları aracılığıyla yasal ve etik gerekliliklerin teknik düzeyde uygulanmasını sağlamaktadır. Böylece veri etiği, veri gizliliği ve güvenlik ilkeleri teknik sistemlere gömülü kontrol mekanizmalarına dönüşmektedir. Özellikle erişim kontrolü, kimlik doğrulama, şifreleme ve güvenlik izleme süreçleri etik ve yasal yönetişimin teknik uygulama boyutunu oluşturmaktadır (ISO, 2022; OECD, 2020; OECD, 2022).

¹⁴² Veri varlıklarını sınıflandırılarak, her bir varlığa uygun koruma düzeyi belirlenmesi

¹⁴³ Erişim yönetimi, güvenlik politikaları, yetki matrisi, veri aktarım prosedürleri gibi süreçlerin netleşmesi

¹⁴⁴ Öğrenci, personel ve diğer rollerin verilerinin yasal gerekliliklere uygun işlenmesinin sağlanması

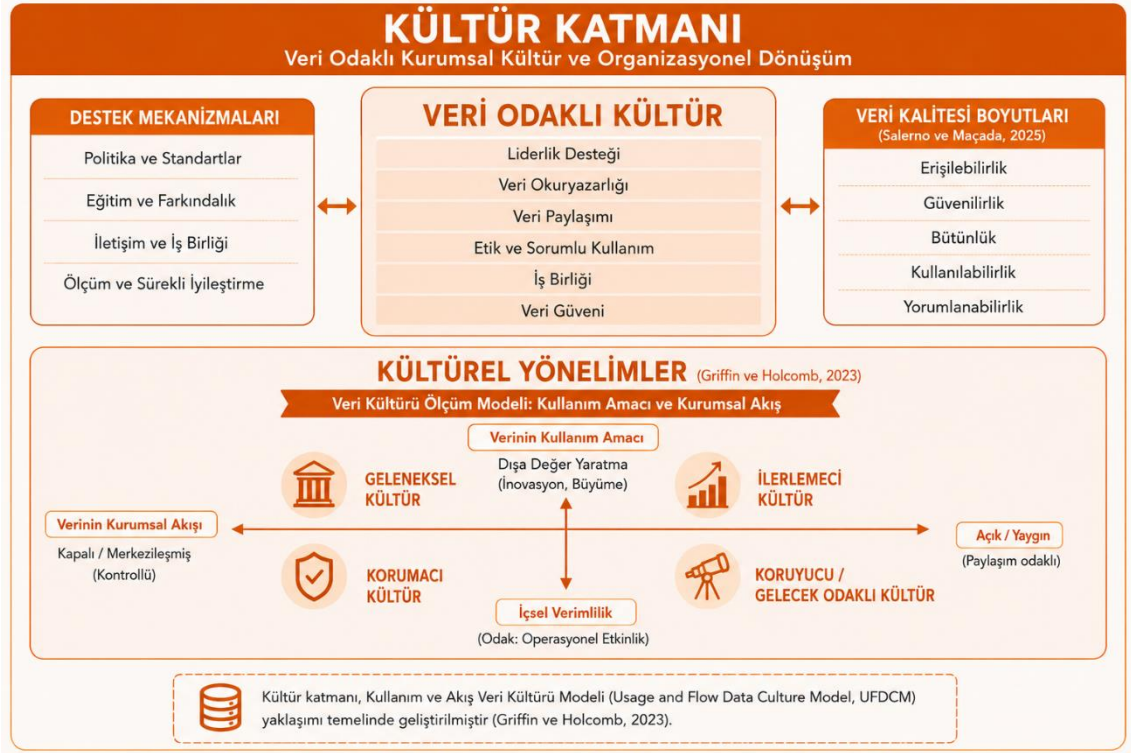
¹⁴⁵ Veri ihlali bildirim süreçlerinin düzenlenerek, hesap verebilirlik ve şeffaflığın artması

¹⁴⁶ Bulut ortamları, yapay zekâ uygulamaları ve veri analitiği platformlarının güvenlik gereksinimlerinin belirlenmesi

Teknik katman, görüşmelerde veri sözlüğü, veri kataloğu ve üst veri çalışmalarının henüz tamamlanmamış olması, farklı bilgi sistemleri arasındaki entegrasyon güçlükleri, veri ambarı, gösterge paneli, erişim yönetimi ve veri kalitesi araçlarına duyulan ihtiyaç gibi bulgulardan hareketle oluşturulmuştur. Bu bulgular, veri mimarisi, veri modelleme, üst veri yönetimi, veri entegrasyonu, veri kalitesi, veri ambarı ve iş zekâsı, erişim yönetimi ve bilgi güvenliği bileşenlerinin model içinde birlikte ele alınmasını gerekli kılmıştır. Uluslararası politika belgelerinde ortak veri tanımları, veri sınıflandırması, şifreleme, kimlik doğrulama, loglama, yedekleme ve kurtarma uygulamalarının vurgulanması da teknik katmanın kapsamını desteklemektedir. Ek 7 ve Ek 8, bu teknik bileşenlerin bulgusal dayanaklarını göstermektedir.

5.2.5. Kültür Katmanı

Kültür katmanı, üniversitelerde veri yönetişiminin sürdürülebilirliğini sağlayan insan merkezli organizasyonel dönüşüm alanını temsil etmektedir. Veri kültürü, kurumsal kültürün özel bir biçimini temsil etmektedir (Kremser ve Brunauer, 2019). Kültür katmanı verinin kurumsal karar alma süreçlerinde güvenilir, paylaşılabılır, etik ve sürdürülebilir biçimde kullanılmasını sağlayan davranışsal, yönetsel ve organizasyonel yapıları kapsamaktadır.



Şekil 26. Kültür katman iş akışı

Literatürde veri yönetişiminin başarısız olmasının temel nedenlerinden biri teknik yetersizliklerden çok organizasyonel kültür eksikliği olarak değerlendirilmektedir (Fattah, 2024; Ladley 2019; Legner vd., 2023; SAS, 2018).

Üst yönetimin veri odaklı karar alma yaklaşımını benimsemesi ve veri kullanımını teşvik eden organizasyonel yapılar oluşturması, veri kültürünün kurum geneline yayılmasını desteklemektedir (Chatterjee vd., 2021; Nagle vd., 2020). Şekil 26’da veri odaklı kültür yapısını çevreleyen organizasyonel unsurlar liderlik desteği, veri okuryazarlığı, veri paylaşımı, etik ve sorumlu kullanım, iş birliği ve veri güveni gibi veri kültürünü besleyen temel bileşenleri içermektedir. Liderlik desteği, veri yönetişimi kültürünün kurumsallaşması açısından kritik öneme sahiptir. Veri okuryazarlığı düzeyi artmadan veri yönetişimi uygulamalarının sürdürülebilir olamamaktadır (Fattah, 2024). Veri yönetimi çabalarını iş hedefleriyle uyumlu hale getirmenin, üst düzey yönetim desteği, liderliği sağlamanın, iş birliği, şeffaflık ve hesap verebilirlik kültürünü geliştirmenin önemlidir (Chukwurah vd., 2024).

Kültür katmanının kuramsal temelini destekleyen önemli çalışmalardan biri Salerno ve Maçada'nın (2025) veri odaklı kültür yaklaşımıdır. Araştırmacılar veri yönetişimi ile veri odaklı kültür arasındaki ilişkinin veri kalitesi aracılığıyla güçlendiğini ortaya koymaktadır. Çalışmada veri kültürü verinin organizasyonel karar alma süreçlerinde temel referans olarak kullanılması, veri paylaşımının teşvik edilmesi ve veri kullanım alışkanlıklarının kurum genelinde yaygınlaştırılması biçiminde tanımlanmaktadır (Salerno ve Maçada, 2025).

Şeklin sağ bölümünde yer alan Veri Kalitesi Boyutları alanı, Salerno ve Maçada'ya (2025) göre veri odaklı kültürün gelişebilmesi için çalışanların kullandıkları veriye güven duyması gerekmektedir. Bu nedenle erişilebilirlik, güvenilirlik, bütünlük, kullanılabilirlik ve yorumlanabilirlik gibi veri kalite boyutları kültür katmanının temel destekleyicileri olarak değerlendirilmiştir. Veri kalitesinin düşük olduğu organizasyonlarda veri paylaşımı ve veri temelli karar alma davranışları zayıflamaktadır. Bu durum veri yönetişimi uygulamalarının sürdürülebilirliğini olumsuz etkilemektedir. Şekilde veri kalite boyutlarının kültür yapısıyla çift yönlü ilişki içerisinde gösterilmesi, veri kalitesi ile veri kültürü arasındaki karşılıklı etkileşimi vurgulamaktadır (ISO, 2025a; Salerno ve Maçada, 2025).

Şeklin sol bölümünde yer alan Destek Mekanizmaları, politika ve standartlar, eğitim ve farkındalık, iletişim ve iş birliği ile ölçme ve sürekli iyileştirme mekanizmaları yer almaktadır. Politika ve standartlar, veri kullanımına ilişkin ortak kuralların belirlenmesini sağlarken eğitim ve farkındalık faaliyetleri veri kültürünün kurum geneline yayılmasına katkı sunmaktadır. İletişim ve iş birliği mekanizmaları organizasyon içerisindeki veri paylaşım kültürünü desteklemektedir. Ölçme ve sürekli iyileştirme süreçleri ise kültürel dönüşümün sürdürülebilirliğini sağlamaktadır. Destek Mekanizmaları, kültür katmanının yönetim katmanı ile doğrudan ilişkili biçimde çalıştığını göstermektedir.

Şeklin alt bölümünde yer alan Kültürel Yönelimler alanı, Griffin ve Holcomb'un (2023) Kullanım ve Akış Veri Kültürü Modeli (Usage and Flow Data Culture Model, UFDCM) yaklaşımına dayandırılmıştır. Bu model, veri kültürünü verinin kullanım amacı ve verinin kurumsal akışı olmak üzere iki temel eksen üzerinden değerlendirmektedir. Şekilde yatay eksen verinin kurumsal akışını temsil etmektedir. Kapalı/merkezileşmiş yapıdan açık/paylaşım odaklı yapıya geçişi göstermektedir. Dikey eksen ise verinin kullanım

amacını ifade etmektedir. Operasyonel verimlilikten dışa dönük değer üretimine kadar uzanan kültürel dönüşümü ortaya koymaktadır. Bu iki eksenin kesişiminde geleneksel kültür¹⁴⁷, korumacı kültür¹⁴⁸, ilerlemeci kültür¹⁴⁹ ve koruyucu/gelecek odaklı¹⁵⁰ kültür olmak üzere dört farklı kültürel yönelim yer almaktadır (Griffin ve Holcomb, 2023).

Şeklin genel yapısı değerlendirildiğinde kültür katmanının diğer tüm katmanlarla doğrudan ilişkili olduğu görülmektedir. Stratejik katman ile veri vizyonunun kurumsal davranışlara aktarılması üzerinden bağlantı kurulurken yönetim katmanı ile rol farkındalığı, hesap verebilirlik ve veri sorumluluğu kültürü aracılığıyla ilişki sağlanmaktadır. Süreç katmanı ile veri kullanım alışkanlıkları ve iş birliği kültürü üzerinden etkileşim kurulmakta, teknik katman ile veri kalitesi boyutları bağlamında ilişki geliştirilmektedir. Yasal ve etik katman ile ise etik veri davranışı, gizlilik farkındalığı ve yasal uyum kültürü aracılığıyla bütünleşme sağlanmaktadır. Bu nedenle kültür katmanı, veri yönetimi modelinde tüm katmanlar arasında davranışsal bağ kuran yatay dönüşüm alanı olarak değerlendirilmektedir.

Kültür katmanı, görüşmelerde veri yönetimi faaliyetlerinin bazı çalışanlar tarafından ek iş yükü olarak algılanması, veri okuryazarlığı ve farkındalık eksikliği, kurumsal hafızanın yetersizliği, birimler arası iş birliği gereksinimi ve üst yönetim desteğinin belirleyici bir kolaylaştırıcı olarak görülmesi bulgularına dayanmaktadır. Bu bulgular, veri yönetiminin yalnızca yapısal ve teknik düzenlemelerle sürdürülemeyeceğini; eğitim, farkındalık, veri paylaşımı, veri güveni, iş birliği ve değişim yönetimi yoluyla desteklenmesi gerektiğini ortaya koymuştur. Uluslararası politika belgelerindeki eğitim, etik kullanım, şeffaflık, ortak veri dili ve hesap verebilirlik vurgusu da kültür katmanını

¹⁴⁷ Geleneksel veri kültürü, verinin daha çok ölçme, performans değerlendirme ve operasyonel süreçleri izleme amacıyla kullanıldığı yapılardır. Bu kültürde veri akışı görece serbesttir. Verinin temel kullanım amacı stratejik keşif veya yenilik üretmekten ziyade mevcut süreçlerin kontrol edilmesi ve performansın izlenmesidir.

¹⁴⁸ Korumacı veri kültürü, verinin sıkı biçimde kontrol edildiği ve daha çok operasyonel ölçüm, güvenlik ve uyumluluk amacıyla kullanıldığı yapılardır. Veri akışı sınırlıdır ve bilmesi gereken kadar erişim yaklaşımı benimsenmektedir.

¹⁴⁹ İlerlemeci veri kültürü, verinin kurum genelinde serbest biçimde paylaşıldığı ve stratejik anlam üretmek amacıyla aktif kullanıldığı en olgun veri kültürü türüdür. Bu kültürde veri yenilik, tahminleme, stratejik farklılaşma ve karar desteği sağlayan kurumsal bir varlık olarak görülmektedir.

¹⁵⁰ Koruyucu veya gelecek odaklı veri kültürü, verinin kontrollü biçimde tutulduğu stratejik analiz, geleceği öngörme ve rekabet avantajı yaratma amacıyla yoğun şekilde kullanıldığı yapılardır. Bu kültürde veri paylaşımı sınırlı olsa da veri kullanım kapasitesi oldukça gelişmiştir.

güçlendirmektedir. Bu bulguların model bileşenleriyle ilişkisi Ek 7 ve Ek 8’de sunulmuştur.

5.2.6. Yasal ve Etik Katman

Yasal ve etik katman, üniversitelerde veri yönetiřimi süreçlerinin hukuki, etik ve düzenleyici çerçeveler doğrultusunda yürütölmesini saęlayan koruyucu yönetiřim alanını temsil etmektedir. Bu katman verinin güvenli, řeffaf, hesap verebilir, etik ilkelere uygun ve yasal düzenlemelerle uyumlu biçimde yönetilmesini amaçlamaktadır.



Şekil 27. Yasal ve etik katman iş akışı

Şekil 27’de gösterilen yasal ve etik katman, veri yönetiřimi uygulamalarının sürdürülebilirlięi açısından veri güvenlięi, mahremiyet, etik kullanım ve yasal uyum temel belirleyiciler arasında deęerlendirilmektedir (Khatri ve Brown, 2010). Özellikle yükseköğretim kurumlarında öğrenci, akademik personel, araştırma ve kurumsal verilerin yoğun biçimde işlenmesi veri güvenlięi ve gizlilik konularını kritik hale getirmektedir.

Bu katmanda veri yönetiřimi küresel standartlar ve ulusal düzenlemelerle ilişkili biçimde ele alınmaktadır. Veri yönetiřimi uygulamalarının farklı kurumlar arasında birlikte

çalışabilir, sürdürülebilir ve güvenilir biçimde yürütülebilmesi için uluslararası standartlarla uyumlu olması gerektiği belirtilmektedir (ISO, 2018). Bu nedenle model kapsamında yasal ve etik katman hem düzenleyici standartları hem de stratejik politika belgelerini bütünleşik biçimde ele almaktadır.

Şeklin sol tarafında yer alan Düzenleyici Çerçeveler veri yönetişiminin hukuki ve standart temelli altyapısını oluşturmaktadır. Bu bölümde yer alan KVKK ve GDPR düzenlemeleri, kişisel verilerin korunması, veri işleme süreçlerinin şeffaf yürütülmesi, veri sahipliği haklarının korunması ve bireysel mahremiyetin güvence altına alınmasını amaçlamaktadır. Özellikle GDPR ile birlikte veri minimizasyonu, açık rıza, hesap verebilirlik ve veri taşınabilirliği gibi ilkeler veri yönetişimi uygulamalarının temel unsurları haline gelmektedir.

ISO/IEC 27001 ve ISO/IEC 27701 standartları ise bilgi güvenliği ve gizlilik yönetimi süreçlerini düzenlemektedir. ISO/IEC 27001, veri güvenliği risklerinin yönetilmesini, erişim kontrol mekanizmalarının oluşturulmasını ve bilgi varlıklarının korunmasını sağlarken ISO/IEC 27701 kişisel veri gizliliği yönetim sistemlerini desteklemektedir (ISO 2022; ISO 2025b).

ISO/IEC 38505 serisi, veri yönetişiminin kurumsal yönetim yaklaşımıyla ilişkilendirilmesini temsil etmektedir. Bu standart verinin stratejik bir kurumsal varlık olarak yönetilmesini, üst yönetim sorumluluğunu ve karar alma süreçlerinde veri odaklı yönetim anlayışını desteklemektedir (ISO, 2017; ISO, 2018; ISO, 2021). ISO/IEC 11179 standardı ise üst veri ve veri sözlüğü yönetimini düzenleyerek veri tanımlarının standartlaştırılmasını ve ortak veri anlayışının oluşturulmasını sağlamaktadır. Standart üniversitelerde farklı bilgi sistemleri arasında veri bütünlüğünün korunması açısından kritik öneme sahiptir (ISO 2019; ISO, 2023b).

Veri kalitesine ilişkin ISO 8000-51:2023, ISO/IEC 5259-5:2025 ve ISO/IEC 25642:2025 standartları ise veri kalite yönetimi, veri kalite değerlendirme çerçeveleri ve veri yönetişiminde kalite ilkelerinin uygulanmasına odaklanmaktadır. Bu standartlar, veri yönetişiminin güvenilir, doğru, kullanılabilir ve sürdürülebilir veri üretimini de kapsamı gerektiğini göstermektedir (ISO, 2023a; ISO 2025a; ISO, 2025c).

Şeklin sağ bölümünde yer alan Stratejik Politika Çerçevesi alanı, veri yönetişiminin ulusal stratejiler ve kurumsal politika belgeleriyle ilişkilendirilmesini temsil etmektedir. Bu bölümde yer alan 12. Kalkınma Planı¹⁵¹, Ulusal Yapay Zeka Stratejisi, YÖK dijital dönüşüm politikaları¹⁵² ve açık bilim politikaları üniversitelerde veri temelli dönüşümün ulusal düzeyde temsilcileridir. Özellikle Ulusal Yapay Zeka Stratejisi veri paylaşımı, veri güvenliği, açık veri ekosistemleri ve etik yapay zeka uygulamaları açısından yükseköğretim kurumlarına önemli sorumluluklar yüklemektedir. UNESCO Yapay Zeka Etik Rehberi ise yapay zeka uygulamalarında insan hakları, şeffaflık, adalet, kapsayıcılık ve hesap verebilirlik ilkelerini ön plana çıkarmaktadır (UNESCO, 2021).

Şekilde yer alan Üniversite Veri Politikaları, Yönergeler ve Yönetmelikler, üniversitenin kendi içinde bulunan kurumsal düzenlemelerdir. Üniversitelerin veri erişim politikaları, araştırma verisi yönetimi politikaları, açık erişim politikaları, bilgi güvenliği yönergeleri ve etik veri kullanım ilkeleri vb. yapılarıdır (ISO, 2021). Böylece yasal ve etik katman, genel düzenleyici çerçevelerin üniversite düzeyinde kurumsallaştırılmasını sağlayan uygulama alanı haline dönüşmektedir.

Model kapsamında yasal ve etik katman, diğer tüm katmanlarla doğrudan ilişkilidir. Stratejik katman ile kurumsal veri stratejisinin yasal düzenlemelerle uyumlu biçimde oluşturulmasını desteklemektedir. Yönetişim katmanı ile veri sorumluluklarının, hesap verebilirlik mekanizmalarının ve etik kurulların yapılandırılması üzerinden ilişki kurmaktadır. Süreç katmanı ile veri erişim, paylaşım, saklama ve imha süreçlerinin hukuki ilkelere uygun yürütülmesini sağlamaktadır. Teknik katman ile bilgi güvenliği, erişim kontrolü, loglama ve veri koruma altyapıları üzerinden bütünleşmektedir. Kültür katmanı ile ise etik veri davranışı, gizlilik farkındalığı ve sorumlu veri kullanım kültürünün geliştirilmesi açısından etkileşim içerisindedir.

Yasal ve etik katman, görüşmelerde KVKK, mahremiyet, anonimleştirme, veri güvenliği, veri sınıflandırması, erişim ve paylaşım politikalarına duyulan gereksinimin vurgulanmasına dayanmaktadır. Özellikle veri kümelerinin paylaşım öncesinde kişisel verilerden arındırılması, bilgi güvenliği standartlarına uyum sağlanması ve yazılı veri

¹⁵¹ Bkz. https://www.sbb.gov.tr/wp-content/uploads/2023/12/On-Ikinci-Kalkinma-Plani_2024-2028_11122023.pdf

¹⁵² Bkz. <https://www.yok.gov.tr/tr>

kullanım politikalarının geliştirilmesi gereği, bu katmanın modelde bağımsız biçimde ele alınmasını gerekli kılmıştır. Uluslararası politika belgelerinde GDPR, FERPA, HIPAA ve benzeri düzenlemeler, veri öznesi hakları, saklama-imha hükümleri, mahremiyet ve etik veri kullanım ilkeleriyle birlikte öne çıkmaktadır. Bu nedenle yasal ve etik katman, diğer katmanların üzerinde işleyen ve veri yönetişimi uygulamalarının hukuki, etik ve düzenleyici sınırlarını belirleyen bir koruyucu çerçeve olarak tasarlanmıştır. Ayrıntılı eşleştirmeler Ek 7 ve Ek 8’de yer almaktadır.

5.3. MODELİN UYGULANMASINA YÖNELİK EYLEM PLANI

5.3.1. Eylem Planının Amacı ve Kapsamı

Üniversiteler İçin Katmanlı Veri Yönetişimi Modeli, stratejik, yönetim, süreç, teknik, kültür, yasal ve etik katmanlardan oluşmaktadır. Modelin tüm bileşenlerinin aynı anda uygulanması insan kaynağı, bütçe, teknik altyapı, kurumsal koordinasyon ve değişim yönetimi açısından üniversiteler için güç olabilir. Modelin üniversitelerde uygulanmasını kolaylaştırmak amacıyla aşamalı, ölçülebilir ve önceliklendirilmiş bir veri yönetişimi eylem planı geliştirilmiştir.

Eylem planı, üniversitelerin mevcut kaynaklarını kullanarak kısa sürede temel yönetim yapılarını oluşturmasını, öncelikli veri alanlarında pilot uygulamalar gerçekleştirmesini ve elde edilen sonuçlar doğrultusunda veri yönetişimini kurum geneline yaymasını amaçlamaktadır. Başlangıçta plan, üniversitenin bütün veri varlıklarını aynı anda kapsamak yerine herhangi bir veri türü (öğrenci, akademik performans, araştırma, personel veya bütçe) üzerine pilot uygulama yapılmasını öngörmektedir.

Eylem planı toplam 24 aylık bir dönemi kapsamakta ve altı aşamadan oluşmaktadır:

1. Kurumsal hazırlık ve üst yönetim sahipliği
2. Mevcut durum ve veri envanteri
3. Politika, rol ve standartların oluşturulması
4. Pilot uygulama ve teknik kontroller
5. Kurum geneline yaygınlaştırma

6. İzleme, olgunluk değerlendirmesi ve sürekli iyileştirme

Eylem planının uygulanmasında aşağıdaki adımlar esas alınabilir:

- Veri yönetişimi üniversitenin akademik ve idari birimlerini kapsayan kurumsal dönüşüm programı olarak yürütülmelidir.
- Rektörlük düzeyinde açık sahiplenme sağlanmadan kapsamlı teknik yatırımlara başlanmamalıdır.
- Veri yönetişimi için ilk aşamada yeni ve büyük bir organizasyon kurmak yerine mevcut birimlerden oluşturulan çekirdek ekip kullanılmalıdır.
- Kurumsal önemi ve risk düzeyi yüksek bir veri alanı pilot olarak seçilmeli ve üniversitenin bütün verileri aynı anda ele alınmamalıdır.
- Önce politika, rol, süreç ve standartlar oluşturulmalıdır.
- Yalnızca yazılım veya veri ambarı yatırımına dayalı bir uygulama yürütülmemelidir.
- Her aşamanın sonunda ölçülebilir çıktılar değerlendirilmelidir ve bir sonraki aşamaya geçiş kararı Veri Yönetişimi Kurulu tarafından verilmelidir.
- Yasal uyum, etik kullanım, veri güvenliği ve veri kültürü tüm aşamalarda yatay bileşenler olarak ele alınmalıdır.

5.3.2. Aşamalı Veri Yönetişimi Eylem Planı

5.3.2.1. Aşama 1: Kurumsal Hazırlık ve Üst Yönetim Sahipliği

Zaman dilimi: 0–30 gün

Amaç: Veri yönetişimi çalışmalarına kurumsallık kazandırmak için üst yönetim desteğini görünür hale getirmek ve uygulamayı yönetecek geçici çekirdek yapıyı oluşturmaktır.

1.1. Üst yönetim sponsorunun belirlenmesi: Rektör veya veri yönetiminden sorumlu rektör yardımcısı, programın üst yönetim sponsoru olarak belirlenmelidir. Sponsorun görevi kaynak tahsisi yapmak, birimler arası anlaşmazlıkları çözmek ve veri yönetişimini üniversitenin stratejik hedefleriyle ilişkilendirmektir.

Sorumlu: Rektörlük

Çıktı: Üst yönetim sponsorunun görevlendirme yazısı

Başarı göstergesi: Sponsorun resmî olarak belirlenmesi

1.2. Veri Yönetişimi Kurulu oluşturulması: Kurulun başkanı üst yönetim sponsorudur. Kurulda akademik ve idari birimler dengeli biçimde temsil edilmelidir. Kurulun temel görevleri: Veri politikalarını onaylamak, veri standartlarını belirlemek, veri sahiplerini atamak, birimler arası anlaşmazlıkları çözmek, veri kalitesi hedeflerini onaylamak, veri erişimi ve paylaşımına ilişkin üst düzey kararları almak, performans göstergelerini izlemek, modelin uygulanmasını değerlendirmek. Kurulun başlangıçta 7–12 kişiden oluşması yeterlidir. İlk aşamada geniş katılımlı ve ağır işleyen bir yapı yerine karar alabilen çekirdek ekip tercih edilmelidir.

Sorumlu: Üst yönetim sponsoru

Çıktı: Veri Yönetişimi Kurulu kuruluş kararı ve görev tanımı

Başarı göstergesi: En az altı temel kurumsal birimin temsil edilmesi

1.3. Veri Yönetişimi Ofisinin Kurulması: Veri ile ilgili tüm operasyonel süreçleri yürütmek, veri politikalarının ve standartlarının uygulanması, veri yönetişimi süreçlerinin koordinasyonu, veri kalitesi yönetimi, üst veri yönetimi ve olgunluk değerlendirme faaliyetlerini yürütmek. Başlangıçta yönetici, yönetici yardımcısı ve uzman personel görevlendirmeleri tercih edilmelidir.

Sorumlu: Veri Yönetişimi Kurulu

Çıktı: Veri yönetişimi ofisinin kuruluş kararı, ofis yöneticisinin görevlendirilmesi, organizasyon şeması

Başarı göstergesi: Veri Yönetişimi Ofisinin resmî olarak kurulması ve görevlendirilmelerin yapılması

1.4. Veri yönetişimi program bildirgesinin hazırlanması: Programın amacı, kapsamı, süresi, başlangıç öncelikleri, karar organları ve beklenen sonuçları iki veya üç sayfalık bir program bildirgesinde açıklanmalıdır. Bildirge en az şu unsurları içermelidir: Veri

yönetişimi programının amacı, kurumsal gereksinim ve sorun alanları, üst yönetim sponsorluğu, veri yönetişimi kurulu ve ofisinin yetkileri, pilot uygulama yaklaşımı, ilk 12 aylık temel hedefler, raporlama ve izleme biçimi.

Sorumlu: Veri Yönetişimi Ofisi

Çıktı: Veri Yönetişimi Program Bildirgesi

Başarı göstergesi: Bildirgenin Üst Yönetim Sponsoru ve Veri Yönetişimi Kurulu tarafından onaylanması

1.4. Öncelikli veri alanının seçilmesi: İlk uygulama için tek bir veri alanı belirlenmelidir. Pilot veri alanı şu ölçütlere göre seçilebilir: üst yönetim kararlarında sık kullanılması, birden fazla birim tarafından üretilmesi veya kullanılması, tutarsızlık ve mükerrerlik sorunlarının bulunması, raporlama ve denetim açısından önem taşıması, sonuçlarının altı ay içinde ölçülebilir olması. Üniversiteler açısından akademik performans verileri, öğrenci sayıları, araştırma verileri veya personel verileri uygun pilot alanlar olabilir.

Sorumlu: Veri Yönetişimi Kurulu ve Veri Yönetişimi Ofisi

Çıktı: Pilot veri alanı karar tutanağı

Başarı göstergesi: Bir veri alanının kapsamı ve sınırlarıyla belirlenmesi

Aşama 1 tamamlanma ölçütü: Üst Yönetim Sponsoru atanmıştır. Veri Yönetişimi Kurulu ve Veri Yönetişimi Ofisi kurulmuştur. Program bildirgesi onaylanmıştır. Pilot veri alanı seçilmiştir.

5.3.2.2. Aşama 2: Mevcut Durum Analizi ve Veri Envanteri

Zaman dilimi: 1–3. aylar

Amaç: Üniversitenin veri varlıklarını, bilgi sistemlerini, veri akışlarını, sorumluluklarını ve temel risklerini görünür hale getirmektir.

2.1. Mevcut düzenlemelerin envanterinin çıkarılması: Üniversitede veriyle ilişkili bütün politika, yönerge, prosedür ve rehberler belirlenmelidir. Bunlar arasında şunlar yer

alabilir: bilgi güvenliği politikası, KVKK ve kişisel veri politikaları, açık erişim politikası, araştırma verisi yönetimi politikası, kayıt saklama ve imha planları, yetkilendirme prosedürleri, bilgi sistemi kullanım yönergeleri, etik kurul düzenlemeleri, veri paylaşım protokolleri. Her belgenin sahibi, yürürlük tarihi, kapsamı, güncelliği ve veri yönetişimi modeliyle ilişkisi kaydedilmelidir.

Sorumlu: Veri Yönetişimi Ofisi ve Hukuk/KVKK birimi

Çıktı: Düzenleyici belge envanteri

Başarı göstergesi: Mevcut belgelerin tamamının tek listede toplanması

2.2. Bilgi sistemleri envanterinin hazırlanması: Öğrenci bilgi sistemi, personel sistemi, idari ve mali sistemler, akademik performans sistemleri, araştırma sistemleri, kütüphane sistemleri, öğrenme yönetim sistemi ve kurumsal raporlama uygulamaları belirlenmelidir. Her sistem için şu bilgiler kaydedilmelidir: Sistem adı ve amacı, sistemin sahibi, teknik yöneticisi, kullanan birimler, ürettiği temel veriler, entegre olduğu sistemler, veri aktarım yöntemi, yedekleme durumu, erişim yöntemi, saklanan kişisel veya hassas veriler.

Sorumlu: Bilgi İşlem Daire Başkanlığı ve Veri Yönetişimi Ofisi

Çıktı: Bilgi sistemleri ve entegrasyon envanteri

Başarı göstergesi: Kritik sistemlerin en az %90'ının kayıt altına alınması

2.3. Pilot alan veri envanterinin oluşturulması: Pilot alandaki temel veri kümeleri, göstergeler, raporlar ve veri kaynakları belirlenmelidir. Başlangıçta bütün veri alanlarını kapsayan kapsamlı bir veri kataloğu yerine basit bir elektronik tablo kullanılabilir. Veri envanterinde en az şu alanlar bulunmalıdır: Veri kümesinin adı, veri tanımı, veri kaynağı, verinin üretildiği birim, veri sahibi, veri sorumlusu, kullanım amacı, veri sınıfı, saklama süresi, paylaşıldığı birimler, kalite sorunu, güncelleme sıklığı, ilgili mevzuat.

Sorumlu: Pilot alandaki birim temsilcileri ve Veri Yönetişimi Ofisi

Çıktı: Pilot veri envanteri

Başarı göstergesi: Öncelikli veri kümelerinin en az %80'inin kayıt altına alınması

2.4. Veri akışlarının haritalanması: Pilot alanda verinin nerede üretildiği, kim tarafından doğrulandığı, hangi sistemlere aktarıldığı, hangi raporlarda kullanıldığı ve kimlerle paylaşıldığı belirlenmelidir. Veri akış haritalarında şu sorular yanıtlanmalıdır: Veri ilk olarak nerede üretilmektedir? Veriyi kim girmektedir? Veriyi kim onaylamaktadır? Veri hangi sistemlere aktarılmaktadır? Aynı veri başka sistemlerde yeniden üretilmekte midir? Raporlamada hangi veri kaynağı esas alınmaktadır? Hatalı veri tespit edildiğinde kim düzeltmektedir?

Sorumlu: Pilot alandaki birim temsilcileri, Bilgi İşlem Daire Başkanlığı ve Veri Yönetişimi Ofisi

Çıktı: Pilot veri akış şeması

Başarı göstergesi: Kritik veri akışlarının kaynak-hedef ilişkileriyle gösterilmesi

2.5. Başlangıç olgunluk değerlendirmesinin yapılması: Üniversitenin başlangıç durumu modelin altı katmanı üzerinden değerlendirilmelidir. Her katman için 1–5 arasında başlangıç puanı verilebilir: Başlangıç, Tekrarlanabilir, Tanımlanmış, Yönetilen, Optimize edilmiş en az şu alanları kapsamalıdır: Strateji ve üst yönetim sahipliği, roller, karar hakları, veri süreçleri, veri kalitesi, teknik altyapı, veri kültürü, farkındalık, yasal ve etik uyum.

Sorumlu: Veri Yönetişimi Kurulu ve Veri Yönetişimi Ofisi

Çıktı: Başlangıç olgunluk raporu

Başarı göstergesi: Altı katman için başlangıç puanlarının belirlenmesi

Aşama 2 tamamlanma ölçütü: Düzenleyici belge envanteri hazırlanmıştır. Kritik bilgi sistemleri listelenmiştir. Pilot veri envanteri oluşturulmuştur. Temel veri akışları haritalanmıştır. Başlangıç olgunluk düzeyi ölçülmüştür.

5.3.2.3. Aşama 3: Politika, Organizasyon ve Standartların Oluşturulması

Zaman dilimi: 3–6. aylar

Amaç: Veri yönetişiminin kurumsal organizasyonunu oluşturmak, karar yetkilerini belirlemek ve pilot uygulamada kullanılacak temel politika ve standartları hazırlamaktır.

3.1. Veri yönetişimi rollerinin atanması: Pilot veri alanı için en az şu roller tanımlanmalıdır: Veri sponsoru: Üst yönetim desteğini ve kaynak tahsisini sağlar. Veri sahibi: Veri alanına ilişkin nihai yönetsel sorumluluğu taşır. Veri sorumlusu: Veri tanımlarını, kalite kurallarını ve günlük uygulamaları yönetir. Teknik veri sorumlusu: Verinin teknik güvenliğini, erişilebilirliğini ve sistem bütünlüğünü sağlar. Veri kullanıcısı: Veriyi yetkisi ve görevi doğrultusunda kullanır. Veri yönetişimi birimi: Koordinasyon, izleme, rehberlik ve raporlama görevini yürütür. Her rol için RACI temelli sorumluluk matrisi hazırlanmalıdır.

Çıktı: Rol ve sorumluluk matrisi

Başarı göstergesi: Pilot veri kümelerinin tamamına veri sahibi ve veri sorumlusu atanması

3.2. Kurumsal veri yönetişimi politikasının hazırlanması: Başlangıç politikası aşırı ayrıntılı olmamalıdır. İlk politika şu başlıkları kapsamalıdır: Amaç, kapsam, temel ilkeler, kurumsal veri tanımı, veri sahipliği, roller ve sorumluluklar, veri sınıflandırması, veri kalitesi, veri erişimi ve paylaşımı, veri güvenliği ve gizlilik, saklama ve imha, ihlal bildirimi, eğitim ve farkındalık, izleme ve güncelleme.

Sorumlu: Veri Yönetişimi Ofisi, Hukuk/KVKK ve Bilgi İşlem Daire Başkanlığı

Çıktı: Onaylanmış Kurumsal Veri Yönetişimi Politikası

Başarı göstergesi: Politikanın Senato ve/veya ve Veri Yönetişimi Kurulu tarafından onaylanması

3.3. Veri sınıflandırma standardının hazırlanması: Üniversitenin bütün verileri için başlangıçta dört temel sınıf kullanılabilir: Kamuya açık, kurum içi, hassas/korumalı, kısıtlı/kritik. Her sınıf için erişim, paylaşım, depolama, şifreleme, saklama ve imha kuralları belirlenmelidir.

Çıktı: Veri sınıflandırma ve etiketleme standardı

Başarı göstergesi: Pilot alandaki veri kümelerinin %100'ünün sınıflandırılması

3.4. Pilot veri sözlüğünün hazırlanması: Pilot veri alanındaki kritik göstergeler için ortak tanımlar oluşturulmalıdır. Örneğin “aktif öğrenci”, “uluslararası öğrenci”, “akademik personel”, “yayın sayısı” veya “mezuniyet oranı” gibi göstergelerin hesaplama kuralları netleştirilmelidir. Her veri sözlüğü kaydı şu bilgileri içermelidir: Terim, tanım, hesaplama kuralı, veri kaynağı, veri sahibi, güncelleme sıklığı, geçerlilik tarihi, ilgili raporlar, onaylayan kurul.

Çıktı: Pilot veri sözlüğü

Başarı göstergesi: En az 25–50 kritik veri ögesinin tanımlanması

3.5. Veri kalitesi kurallarının belirlenmesi: Pilot veri alanı için doğruluk, bütünlük, tutarlılık, güncellik, geçerlilik ve erişilebilirlik boyutlarında kurallar oluşturulmalıdır. Örnek kalite göstergeleri: Zorunlu alanların doluluk oranı, mükerrer kayıt oranı, hatalı kimlik veya kod oranı, sistemler arası tutarsızlık oranı, zamanında güncellenen kayıt oranı, manuel girilen ve doğrulanmamış veri oranı.

Çıktı: Veri kalitesi kural seti

Başarı göstergesi: Pilot alan için en az 10 ölçülebilir kalite kuralının tanımlanması

5.3.2.4. Aşama 4: Pilot Uygulama ve Hızlı Kazanımlar

Zaman dilimi: 6–9. aylar

Amaç: Oluşturulan politika, rol, standart ve teknik kontrolleri sınırlı bir veri alanında uygulamak ve kısa sürede ölçülebilir sonuç üretmektir.

4.1. Pilot veri kayıtlarının temizlenmesi: Pilot veri kümesindeki eksik, hatalı, mükerrer ve tutarsız kayıtlar belirlenmelidir. Hatalar veri sorumluları ve ilgili birimler tarafından düzeltilmelidir.

Çıktı: Temizlenmiş pilot veri kümesi

Başarı göstergeleri: Mükerrer kayıtların en az %50 azaltılması, zorunlu alan doluluk oranının %95'e çıkarılması, kritik tutarsızlıkların giderilmesi

4.2. Rol temelli erişimlerin uygulanması: Pilot alandaki mevcut kullanıcı yetkileri incelenmeli ve görev tanımlarıyla uyumsuz erişimler kaldırılmalıdır. Uygulamada: Kullanıcı–rol matrisi hazırlanmalı, ayrılan personelin erişimleri kapatılmalı, görev değişiklikleri yetkilere yansıtılmalı, hassas verilere erişim ek onaya bağlanmalı, periyodik yetki gözden geçirmesi başlatılmalı.

Çıktı: Güncellenmiş erişim matrisi

Başarı göstergesi: Yetkilerin %100’ünün görev ve rol ile eşleştirilmesi

4.3. Erişim ve hareket kayıtlarının tutulması: Kritik veriler üzerinde kimlerin görüntüleme, değiştirme, aktarma veya silme işlemi yaptığı kayıt altına alınmalıdır.

Çıktı: Loglama ve izleme düzeni

Başarı göstergesi: Kritik sistemlerde erişim ve hareket kayıtlarının tutulması ve aylık kontrol edilmesi

4.4. Pilot rapor veya gösterge panelinin hazırlanması: Temizlenmiş ve doğrulanmış veri kullanılarak üst yönetim için sınırlı kapsamlı bir rapor veya gösterge paneli hazırlanmalıdır. Gösterge paneli başlangıçta en fazla 10–15 kritik gösterge içermelidir. Göstergelerin veri sözlüğündeki tanımlarla uyumlu olması sağlanmalıdır.

Çıktı: Pilot yönetim gösterge paneli

Başarı göstergesi: Göstergelerin veri sahibi tarafından onaylanması

4.5. Veri erişim ve paylaşım iş akışının uygulanması: Veri talepleri e-posta veya sözlü iletişim yerine standart bir form üzerinden alınmalıdır. Talepte en az şu bilgiler bulunmalıdır: Talep edilen veri, kullanım amacı, talep sahibi, kullanım süresi, paylaşım biçimi, kişisel veya hassas veri içerip içermediği, onaylayan veri sahibi, imha veya erişim sonlandırma tarihi.

Çıktı: Veri erişim ve paylaşım talep formu

Başarı göstergesi: Pilot alandaki taleplerin %90’ının kayıtlı süreç üzerinden yürütülmesi

4.6. Hizmet içi eğitimlerin verilmesi: Pilot birim çalışanlarına 60–90 dakikalık kısa eğitimler verilmelidir. Eğitim içeriği: Veri yönetiřimi nedir? Veri sahibi ve veri sorumlusu kimdir? Veri sınıflandırması nasıl yapılır? Veri paylaşımında nelere dikkat edilir? Veri kalitesinden kim sorumludur? İhlal durumunda ne yapılır?

Çıktı: Eğitim materyali ve katılım listesi

Başarı göstergesi: Pilot birimdeki ilgili çalışanların en az %80’inin eğitimi tamamlaması

5.3.2.5. Aşama 5: Değerlendirme ve Kurum Geneline Yaygınlaştırma

Zaman dilimi: 9–18. aylar

Amaç: Pilot uygulamanın sonuçlarını değerlendirmek, başarılı uygulamaları standartlaştırmak ve veri yönetiřimi modelini diğerkurumsal veri alanlarına yaymaktır.

5.1. Pilot uygulama değerlendirme raporunun hazırlanması: Pilot öncesi ve sonrası veriler karşılaştırılmalıdır. Değerlendirmede řu sorular yanıtlanmalıdır: Veri kalitesi ne ölçüde iyileřmiştir? Veri üretim ve raporlama süresi azalmıř mıdır? Mükerrer veri üretimi azalmıř mıdır? Eriřim yetkileri daha kontrollü hale gelmiř midir? Kullanıcıların farkındalıęı artmıř mıdır? Hangi politika veya süreçler uygulanamamıřtır? Yeni insan kaynaęı veya teknik yatırım gereksinimi oluřmuř mudur?

Çıktı: Pilot değerlendirme ve öğrenilen dersler raporu

5.2. İkinci ve üçüncü veri alanlarının seçilmesi: Pilot uygulama başarıyla tamamlandıktan sonra model, kurumsal risk ve stratejik önceliklere göre diğerveri alanlarına yaygınlaştırılmalıdır.

Önerilen sıra: Akademik performans ve araştırma verileri, öğrenci ve eğitim verileri, personel verileri, mali ve idari veriler, kütüphane ve öğrenme sistemleri verileri, dış paylaşımlar

5.3. Kurumsal veri kataloğunun genişletilmesi: Pilot envanterde kullanılan yapı üniversite geneline yaygınlaştırılmalıdır. Başlangıçta elektronik tabloyla yürütölen katalog, veri hacmi ve kaynaklar yeterliyse kurumsal veri kataloęu yazılımına

aktarılabılır. Başarı göstergesi: Kritik kurumsal veri kümelerinin en az %70'inin kataloglanması

5.4. Kurumsal veri sözlüğünün genişletilmesi: Birimlerce kullanılan temel göstergeler ve veri tanımları ortak sözlüğe eklenmelidir. Bir gösterge için birden fazla tanım bulunması halinde Veri Yönetişimi Kurulu karar vermelidir.

Başarı göstergesi: Kritik kurumsal göstergelerin en az %80'inin standart tanıma uyması

5.5. Veri entegrasyon önceliklerinin belirlenmesi: Bütün sistemlerin aynı anda entegre edilmesi yerine en çok veri tekrarı ve tutarsızlığı üreten sistemler önceliklendirilmelidir. Her entegrasyon için ana veri kaynağı, hedef sistem, veri sahibi, aktarım sıklığı, kontrol kuralı, hata yönetimi, teknik sorumlu belirlenmelidir.

Çıktı: Entegrasyon önceliklendirme planı

Başarı göstergesi: En az iki kritik sistem arasındaki manuel veri aktarımının azaltılması

5.6. Saklama, arşivleme ve imha kurallarının uygulanması: Veri türleri için yasal, idari, akademik ve tarihsel gerekliliklere göre saklama süreleri belirlenmelidir. Süresi dolan veriler için güvenli imha süreçleri oluşturulmalıdır.

Çıktı: Veri saklama ve imha planı

Başarı göstergesi: Kritik veri türlerinin tamamı için saklama süresinin belirlenmesi

5.7. Veri ihlali ve uyumsuzluk yönetiminin yapılandırılması: Veri ihlali, yetkisiz erişim, yanlış paylaşım veya veri kaybı durumunda izlenecek adımlar tanımlanmalıdır. Süreç şu aşamalardan oluşmalıdır: İhlalin bildirilmesi, ilk değerlendirmenin yapılması, etkilenen veri ve kişilerin belirlenmesi, teknik ve yönetsel önlemlerin alınması, hukuk/KVKK biriminin değerlendirmesi, gerekli bildirimlerin yapılması, düzeltici ve önleyici faaliyetlerin uygulanması

Çıktı: Veri ihlali müdahale prosedürü

5.3.2.6. Aşama 6: Kurumsallaştırma, Ölçme ve Sürekli İyileştirme

Zaman dilimi: 18–24. aylar

Amaç: Veri yönetişimini geçici bir proje olmaktan çıkararak üniversitenin sürekli yönetim faaliyetlerinden biri haline getirmektir.

6.1. Veri yönetişimi performans göstergelerinin izlenmesi: Performans göstergeleri üçer veya altışar aylık dönemlerde izlenmelidir.

Önerilen temel göstergeler: Veri sahibi atanmış kritik veri kümelerinin oranı, ortak tanımı oluşturulmuş kritik göstergelerin oranı, veri kalite kurallarını karşılayan kayıtların oranı, periyodik olarak gözden geçirilen kullanıcı yetkilerinin oranı, kayıt altına alınan ve kapatılan ihlal sayısı, entegre edilen kritik sistem sayısı, eğitimi tamamlayan çalışan oranı doğrulanmış veriyle hazırlanan yönetim raporlarının oranı, standart form üzerinden yürütülen veri taleplerinin oranı, güncel politika ve prosedürlerin oranı.

6.2. Yıllık olgunluk değerlendirmesinin yapılması: Başlangıçta yapılan değerlendirme 12. ve 24. aylarda tekrarlanmalıdır. Her katmanın puanındaki değişim raporlanmalıdır.

Hedeflenen asgari gelişim: Üniversitenin *başlangıç* düzeyindeki olgunluk seviyesinin 24 ay sonunda *tanımlanmış* düzeye ulaşması, kritik süreçlerin belgelenmesi, rollerinin atanması, en az bir veri alanında ölçülebilir kalite iyileşmesi, düzenli kurul ve raporlama mekanizmasının çalışması.

6.3. Politika ve standartların güncellenmesi: Politika ve standartlar yılda en az bir defa veya önemli mevzuat, organizasyon ya da sistem değişikliği olduğunda gözden geçirilmelidir. Her belge için belge sahibi, onaylayan makam, yürürlük tarihi, son gözden geçirme tarihi, sonraki gözden geçirme tarihi, değişiklik geçmişi tutulmalıdır.

6.4. Veri yönetişimi faaliyet raporunun yayımlanması: Üniversite içinde paylaşılacak üzere yıllık faaliyet raporu hazırlanmalıdır. Raporda şu bilgiler yer alabilir: Oluşturulan politika ve standartlar, atanan veri sahipleri ve sorumluları, veri kalitesi sonuçları, tamamlanan entegrasyonlar, eğitim faaliyetleri, ihlal ve uyumsuzluk istatistikleri, pilot uygulama sonuçları, sonraki yılın öncelikleri

6.5. Kurumsal bütçe ve insan kaynağının kalıcı hale getirilmesi: Pilot uygulama sonuçlarına göre veri yönetişimi birimine kalıcı personel, görev süresi ve bütçe ayrılmalıdır. Veri yönetişimi yalnızca akademisyenlerin ek görevleriyle

yürütülmemelidir. Veri analizi, veri kalitesi, bilgi yönetimi, veri güvenliği ve hukuk alanlarında uzmanlık desteği sağlanmalıdır.

5.4. TARTIŞMA

Bu araştırmanın en önemli katkısı, veri yönetişimi alanında geliştirilen uluslararası standart, çerçeve ve iyi uygulama örneklerini yükseköğretim kurumlarının özgün ihtiyaçları doğrultusunda ampirik bulgularla bütünleştirerek Üniversiteler İçin Katmanlı Veri Yönetişimi Modelini geliştirmiş olmasıdır. Literatürde yer alan DMBOK2, DCAM, DGI, ISO/IEC 38505 ve OECD gibi veri yönetişimi yaklaşımları veri yönetişiminin temel ilkelerini ortaya koymaktadır. Bu çerçeveler yükseköğretim kurumlarına özgü organizasyon yapıları ve yönetsel gereksinimleri ele almamaktadır. Bu sebeple uluslararası üniversitelerin veri yönetişimi politika belgelerinin tematik analizi, Türkiye'deki üniversitelerin mevcut durumuna ilişkin doküman incelemeleri ve Türkiye'deki 10 üniversite temsilcisi ile gerçekleştirilen yarı yapılandırılmış görüşmelerden elde edilen araştırma bulguları ile birlikte değerlendirilmiştir. Böylece modelin her bir katmanı, kuramsal yaklaşımlar ile araştırma kapsamında elde edilen ampirik bulguların bütünleştirilmesi sonucunda oluşturulmuştur.

Araştırmanın önemli bulgularından biri, uluslararası üniversitelerde veri yönetişiminin açık rol tanımları, kurumsallaşmış yönetim mekanizmaları, veri standartları ve güçlü politika belgeleriyle desteklenirken Türkiye'deki üniversitelerde uygulamaların kurumdan kuruma değiştiği, veri yönetişimi yapılanmalarının henüz gelişim sürecinde olduğu ve birçok faaliyetin teknik birimler tarafından yürütüldüğüdür. Doküman analizinde veri yönetişimi birimlerinin kuruluş biçimleri, bağlı oldukları idari yapılar ve görev alanlarının farklılık gösterdiği belirlenmiştir. Görüşmelerde ise veri yönetişimi faaliyetlerinin sınırlı personelle yürütüldüğü, veri sahipliği rollerinin yeni tanımlanmaya başlandığı ve koordinasyonun çoğunlukla bilgi işlem birimleri tarafından sağlandığı ifade edilmiştir. Bu bulgular, Türkiye'de veri yönetişiminin kurumsal düzeyde standartlaşmış bir yönetim modeli yerine parçalı uygulamalar üzerinden yürütüldüğünü göstermektedir.

Araştırma bulguları, veri yönetişiminin üniversitelerde üst yönetim tarafından sahiplenilmesi gereken stratejik bir yönetim yaklaşımı olduğunu göstermektedir.

Uluslararası üniversitelerdeki veri yönetişimi politika belgeleri incelendiğinde, veri yönetişiminin kurumsal stratejiyle ilişkilendirildiği, üst yönetimin politika onayı, kaynak tahsisi ve kurumsal önceliklerin belirlenmesinde aktif rol üstlendiği görülmektedir. Türkiye'deki üniversitelerle yapılan görüşmeler, veri yönetişimi birimlerinin çoğunlukla doğrudan rektörlük veya ilgili rektör yardımcılığına bağlı olarak yapılandırıldığını ortaya koymuştur. Bu durum, veri yönetişiminin kurumsal düzeyde stratejik bir yönetim fonksiyonu olarak algılandığını göstermektedir. Bununla birlikte veri yönetişimi faaliyetlerinin uzun dönemli stratejik planlama, performans yönetimi ve kurumsal hedeflerle sistematik biçimde ilişkilendirildiğine yönelik sınırlı bulgular elde edilmiştir. Bu ihtiyaç doğrultusunda geliştirilen modelin Stratejik Katmanı, veri stratejisi ve yol haritası, liderlik desteği, stratejik sahiplik, politika yönetimi, standartların belirlenmesi, karar yönetimi, risk ve uyum yönetimi ile izleme ve geri besleme bileşenlerinden oluşturulmuştur. Böylece araştırmada belirlenen stratejik sahiplenme ihtiyacının veri yönetişiminin kurumsal planlama ve performans sistemlerinin bir parçası haline gelmesi amaçlanmıştır.

Araştırmanın en belirgin bulgularından biri, veri yönetişimi yapılanmalarının üniversiteler arasında önemli farklılıklar göstermesidir. Uluslararası üniversitelerin incelenen politikalarda veri yönetişimi kurulları, veri sahipleri, veri sorumluları gibi görevler tanımlarıyla yapılandırılmıştır. Türkiye'deki üniversitelerin belge incelemelerinde ise koordinatörlük, uygulama ve araştırma merkezi ya da farklı idari yapılanmalar görülmektedir. Görüşmelerde veri yönetişimi faaliyetlerinin sınırlı personelle yürütüldüğü, birçok kurumda veri yöneticisi ve veri sorumlusu rollerinin yeni tanımlanmaya başladığı ifade edilmiştir. Ayrıca personel yetersizliği ve koordinasyon eksikliği veri yönetişiminin sürdürülebilirliğini zorlaştıran temel sorunlar arasında gösterilmiştir. Bu bulgular doğrultusunda geliştirilen modelde Yönetişim Katmanı, Veri Yönetişimi Kurulu, Veri Yönetişimi Ofisi, veri sahipleri, veri sorumluları, teknik veri sorumluları, domain liderleri ve veri kullanıcılarından oluşan çok katmanlı bir yönetim yapısı olarak tasarlanmıştır. Böylece veri yönetişimi teknik ve kurumsal düzeyde paylaşılan bir yönetim mekanizması haline getirilmiştir.

Uluslararası üniversitelerin politika metinleri, veri yönetişimini veri üretiminden veri imhasına kadar tanımlanmış süreçler üzerinden yürütüldüğünü göstermektedir. Politika

belgelerinde veri sınıflandırması, erişim, paylaşım, saklama, arşivleme ve imha faaliyetleri veri yaşam döngüsünün birbirini tamamlayan aşamaları olarak ele alınmaktadır. Görüşme verilerine göre, Türkiye'deki üniversitelerde ise bu süreçlerin Avesis yazılımı üzerinden gerçekleştirildiği anlaşılmıştır. Bu nedenle modelin Süreç Katmanı, veri yaşam döngüsü esas alınarak tasarlanmıştır. Veri üretimi, sınıflandırılması, doğrulanması, paylaşılması, depolanması, arşivlenmesi ve güvenli biçimde imha edilmesine ilişkin süreçler birbirini tamamlayan ve sürekli iyileştirmeye açık bir yapı içerisinde ele alınmıştır. Modelin bir diğer özgün yönü, uluslararası veri yönetişimi politikalarında politika geliştirmenin doğrusal bir süreç yerine döngüsel bir yaşam döngüsü olarak ele almasıdır. Bu yaklaşım, üniversitelerin dinamik yapısı ve değişen düzenleyici gereksinimler karşısında politikaların sürekli güncellenmesini mümkün kılmaktadır.

Politika metinlerine göre uluslararası üniversitelerde veri standartlarının, veri sözlüklerinin, üst veri kataloglarının, veri kalitesi uygulamalarının ve sistemler arası veri entegrasyonunun veri yönetişiminin temel bileşenleri olarak tanımlanmaktadır. Türkiye'deki üniversitelerdeki görüşme verilerine göre veri standartlarının yazılı olmayan şekilde belirlendiği ve veri sözlüğü, üst veri yönetimi, veri kalitesi ve entegrasyon uygulamalarının farkındalığının olduğu anlaşılmıştır. Bilgi İşlem Daire Başkanlığı ve Avesis iş birliğinde veri güvenliği uygulamalarında şifreleme, loglama ve erişim kontrolleri yürütülmektedir. Bu doğrultuda modelin Teknik Katmanı, veri mimarisi, veri modelleme ve tasarımı, veri entegrasyonu ve uyumluluk, veri kalitesi yönetimi, üst veri yönetimi, veri güvenliği, veri depolama ve operasyonlar ile veri ambarı ve iş zekası bileşenlerinden oluşturulmuştur. Bu yönüyle model, veri yönetişimini sadece BT birimlerinin sorumluluğu olarak ele alan geleneksel yaklaşımlardan ayrılmaktadır (Nielsen 2017; Panian 2010; Weber vd., 2009).

Uluslararası üniversitelerin bulguları literatürle benzer şekilde (Fattah, 2024) yükseköğretim kurumlarında veri yönetişiminin başarısının kurumsal kültüre de bağlı olduğunu göstermektedir. Görüşmelerde veri paylaşımı ve veri giriş süreçlerinin bazı çalışanlar tarafından ek iş yükü olarak algılanması, veri yönetişimi uygulamalarına yönelik kurumsal direncin önemli bir sorun alanı olduğunu ortaya koymuştur. Ayrıca Türkiye'deki üniversitelerde veri sahibi ve veri sorumlusu gibi rollerin resmî olarak

tanımlanması, veri sahipliği ve sorumluluklarının açık biçimde belirlenmesinin yönetim süreçlerinin etkinliği açısından kritik olduğunu göstermektedir. Bununla birlikte görüşme verileri, veri yönetişimi faaliyetlerinin büyük ölçüde raporlama odaklı yürütülmesi, verinin stratejik karar alma süreçlerinde daha etkin kullanılmasını destekleyecek kurumsal uygulamaların geliştirilmesine ihtiyaç bulunduğunu ortaya koymaktadır.

Literatürde veri yönetişimi çoğunlukla teknik kontrol, veri kalite yönetimi ve süreç standartlaşması ekseninde ele almaktadır (Abraham vd., 2019; DGI, t.y.; Khatri ve Brown, 2010; Leghemo vd., 2025; Legner vd., 2023; Otto, 2011; Weber vd., 2009). Bu bağlamda geliştirilen veri kültürü katmanının merkezi bir konumda yer alması önemli görülmektedir. Bu çalışmada veri kültürü, etik yönetim ve kurumsal farkındalık boyutları merkezi bir yapı olarak değerlendirilmiştir. Özellikle veri kültürünün stratejik yönetim mekanizmalarıyla ilişkilendirilmesi, modelin özgün yönlerinden biri olarak değerlendirilebilir.

Literatürde Kremser ve Brunauer (2019) tarafından ifade edildiği üzere veri odaklı kültür, veri kullanımını destekleyen kurumsal davranışların, normların ve yönetsel yaklaşımların bütünüdür. Bu çalışmada geliştirilen model de veri yönetişiminin sürdürülebilirliğini kurumsal kültür dönüşümü ile ilişkilendirmektedir.

Araştırmada geliştirilen modelin dikkat çekici yönlerinden biri, etik ve yasal uyum boyutunun veri yönetişiminin temel katmanlarından biri olarak ele alınmasıdır. Uluslararası üniversitelerin politika belgelerinde GDPR, FERPA ve HIPAA gibi düzenlemelere uyumun, veri sınıflandırmasına dayalı erişim kontrolü, rol temelli yetkilendirme, şifreleme, loglama, veri saklama ve güvenli imha uygulamalarıyla birlikte ele alındığı belirlenmiştir. Türkiye'deki üniversitelerle yapılan görüşmeler ve belge analizi sonucunda KVKK ve bilgi güvenliği ile ilgili düzenlemelere yer verdiği anlaşılmıştır. Etik veri kullanımı, veri sorumluluğu ve kurumsal uyum mekanizmalarının kurumlar arasında farklılık gösterdiği görülmüştür. Bu bulgular doğrultusunda geliştirilen modelde, kişisel verilerin korunması, veri güvenliği, veri erişim yetkileri, veri paylaşımı, veri saklama ve imha süreçleri ile veri kullanımına ilişkin etik sorumluluklar, Yasal ve Etik Katmanın temel bileşenleri olarak yapılandırılmıştır.

Araştırmanın uygulamaya yönelik özgün katkısı ise modelin yalnızca kavramsal bir çerçeve olarak bırakılmaması, uygulanabilirliğini desteklemek amacıyla altı aşamalı Veri Yönetişimi Eylem Planı ile birlikte sunulmasıdır. Kurumsal hazırlık ve üst yönetim sahipliğinden başlayarak mevcut durum analizi, politika ve standartların geliştirilmesi, pilot uygulama, kurum geneline yaygınlaştırma ile olgunluk değerlendirme ve sürekli iyileştirme aşamalarını içeren bu plan, modelin üniversitelerde adım adım hayata geçirilmesine yönelik somut bir yol haritası sunmaktadır. Bu yönüyle çalışma, bir veri yönetişimi modelinin nasıl olması gerektiğine ve uygulama aşamalarına cevap vermektedir. Modelin katmanlı yapısı, kurumların veri yönetişimi olgunluk düzeylerine göre aşamalı uygulama yapabilmesine olanak sağlamaktadır. Bu durum modelin uygulanabilirliğini artıran önemli unsurlardan biridir.

Bu araştırmanın bazı sınırlılıkları bulunmaktadır. Öncelikle geliştirilen model, belirli veri yönetişimi çerçeveleri ve yükseköğretim kurumlarının mevcut uygulamaları temel alınarak oluşturulmuştur. Bu nedenle modelin farklı sektörlerde doğrudan uygulanabilirliği sınırlı olabilir.

Önerilen model, Türkiye'deki üniversitelerin mevcut yapısı dikkate alınarak değerlendirilmiştir. Türkiye'deki üniversiteler genellikle merkezi yönetim yapısına sahip olmakla birlikte, fakülte ve bölümler düzeyinde belirli bir özerklik söz konusudur. Bu durum, modelde önerilen federatif veri yönetişimi yaklaşımı ile uyumlu olduğu için uygulanabilir bir çerçeve sunduğu düşünülmektedir.

Ayrıca modelin ampirik performansı uzun dönemli uygulama sonuçları üzerinden test edilmemiştir. Gelecek çalışmalarda modelin farklı üniversitelerde uygulanarak veri kalitesi, karar alma performansı ve kurumsal verimlilik üzerindeki etkilerinin ölçülmesi önerilmektedir.

Gelecek araştırmalarda geliştirilen veri yönetişimi modelinin farklı üniversite türlerinde uygulanması ve karşılaştırmalı analizlerle değerlendirilmesi önerilmektedir. Ayrıca veri yönetişimi olgunluk düzeyleri ile kurumsal performans arasındaki ilişkinin incelenmesi, alan yazına önemli katkılar sağlayabilir.

Bunun yanında yapay zeka yönetiřimi, büyük veri yönetimi ve etik veri kullanımı gibi yeni nesil veri yönetiřimi alanlarının modele entegre edilmesi gelecekteki çalışmalar açısından önemli bir araştırma alanı oluşturmaktadır.

Bununla birlikte, modelin uygulanmasında karşılaşılabilecek temel zorluklar arasında kurumsal direnç, veri kültürünün yetersizlięi ve teknik altyapı farklılıkları yer almaktadır. Bu nedenle modelin aşamalı bir yaklaşımla uygulanması önerilmektedir.

6. BÖLÜM

SONUÇ VE ÖNERİLER

6.1.SONUÇ

Bu araştırmada, Türkiye’deki üniversitelerde veri yönetişiminin mevcut durumu organizasyonel yapı, kurumsal kültür ve farkındalık, süreç ve teknik altyapı, politika ve standartlar ile engeller ve kapasite gereksinimleri bakımından araştırma sorularıyla incelenmiştir. Ulusal üniversitelerin bulguları, uluslararası üniversitelerin uygulamalarıyla birlikte değerlendirilerek Türkiye’deki üniversiteler için uygulanabilir bir veri yönetişimi modeli geliştirilmiştir. Araştırma sonuçları, Türkiye’deki üniversitelerde veri yönetişimi süreçleri daha görünür ve kurumsal bir niteliğe kavuşmuş olmasına karşın tam anlamıyla standartlaşmış ve olgunlaşmış bir yapıya ulaşamadığını göstermiştir.

Araştırmanın organizasyonel yapıya ilişkin sonuçları, veri yönetişimi birimlerinin kurumsal görünürlük kazanmasına rağmen yapı, yetki ve insan kaynağı bakımından üniversiteler arasında önemli farklılıklar bulunduğunu ortaya koymaktadır.

Araştırmada geliştirilen ilk araştırma sorusu “üniversitelerde veri yönetişimi süreçleri nasıl yapılandırılmıştır?” şeklindedir. Türkiye’deki üniversitelerde veri yönetişimi süreçleri kurumsal bir nitelik kazanmaya başlamıştır. Ancak henüz standartlaşmış ve olgunlaşmış ortak bir yapıya ulaşamamıştır. Üniversitelerde veri yönetişimi çoğunlukla koordinatörlük, ofis, uygulama ve araştırma merkezi gibi yapılar üzerinden yürütülmektedir. Bu yapılar genellikle rektörlüğe veya ilgili rektör yardımcılığına bağlı olarak konumlandırılmaktadır. Koordinatörlük ve ofislerin kurumsal verilerin merkezi ve bütüncül biçimde yönetilmesi, veri kalitesi ve bütünlüğünün sağlanması, raporlama ve performans izleme faaliyetlerinin yürütülmesi ve veriye dayalı karar alma süreçlerinin desteklenmesi amacıyla yapılandırıldığı anlaşılmaktadır. Araştırma merkezleri ise daha çok veri analizi, büyük veri, yapay zeka, danışmanlık ve Ar-Ge işlevleri etrafında şekillenmektedir.

Araştırmanın ikinci araştırma sorusu “veri yönetişiminden kimler sorumludur ve bu sorumluluklar hangi kurumsal yapılar üzerinden yürütülmektedir?” yanıt aranmıştır. Veri

yönetişiminden sorumlu rollerin tek ve standart bir kurumsal çerçevede toplanmadığı görülmektedir. Birçok üniversitede faaliyetler bir öğretim üyesinin yöneticiliğinde, sınırlı sayıda yönetici yardımcısı ve idari personelin desteğiyle yürütülmektedir. Bazı üniversitelerde veri yöneticisi, veri sorumlusu veya birim veri sorumlusu gibi roller tanımlanmaya başlanmış olmakla birlikte, bu rollerin çoğu kurumda ayrıntılı ve profesyonel bir görev mimarisi içinde düzenlenmediği anlaşılmaktadır. Veri yönetişimi sorumlulukları çoğu zaman mevcut personelin asli görevlerine ek olarak yerine getirilmektedir. Bu kapsamda, veri yönetişimi süreçlerinin kurumsal açıdan görünür hale gelmesine rağmen uzmanlaşmış insan kaynağı, yetki dağılımı, hesap verebilirlik ve rol netliği bakımından gelişim aşamasında olduğunu göstermektedir.

Üçüncü araştırma sorusu kapsamında “üniversitelerde veri yönetişimi kültürü hangi faktörlerden etkilenmektedir?” sorusu ele alınmıştır. Üniversitelerde veri yönetişimi kültürü üst yönetimin stratejik sahiplenmesi, etik sorumluluk anlayışı, eğitim ve farkındalık faaliyetleri, katılımcı yönetim mekanizmaları, hesap verebilirlik ve ortak bir veri dili oluşturma çabalarından etkilenmektedir. Verinin kurumsal bir varlık olarak tanımlanması, veriyle ilgili düzenlemelerin üst yönetim onayıyla ilişkilendirilmesi ve veri sözlüğü ile üst veri çalışmalarının yürütülmesi, veri yönetişimini teknik bir faaliyet olmaktan çıkararak kurumsal davranış ve değerler sisteminin bir parçası haline getirmektedir. Bununla birlikte, bu kültürün sürdürülebilir biçimde yerleşmesinde düzenli eğitim, farkındalık, iletişim ve hesap verebilirlik mekanizmalarının belirleyici olduğu anlaşılmaktadır. Bu bağlamda Türkiye’deki üniversitelerdeki veri yönetişimi kültürünün oluşabilmesi uzun zaman alacak gibi görünmektedir.

Araştırmanın dördüncü araştırma sorusunda “veri yönetişimi farkındalığı, kurumların karar alma ve yönetsel süreçlerine nasıl yansımaktadır?” konusu sorgulanmıştır. Veri yönetişimi farkındalığının karar alma ve yönetsel süreçlere yansımaları raporlama, performans izleme, akreditasyon, kalite güvencesi ve üst yönetime düzenli veri sunulması uygulamalarında görünür hale gelmektedir. Üniversitelerde veri yönetişiminin akademik performansın izlenmesi, stratejik göstergelerin takibi ve kurumsal kararların desteklenmesi için işlevsel bir araç olarak değerlendirildiğini göstermektedir. Haftalık, aylık veya dönemsel raporların hazırlanması, sonuçların üst yönetime sunulması ve verilerin akreditasyon süreçlerinde kullanılması, veri farkındalığının yönetsel düzeyde

karşılık bulduğunu göstermektedir. Ancak veri yönetişiminin raporlama ve performans takibiyle sınırlı kaldığı, verinin politika geliştirme, risk yönetimi, kaynak tahsisi ve ileriye dönük stratejik karar alma süreçlerindeki kullanımının henüz yeterince derinleşmediği anlaşılmaktadır.

Beşinci araştırma sorusunda “üniversitelerde veri toplama, saklama, erişim, paylaşım ve imha süreçleri nasıl yürütülmektedir?” sorusuna odaklanılmıştır. Üniversitelerde veri toplama, saklama, erişim, paylaşım ve imha süreçleri tek tip ve standart bir modele dayanmamaktadır. Veriler çoğunlukla AVESIS ve ilişkili bilgi sistemleri üzerinden toplanmaktadır. Veri girişleri farklı düzeylerde doğrulama işlemlerinden geçirilmektedir. Bazı üniversitelerde veriler, tanımlama, doğrulama, işleme, analiz, saklama, paylaşma, arşivleme ve imha aşamalarını içeren bir yaşam döngüsü yaklaşımıyla ele alınmaktadır. Erişim süreçlerinde rol tabanlı yetkilendirme uygulanmaktadır. Kullanıcıların unvan ve görevlerine göre farklı veri düzeylerine erişmesi sağlanmaktadır. Veri paylaşımı ise çoğunlukla görev tanımı, kurumsal ihtiyaç ve erişim yetkisi çerçevesinde gerçekleştirilmektedir. Saklama, arşivleme ve imha süreçlerine bazı yönerge ve uygulamalarda yer verilmesine karşın bu süreçlerin bütün üniversitelerde aynı ayrıntı düzeyinde tanımlanmadığı görülmektedir. Bu durum veri yönetişimi süreçlerinin bütüncül politika, standart ve denetim mekanizmalarıyla desteklenme düzeyinin sınırlı kaldığını ortaya koymaktadır.

Altıncı araştırma sorusu çerçevesinde “veri standardizasyonu, kalite güvencesi ve bütünlük sağlama konularında hangi zorluklar yaşanmaktadır?” sorusu incelenmiştir. Veri standardizasyonu, kalite güvencesi ve bütünlüğün sağlanmasında karşılaşılan başlıca zorluklar, ortak veri tanımlarının eksikliği, yazılı veri standartlarının sınırlılığı, veri sözlüğü çalışmalarının tamamlanmamış olması, veri sahipliği ve sorumluluklarının netleşmemesi ve aynı verinin farklı sistemlerde farklı biçimlerde tutulmasıdır. Üniversiteler doğruluk, bütünlük, güncellik, gizlilik ve erişilebilirlik gibi veri kalitesi boyutlarının önemini kabul etmekle birlikte, kalite kontrolleri çoğu zaman yazılı standartlar ve ölçülebilir göstergeler yerine uygulama içi kontroller ile insan denetimine dayanmaktadır. Bu kapsamda, veri kalitesinin sürdürülebilir ve ölçülebilir bir güvence sistemi içinde yönetilmesinden çok, kuruma veya sisteme özgü çözümlerle korunmaya çalışıldığını göstermektedir.

Yedinci araştırma sorusu olan “üniversitelerdeki bilgi sistemleri arasında veri entegrasyonu ne düzeydedir?” ile üniversitelerin teknik bütünleşme düzeyi değerlendirilmiştir. Üniversitelerde AVESIS, ATOSİS, APSİS ve kurum içinde geliştirilen farklı yazılımlar arasında entegrasyon ihtiyacı açık biçimde hissedilmektedir. Bazı kurumlar bu sistemleri ortak bir üst yapı altında birleştirmeye çalışsa da verilerin farklı sistemlerde dağınık biçimde bulunması, yinelenen veri girişlerine ve veri tutarsızlıklarına yol açmaktadır. Bu durum raporlama ile bütüncül analiz kapasitesini sınırlandırmaktadır. Bu nedenle entegrasyon düzeyi kısmi ve gelişmekte olan bir yapı sergilemektedir. Tam kurumsal bütünlük henüz birçok üniversitede sağlanamamaktadır.

Sekizinci araştırma sorusunda “üniversitelerde veri yönetişimine ilişkin tanımlı politika, standart veya yönergeler mevcut mudur?” sorusu üzerinden üniversitelerin yasal düzenleyicileri araştırılmıştır. Üniversitelerde veri yönetişimine ilişkin belirli bir düzenleyici çerçevenin oluşmaya başladığını ancak bu çerçevenin politika düzeyinde yaygın biçimde kurumsallaşmadığını göstermektedir. Bazı üniversitelerde yönerge veya yönetmeliklerle veri kalitesi, veri sözlüğü, veri haritası, standart oluşturma ve veri yönetişimi süreçleri tanımlanmış olsa da önemli bir bölümde resmî düzenleme bulunmamaktadır. Ayrıca politika belgesi düzeyinde açık ve veri yönetişimi çerçevesine sahip üniversite sayısı son derece sınırlıdır. Veri yönetişiminin çoğu kurumda uygulama düzeyinde ilerlediğini stratejik, ilkesel ve uzun vadeli yönlendirme araçlarının ise henüz yaygınlaşmadığını göstermektedir.

Dokuzuncu araştırma sorusu kapsamında “mevcut politikalar, uluslararası veri yönetişimi çerçeveleriyle hangi açılardan benzerlik veya farklılık göstermektedir?” sorusu karşılaştırmalı olarak ele alınmıştır. Türkiye’deki üniversitelerde veri sahipliği, veri kalitesi, veri yaşam döngüsü, erişim yetkileri, üst veri, veri sözlüğü, rol tabanlı sorumluluk ve veri güvenliği gibi alanların literatürde bulunan DGI ve DAMA gibi çerçevelerle kavramsal benzerlik taşımamaktadır. Bu değerlendirme, doğrudan çerçeve eşleştirmesinden çok bulgulara dayalı bir çıkarımdır. Uluslararası çerçevelerde öne çıkan sistematik politika yapısı, açık rol mimarisi, ölçülebilir standartlar, denetim mekanizmaları ve yönetim yaklaşımının Türkiye’deki üniversitelerde henüz parçalı ve uygulama ağırlıklı kaldığını da göstermektedir. Yani kavramsal düzeyde benzer unsurlar mevcut olmakla birlikte, uygulama olgunluğu ve kurumsal derinlik açısından belirgin sınırlılıklar vardır.

Araştırmanın onuncu sorusu olan “üniversitelerde veri güvenliği, gizlilik, etik kullanım ve paylaşım konularında hangi uygulamalar yürütülmektedir?” ile güvenlik, gizlilik, etik kullanım ve paylaşım uygulamalarının belirlenmesi amaçlanmıştır. Üniversitelerde veri güvenliği, gizlilik, etik kullanım ve paylaşım amacıyla rol tabanlı erişim, yetkilendirme, görev ve meşru amaçla sınırlı kullanım gibi uygulamaların yürütüldüğü görülmektedir. Bazı kurumlarda kişisel verilerden arındırılmış veri setlerinin araştırmacılara sunulması ve kullanıcıların yalnızca yetkileri kapsamındaki verilere erişebilmesi de dikkat çeken uygulamalardır. Buna rağmen, bu alanlarda yazılı standartların ve ayrıntılı iş akışlarının her kurumda aynı düzeyde gelişmemiş olması, güvenlik ve etik uygulamalarının kurumsal bütünlüğünü zayıflatmaktadır.

On birinci araştırma sorusunda “etkili bir veri yönetiřimi sisteminin oluřturulmasının önündeki başlıca engeller nelerdir?” sorusundan hareketle başlıca kurumsal engeller ortaya konulmuřtur. Etkili bir veri yönetiřimi sisteminin kurulmasının önündeki başlıca engeller; uzman insan kaynağı ve personel yetersizliğı, rollerin açık biçimde tanımlanmamıř olması, faaliyetlerin ek görev anlayıřıyla yürütölmesi, bağımsız bütçe eksikliğı, politika ve standartların sınırlılığı, bilgi sistemleri arasındaki entegrasyon sorunları ve veri standardizasyonundaki parçalı yapıdır. Ayrıca veri yönetiřiminin birçok kurumda stratejik bir yönetiřim alanından çok raporlama ve veri toplama işleviyle ilişkilendirilmesi, kurumsal derinliğı sınırlamaktadır. Belirlenen bu engeller, veri yönetiřiminin sürdüröllebilir, profesyonel ve kurum geneline yayılmış bir kapasiteye dönüşmesini güçleřtirmektedir.

On ikinci araştırma sorusu kapsamında “veri yönetiřimi süreçlerin geliştirilmesi için kurumlar hangi alanlarda kapasite geliřtirmeye ihtiyaç duymaktadır?” sorusu ele alınarak üniversitelerin kapasite gereksinimleri belirlenmiştir. Üniversitelerde etkili bir veri yönetiřimi sisteminin kurulmasının önündeki başlıca engeller uzman insan kaynağı eksikliğı, personel yetersizliğı, rollerin net tanımlanmamıř olması, veri yönetiřiminin çoğı zaman ek görev mantığıyla yürütölmesi, bağımsız bütçe eksikliğı, politika ve standartların sınırlılığı, sistemler arası entegrasyon sorunları ve veri standardizasyonundaki parçalı yapı olarak öne çıkmaktadır. Ayrıca veri yönetiřiminin birçok kurumda stratejik yönetiřim alanı olmaktan çok raporlama ve veri toplama işleviyle ilişkilendirilmesi, bu alandaki kurumsal derinliğı sınırlayan bir başka etkidir. Bu engeller, veri yönetiminin sürdüröllebilir, profesyonel ve kurum geneline yayılmış bir kapasiteye dönüşmesini zorlařtırmaktadır.

Araştırmanın on üçüncü ve son araştırma sorusunda “Türkiye'deki üniversiteler için nasıl bir veri yönetişimi modeli geliştirilebilir?” sorusuna yanıt aranmıştır. Uluslararası üniversiteler ile Türkiye'deki üniversitelerin uygulamaları karşılaştırıldığında, veri yönetişiminin küresel ölçekte giderek daha fazla politika temelli ve kurumsallaşmış bir yapıya kavuştuğu görülmektedir. Özellikle ABD üniversitelerinde stratejik sahiplik, açık rol tanımları, veri standartları, erişim mekanizmaları, güvenlik ve veri kültürünü bütünleştiren yapılara rastlanmaktadır. Birleşik Krallık ve Avustralya üniversitelerinde de benzer bileşenler bulunmakla birlikte uygulamaların kapsamı ve kurumsal olgunluğu farklılaşmaktadır. Türkiye'de ise yapı çoğunlukla operasyonel ve teknik düzeyde kalmaktadır. Standartlar ve süreçler sıklıkla yazılı politikalardan çok fiilî uygulamalar üzerinden yürütülmektedir. Veri yönetişimi farkındalığı artmasına rağmen yaklaşımın etik, hesap verebilirlik, şeffaflık ve veriye dayalı karar alma kültürüyle bütünleşmesi henüz tamamlanmamıştır.

Bu sonuçlar, Türkiye'deki üniversiteler için geliştirilebilecek modelin merkezi, katılımcı, standartlaştırılmış, kurumsal farklılıklara uyarlanabilir ve teknik boyutla birlikte stratejik, yönetsel, süreçsel, kültürel, yasal ve etik boyutları kapsayan katmanlı ve hibrit bir yapıya dayanması gerektiği sonucuna ulaşılmıştır. Modelde üst yönetim stratejik sahipliği üstlenmeli, Veri Yönetişimi Kurulu karar ve gözetim işlevini yürütmeli, rektörlük veya ilgili rektör yardımcılığına bağlı Veri Yönetişimi Ofisi kurumsal eşgüdümü sağlamalıdır. Akademik ve idari birimlerde veri sahipleri, veri alan liderleri, veri sorumluları ve veri kullanıcıları tanımlanmalıdır. Bu rollerin yetkileri, sorumlulukları, karar hakları ve hesap verebilirlik ilişkileri açıkça düzenlenmelidir.

Model, veri sahipliği, veri kalitesi, veri sınıflandırması, erişim yetkileri, veri paylaşımı, saklama ve imha, güvenlik, gizlilik ve etik kullanım alanlarını politika düzeyinde tanımlamalıdır. Veri sözlüğü, üst veri kataloğu, veri envanteri, veri kalite kuralları ve veri yaşam döngüsü yaklaşımı temel uygulama bileşenleri olmalıdır. Verinin tek merkezde toplanmasından çok üretildiği birimlerde tutulduğu, ancak politika ve standartlarla yönetildiği federatif yaklaşım, üniversitelerin çeşitlenen yapılarına uygun bir çözüm sunmaktadır. Böylece merkezi stratejik yönlendirme ile birim temelli sorumluluk arasında denge kurulabilir.

Önerilen modelin aşamalı biçimde uygulanması, mevcut durum ve olgunluk değerlendirmesiyle başlanmasını, politika ve rollerin tanımlanmasını, veri envanteri ile sözlük çalışmalarının tamamlanmasını, seçilmiş alanlarda pilot uygulamalar yürütülmesini ve sonuçların izleme, değerlendirme ve sürekli iyileştirme mekanizmalarıyla kurum geneline yaygınlaştırılmasını gerektirmektedir. Araştırma soruları kapsamında belirlenen parçalı organizasyon, rol belirsizliği, sınırlı veri kültürü, standart ve entegrasyon eksikliği, yetersiz politika altyapısı ve insan kaynağı sorunlarına bütüncül bir yanıt oluşturmaktadır. Araştırma sorularının birlikte değerlendirilmesi, Türkiye'deki üniversitelerin veri yönetişimi bakımından önemli bir dönüşüm sürecinde bulunduğunu, ancak uluslararası örneklere kıyasla erken bir olgunluk aşamasında olduğunu göstermektedir. Veri yönetişimi süreçlerinin dağınık, kısmen tanımsız ve kişisel inisiyatiflere bağlı yürütülmesi, veri bütünlüğü, erişim standartları ve güvenlik politikalarının kurumsallaşmasını zorlaştırmaktadır. Bu nedenle politika temelli yaklaşımın güçlendirilmesi, rol ve sorumlulukların netleştirilmesi, veri standartlarının kurumsallaştırılması, sistem entegrasyonunun geliştirilmesi, uzman insan kaynağının artırılması ve veri kültürünün kurum genelinde yaygınlaştırılması gerekmektedir. Araştırmanın önerdiği katmanlı veri yönetişimi modelinin söz konusu gereksinimleri stratejik, yönetişimsel, süreçsel, teknik, kültürel, yasal ve etik boyutları bir araya getirerek karşılaması düşünülmektedir.

6.2.ÖNERİLER

Elde edilen bulgular doğrultusunda Türkiye'deki üniversitelerde veri yönetişimi sistemlerinin geliştirilmesine yönelik aşağıdaki öneriler sunulmaktadır:

1. Politika Temelli Yönetişim Yaklaşımının Geliştirilmesi: Üniversitelerde veri yönetişimi faaliyetlerinin sürdürülebilir ve kurumsal bir yapıya kavuşabilmesi için, veri yönetişimi politikalarının oluşturulması kritik öneme sahiptir. Bu politikalar veri sahipliği, veri kalitesi, veri erişimi, güvenlik, etik kullanım ve veri yaşam döngüsü gibi temel alanları kapsayan bir çerçeve sunmalıdır. Politika belgeleri, yönerge ve yönetmeliklerle desteklenerek çok katmanlı bir düzenleyici yapı oluşturulmalıdır.

2. Organizasyonel Yapı ve Rol Tanımlarının Netleştirilmesi: Veri yönetişimi birimlerinin koordinasyon ve raporlama işleviyle sınırlı kalmaması, stratejik karar alma

süreçlerine entegre edilmesi gerekmektedir. Veri sahibi, veri sorumlusu, veri yöneticisi ve teknik veri sorumlusu gibi roller açık biçimde tanımlanmalıdır. Yetki ve sorumluluklar standartlaştırılmalıdır. Bu sayede hesap verebilirlik ve süreç yönetimi güçlendirilebilir.

3. Uzman İnsan Kaynağının Geliştirilmesi: Veri yönetiřimi, multidisipliner uzmanlık gerektiren bir alan olduėundan, üniversitelerde bu alanda uzman personel istihdamı artırılmalıdır. Veri bilimi, veri yönetimi ve bilgi güvenliėi alanlarında eğitim almıř profesyonellerin veri yönetiřimi birimlerinde görev alması sağlanmalıdır. Ayrıca mevcut personel için sürekli eğitim programları oluşturulmalıdır.

4. Veri Standartlarının Kurumsallařtırılması: Veri sınıflama, metadata yönetimi, veri kalitesi ve veri entegrasyonu gibi alanlarda yazılı ve standartlařtırılmıř uygulamalar geliřtirilmelidir. Kurumsal veri sözlüėü, veri katalogları ve ortak veri modelleri oluşturularak kurum genelinde ortak bir veri dili sağlanmalıdır. Bu standartların izlenmesi ve güncellenmesi için denetim mekanizmaları kurulmalıdır.

5. Veri Eriřimi ve Güvenlik Mekanizmalarının Güçlendirilmesi: Veri eriřimi ve paylařımı süreçleri rol temelli ve veri sınıflamasına dayalı olarak yeniden yapılandırılmalıdır. Yetkilendirme, loglama ve ihlal yönetimi süreçleri ayrıntılı biçimde tanımlanmalıdır. Ayrıca veri güvenliėi ve gizlilik uygulamaları yasal düzenlemelerle uyumlu şekilde güçlendirilmelidir.

6. Veri Kültürünün Yaygınlařtırılması: Veri yönetiřiminin bir kurum kültürü olduėu dikkate alınmalıdır. Bu doėrultuda veri temelli karar alma, etik veri kullanımı ve kurumsal sorumluluk bilincini artırmaya yönelik eğitim ve farkındalık programları yaygınlařtırılmalıdır. Üst yönetimin veri yönetiřimini sahiplenmesi ve bu kültürü teşvik etmesi kritik öneme sahiptir.

7. Entegrasyon ve Dijital Altyapının Geliřtirilmesi: Üniversitelerde farklı sistemler arasında veri entegrasyonunun sağlanması, veri yönetiřiminin etkinliėi açısından temel bir gerekliliktir. Veri ambarı, veri gölü ve entegrasyon platformları gibi teknolojik altyapılar geliřtirilmelidir. Veri akıřları merkezi olarak yönetilmelidir.

8. Performans Ölçümü ve Süreklilik Mekanizmalarının Oluřturulması: Veri yönetiřimi uygulamalarının etkinliėini deėerlendirmek için performans göstergeleri

belirlenmeli ve düzenli izleme mekanizmaları kurulmalıdır. Veri kalitesi, erişim süreleri, kullanıcı memnuniyeti ve uyum düzeyi gibi göstergeler üzerinden sürekli iyileştirme sağlanmalıdır.

KAYNAKÇA

- 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>
- Acceldata (2025, 25 Mart). *Data governance model: How leading companies ensure compliance and security*. 10 Mayıs 2025 tarihinde <https://www.acceldata.io/blog/data-governance-model-how-leading-companies-ensure-compliance-and-security> adresinden edinilmiştir.
- Ai, B., Li, Y., Ma, W., Qiu, M. ve Liu, M. (2023). Assessing the value of data assets: An exploratory study of valuation methods. *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* içinde (ss. 2147-2151). doi: 10.1109/TrustCom60117.2023.00299
- Aisyah, M. ve Ruldeviyani, Y. (2018). Designing data governance structure based on data management body of knowledge (DMBOK) framework: A case study on Indonesia deposit insurance corporation (IDIC). *International Conference on Advanced Computer Science and Information Systems (ICACSIS)* içinde (ss. 307-312). Yogyakarta, Indonesia. doi: 10.1109/ICACSIS.2018.8618151
- Alation. (2025, 29 Aralık). *Understand these data governance models: Centralized, decentralized, and federated*. 10 Ocak 2026 tarihinde <https://www.alation.com/blog/understand-data-governance-models-centralized-decentralized-federated/> adresinden edinilmiştir.
- 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>
- 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-Ruithe, M., Benkhelifa, E. ve Hameed, K. A (2019). A systematic literature review of data governance and cloud data governance. *Pers Ubiquit Computing*, 23, 839–859. <https://doi.org/10.1007/s00779-017-1104-3>
- Altexsoft (2023, 2 Mart). *Data governance: Concept, models, framework, tools, and implementation best practices*. 10 Mayıs 2025 tarihinde <https://www.altexsoft.com/blog/data-governance/> adresinden edinilmiştir.
- Askham, N. (2014). *Squaring the circle: Using a data governance framework to support data quality*. Experian white paper. Experian.
- Atlan. (2023, 19 Nisan). *Data governance model: Creating a sustainable framework for effective data management*. 10 Mayıs 2025 tarihinde <https://atlan.com/data-governance-model/> adresinden edinilmiştir.
- Australian Government. (2015, 7 Aralık). *Australian Government public data policy statement*. https://www.finance.gov.au/sites/default/files/2022-10/aust_govt_public_data_policy_statement.pdf

- Australian Government. (2025a, 19 Aralık). *Data governance framework*. <https://www.finance.gov.au/government/public-data/public-data-policy/data-governance-framework>
- Australian Government. (2025b, Mart). *Data strategy 2025–29: Smart data use informs good decisions*. Commonwealth of Australia. <https://www.infrastructure.gov.au/sites/default/files/documents/ditdrc-data-strategy-2025-2029.pdf>
- Bak, J. (2023, 25 Mart). *Big on data: Study shows why data-driven companies are more profitable than their peers*. Google Cloud. <https://cloud.google.com/blog/transform/data-leaders-more-profitable-innovative-hbr-data>
- Bena, Y. A., Ibrahim, R., Mahmood, J., Al-dhaqm, A., Alshammari, A., Nasser, M., Nura Yusuf, M., ve Ayemowa, M. O. (2025). Big data governance challenges arising from data generated by intelligent systems technologies: A systematic literature review. *IEEE Access*, 13, 12859-12888. <https://doi.org/10.1109/access.2025.3528941>
- Benfeldt, O. ve Persson, J.S. (2025). Semiotic mediation in data governance: Towards valuing data as assets. *Information and Organization*, 35(3), 100588. doi.org/10.1016/j.infoandorg.2025.100588
- Benfeldt, O., Persson, J.S. ve Madsen, S. (2020). Data governance as a collective action problem. *Information Systems Frontiers*, 22(2), 299-313. [10.1007/s10796-019-09923-z](https://doi.org/10.1007/s10796-019-09923-z)
- Bhansali, N. (2014). The role of data governance in an organization. N. Bhansali (Ed.). *Data governance: Creating value from information assets* içinde (s. 1-18). Taylor & Francis
- Braun, V., ve Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- British Academy ve Royal Society. (2017). *Data governance: Landscape review*. <https://royalsociety.org/~media/policy/projects/data-governance/data-governance-landscape-review.pdf>
- Brous, P., Herder, P. ve Janssen, M. (2016a). Governing asset management data infrastructures. *Procedia Computer Science*, 95, 303-310. <https://doi.org/10.1016/j.procs.2016.09.339>
- Brous, P., ve Janssen, M. (2020). Trusted decision-making: Data governance for creating trust in data science decision outcomes. *Administrative Sciences*, 10(4), 81.
- Brous, P., Janssen, M. ve Vilminko-Heikkinen, R. (2016b). Coordinating decision-making in data management activities: A systematic review of data governance principles. *5th International Conference on Electronic Government and the Information Systems Perspective (EGOV)*, Porto, Portugal, 115-125. <https://inria.hal.science/hal-01636460/document>
- Burchardi, K., Nath, D. ve Lan, J. (2024). *Federated data governance Model: Critical path for organization data maturity transformation journey*. BCG Platinion. <https://media-publications.bcg.com/Federated-Data-Governance-Model.pdf>
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

- Caballero, I., Gualo, F., Rodríguez, M. ve Piattini, M. (2023). A maturity model for data governance, data quality management, and data management. M. Naiouf, E. Rucci, F. Chichizola ve L. De Giusti (Ed.), *Cloud computing, big data & emerging topics* içinde. Springer. https://doi.org/10.1007/978-3-031-40942-4_12
- Castro-Edwards, J. (2025, 2 Temmuz). The UK's next data chapter: DUAA 2025 explained. *Arnold&Porter*. <https://www.arnoldporter.com/en/perspectives/advisories/2025/07/the-data-use-and-access-act-2025-explained>
- Chatterjee, S., Chaudhuri, R. ve Vrontis, D. (2021). Does data-driven culture impact innovation and performance of a firm? *An empirical examination. Annals of Operations Research*, 333(2-3), 601-626. <https://doi.org/10.1007/s10479-020-03887-z>
- Cheong, L. K. ve Chang, V. (2007). The need for data governance: A case study. *ACIS 2007 Proceedings*. 100. <http://aisel.aisnet.org/acis2007/100>
- Chen, R. (2021). *Mapping data governance legal frameworks around the world: Findings from the Global Data Regulation Diagnostic*. Policy Research Working Paper No. 9615). World Bank. <http://documents.worldbank.org/curated/en/581331617817680243>
- Chen, Y. C. (2017). *Managing digital governance: Issues, challenges, and solutions*. Routledge.
- Chukwurah, N., Ige, A. B., Idemudia, C. ve Adebayo, V. I. (2024). Strategies for engaging stakeholders in data governance: Building effective communication and collaboration. *Journal of Multidisciplinary Studies*, 08(01), 057–067. <https://doi.org/10.53022/oarjms.2024.8.1.0045>
- Claravine. (t.y.). *Data governance frameworks: The cornerstone of data-driven enterprises*. 10 Mayıs 2025 tarihinde <https://www.claravine.com/resources/data-governance-framework/#:~:text=3%20Types%20of%20Data%20Governance,centralized%2C%20decentralized%2C%20and%20hybrid.> adresinden edinilmiştir.
- Clarke, V. ve Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, 26(2), 120–123.
- Corban, T. (2021). Data as a Strategic Asset. *Strategic Finance*, 102(10), 60–61.
- DAMA. (2009). *The DAMA guide to the data management body of knowledge: (DAMA DMBOK Guide)*. Technics Publications, LLC., New Jersey.
- DAMA. (2013). *The six primary dimensions for data quality assessment: defining data. quality dimensions. DAMA UK Working Group white paper*. <https://www.sbctc.edu/resources/documents/colleges-staff/commissions-councils/dgc/data-quality-deminsions.pdf>
- DAMA. (2017). *DAMA-DMBOK: Data Management Body of Knowledge*. (2. basım). Technics Publication.
- Department for Digital, Culture, Media ve Sport. (2020). *UK National Data Strategy*. https://data.parliament.uk/DepositedPapers/Files/DEP2020-0521/UK_National_Data_Strategy.pdf
- Dismute, W.S. (2009). *Data governance: A study of the current state and emerging trends* [Yayınlanmamış yüksek lisans tezi]. University of Arkansas at Little Rock.

- Data Governance Institute (DGI). (t.y.). *DGI Data Governance Framework*. <https://datagovernance.com/the-dgi-data-governance-framework/>
- EDM Association. (2025). *Introducing DCAM® v3: The new era of best practices*. <https://edmcouncil.org/frameworks/dcam/>
- El Abed, W. ve Njonko, P. B. F. (2014). Governance of organizational data and information. Topi, H., ve Tucker, A. (Ed.), *Computing handbook* içinde (3. baskı). Chapman and Hall/CRC. <https://doi.org/10.1201/b16768>
- Eroğlu, Ş. (2025). Veri yönetişimi: Küresel uygulamalar çerçevesinde Türkiye’deki uygulamalara yönelik stratejik bir değerlendirme. *Bilgi Yönetimi Dergisi*, 8(1), 1- 24.
- Eryurek, E., Gilad, U., Lakshmanan, V., Kibunguchy-Grant, A. ve Ashdown, J. (2021). *Data governance: The definitive guide: People, processes, and tools to operationalize data trustworthiness*. O’Reilly Media
- European Commission. (2020a). *Data governance and data policies at the European Commission*. https://commission.europa.eu/system/files/2020-07/summary-data-governance-data-policies_en.pdf
- European Commission. (2020b). *Communication from the commission to the European Parliament, the council, the European economic and social committee and the committee of the regions: A European strategy for data*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>
- Farmer, D. (2024, 10 Eylül). *5 data governance framework examples*. TechTarget. <https://www.techtarget.com/searchdatamanagement/tip/5-data-governance-framework-examples>
- Fattah I. A. (2024). The mediating effect of data literacy competence in the relationship between data governance and data-driven culture. *Industrial Management & Data Systems*, 124(5), 1823–1845. doi: <https://doi.org/10.1108/IMDS-11-2023-0812>
- Federal CDO Council, CISO Council ve CIO.GOV. (2025). *Federal zero trust data security guide*. https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf
- Federal Data Strategy. (t.y.-a). *Data ethics framework*. <https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf>
- Federal Data Strategy. (t.y.-b). *Federal Data Strategy — Data, accountability, and transparency: creating a data strategy and infrastructure for the future* <https://strategy.data.gov/>
- Federal Data Strategy. (2020a). *Federal Data Strategy 2020 Action Plan*. <https://strategy.data.gov/assets/docs/2020-federal-data-strategy-action-plan.pdf>
- Federal Data Strategy. (2020b). *Data governance playbook*. <https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf>
- Federal Data Strategy. (2021). *Federal Data Strategy 2021 Action Plan*. <https://strategy.data.gov/assets/docs/2021-Federal-Data-Strategy-Action-Plan.pdf>

- Firican, G. (2020). *Stanford data governance maturity model*. 18 Şubat 2026 tarihinde <https://www.lightsondata.com/data-governance-maturity-models-stanford/> adresinden edinilmiştir.
- Fisher, T. (2009). *The data asset: How smart companies govern their data for business success*. John Wiley & Sons.
- Griffin, G. W ve Holcomb, D. (2023). *Building a data culture: The usage and flow data culture model*. Springer.
- Guest, G., MacQueen, K. M., ve Namey, E. E. (2012). *Applied thematic analysis*. Sage.
- Hanisch, M., Goldsby, C. M., Fabian, N. E. ve Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research*, 162, 113777. <https://doi.org/10.1016/j.jbusres.2023.113777>
- Hannila, H., Silvola, R., Harkonen, J., ve Haapasalo, H. (2019). Data-driven begins with DATA; potential of data assets. *Journal of Computer Information Systems*, 62(1), 29–38. <https://doi.org/10.1080/08874417.2019.1683782>
- Hennink, M., Hutter, I. ve Bailey, A. (2020). *Qualitative research methods*. SAGE Publications Limited.
- Hikmawati, S., Santosa, P.I. ve Hidayah, I. (2021). Improving data quality and data governance using master data management: A review. *IJITEE*, 5(3), 90-95.
- Hu, C., Li, Y., ve Zheng, X. (2022). Data assets, information uses, and operational efficiency. *Applied Economics*, 54(60), 6887–6900. <https://doi.org/10.1080/00036846.2022.2084021>
- Huff, E., ve Lee, J. (2020). Data as a strategic asset: Improving results through a systematic data governance framework. *SPE Latin American and Caribbean Petroleum Engineering Conference*. doi: <https://doi.org/10.2118/198950-MS>
- IBM. (2007). *IBM data governance maturity model: A roadmap*. 18 Şubat 2026 tarihinde <https://studylib.net/doc/8219376> adresinden edinilmiştir.
- Ige, A. B., Chukwurah, N., Idemudia, C., ve Adebayo, V. I. (2024). Ethical considerations in data governance: Balancing privacy, security, and transparency in data management. *Journal of Ethical Data Practices*, 20(7), 462-468.
- ISO. (2017). *Information technology — Governance of IT — Governance of data: Part 1: Application of ISO/IEC 38500 to the governance of data* (ISO Standard No. 38505-1:2017). <https://www.iso.org/standard/56639.html>
- ISO. (2018). *Information technology — Governance of IT — Governance of data: Part 2: Implications of ISO/IEC 38505-1 for data management* (ISO Standard No. 38505-2:2018). <https://www.iso.org/standard/70911.html>
- ISO. (2019). *Information technology — Metadata registries (MDR) Part 2: Classification* (ISO Standard No. 11179-2:2019). <https://www.iso.org/standard/74570.html>
- ISO. (2021). *Information technology — Governance of data: Part 3: Guidelines for data classification* (ISO Standard No. 38505-3:2021). <https://www.iso.org/standard/56639.html>

- ISO. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO Standard No. 27001:2022). <https://www.iso.org/standard/27001>
- ISO. (2023a). *Data quality: Part 51: Data governance: Exchange of data policy statements* (ISO Standard No. 8000-51:2023). <https://www.iso.org/standard/78708.html>
- ISO. (2023b). *Information technology — Metadata registries (MDR) Part 1: Framework* (ISO Standard No. 11179-1:2023). <https://www.iso.org/standard/78914.html>
- ISO. (2025a). *Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 5: Data quality governance framework* (ISO Standard No. 5259-5:2025). <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:5259:-5:ed-1:v1:en>
- ISO. (2025b). *Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance* (ISO Standard No. 27701:2025). <https://www.iso.org/standard/27701>
- ISO. (2025c). *Bilgi teknolojisi — Veri yönetiřimi — Veri iřbirlięi çerçevesi.* (ISO Standard No. 25642:2025). <https://www.iso.org/standard/90990.html>
- Jang, K. A. ve Kim, W. J. (2021). Development of data governance components using DEMATEL and content analysis. *Journal of Supercomputing*, 77(4), 3695–709.
- Janssen, M., Brous, P., Estevez, E., Barbosa, L. S. ve Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly*, 37(3), 101493. <https://doi.org/10.1016/j.giq.2020.101493>
- Jim, C. K. ve Chang, H. C. (2018). The current state of data governance in higher education. L. Freund (Ed.). *Proceedings of the Association for Information Science and Technology* içinde (s. 198-206). Wiley. <https://doi.org/10.1002/pr2.2018.14505501022>
- Jolliffe, D., Mahler, D.G., Veerappan, M., Kilic, T. ve Wollburg, P. (2021). *Under what conditions are data valuable for development?* (Policy Research Working Paper No. 9811). World Bank.
- Kansas State University. (2026). *Data governance*. 16 Mart 2026 tarihinde <https://www.k-state.edu/data/data-governance/> adresinden edinilmiřtir.
- Karkořková, S. (2023). Data governance model to enhance data quality in financial institutions. *Information systems management*, 40(1), 90-110. <https://doi.org/10.1080/10580530.2022.2042628>
- 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>
- Kirk, J., ve Miller, M. L. (1986). *Reliability and validity in qualitative research*. Sage Publications.
- King, N. (2004). Using templates in the thematic analysis of text. C. Cassell ve G. Symon (Ed.), *Essential guide to qualitative methods in organizational research* içinde (ss. 256–270). Sage Publications Ltd.
- Kirvan, P. (2025). *U.S. data privacy protection laws: 2026 guide*. <https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws>

- Klievink, B., Romijn, B.J., Cunningham, S. ve Bruijn, H. (2017). Big data in the public sector: Uncertainties and readiness. *Information Systems Frontiers*, 19, 267–283. <https://doi.org/10.1007/s10796-016-9686-2>
- Koltay, T. (2016). Data governance, data literacy and the management of data quality. *IFLA Journal*, 42(4), 303-312. <https://doi.org/10.1177/0340035216672238>
- Korhonen, J. J., Melleri, I., Hiekkänen, K. ve Helenius, M. (2013). Designing data governance structure: An organizational perspective. *GSTF Journal on Computing (JoC)*, 2(4), 11-17.
- Kotter, J. P. (2012). *Leading change*. Harvard Business Review Press.
- Kremser, W. ve Brunauer, R. (2019). Do we have a data culture? Haber, P., Lampoltshammer, T. Ve Mayr, M. (Ed.), *Data Science – Analytics and Applications*. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-27495-5_11.
- Kvale, S. (1996). *InterViews: An introduction to qualitative research interviewing*. Sage Publications.
- Kuzio J., Ahmadi M., Kim, K. C., Migaud, M. R., Wang, Y. F. ve Bullock, J. (2022). Building better global data governance. *Data & Policy*. 4(e25). doi:10.1017/dap.2022.17
- Leavy, P. (2014). *The Oxford handbook of qualitative research*. Oxford University Press.
- Ladley, J. (2020). *Data governance: How to design, deploy, and sustain an effective data governance program*. Elsevier
- Laney, D. B. (2017). *Infonomics. How to monetize, manage, and measure information as an asset for competitive advantage*. Bibliomotion
- 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 (Ed.), *Data Governance* içinde (ss. 99-119). Springer. https://doi.org/10.1007/978-3-031-43773-1_5
- Li, X., Cheng, Y. ve Möller, C. (2026). Data governance: a critical foundation for data driven decision-making in operations and supply chains. *Industrial Management & Data Systems*, 1–29. <https://doi.org/10.1108/IMDS-05-2025-0650>
- Lifebit (2025, 11 Temmuz). *Federated data governance explained simply (yes, really!)*. 10 Ocak 2026 tarihinde <https://lifebit.ai/blog/federated-data-governance/> adresinden edinilmiştir.
- Liu, Z. (2020). Practice research on university data center construction from the perspective of data governance. *2020 2nd International Conference on Information Technology and Computer Application (ITCA)* (ss. 489–492). doi: 10.1109/ITCA52113.2020.00108.
- Ma, J., Yang, X., ve Li, M. (2024). Are data assets useful? —Evidence based on corporate cost stickiness. *Emerging Markets Finance and Trade*, 60(15), 3734–3752. <https://doi.org/10.1080/1540496X.2024.2349655>

- Mahanti, R. (2019). *Data quality: Dimensions, measurement, strategy, management, and governance*. ASQ Quality Press.
- Marcucci, S., Alarcon, N. G. ve Verhulst, S. G. (2023). Informing the Global Data Future: Benchmarking Data Governance Frameworks. *Data & Policy*, 5, e30. doi:10.1017/dap.2023.24
- Micheli, M., Ponti, M., Craglia, M., ve Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2), 1-15. <https://doi.org/10.1177/2053951720948087>
- Miller, R., Whelan, H., Chrubasik, M., Whittaker, D., Duncan, P., ve Gregório, J. (2024). A framework for current and new data quality dimensions: An overview. *Data*, 9(12), 151. <https://doi.org/10.3390/data9120151>
- Nagle, T., Redman, T. ve Sammon, D. (2020). Assessing data quality: a managerial call to action. *Business Horizons*, 63(3), 325-337. <https://doi.org/10.1016/j.bushor.2020.01.006>
- NewVantage Partners. (2022). *Data and AI leadership executive survey 2022: Executive summary of findings: the quest to achieve data-driven leadership a progress report on the state of corporate data initiatives*. https://c6abb8db-514c-4f5b-b5a1-fc710f1e464e.filesusr.com/ugd/e5361a_2f859f3457f24cff9b2f8a2bf54f82b7.pdf
- 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>
- OECD. (2019). *Digital government review of Argentina: Accelerating the digitalisation of the public sector*. OECD Digital Government Studies, OECD Publishing.. <https://dx.doi.org/10.1787/354732cc-en>
- OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*. OECD Public Governance Policy Papers, No. 02, OECD Publishing. <http://dx.doi.org/10.1787/f64fed2a-en>
- OECD. (2022). *Going digital guide to data governance policy making*. OECD Publishing. <https://doi.org/10.1787/40d53904-en>
- Office of the National Data Commissioner. (2025). *National Data Commissioner Annual Report 2024–25*. <https://www.datacommissioner.gov.au/sites/default/files/2025-10/Annual%20Report%20of%20the%20National%20Data%20Commissioner%202024-2025.pdf>
- Oracle. (2011). *Enterprise Information Management: Best Practices in Data Governance. Oracle White Paper*. 18 Şubat 2026 tarihinde <https://www.oracle.com/assets/oca-best-practices-data-gov-1357848.pdf> adresinden edinilmiştir.
- Otto, B. (2011). A morphology of the organisation of data governance. *ECIS 2011 Proceedings*. 272. <http://aisel.aisnet.org/ecis2011/272>
- Panian, Z. (2010). Some practical experiences in data governance. *World Academy of Science, Engineering and Technology*, 62, 939–946.

- Plotkin, D. (2013). Data stewardship and data governance: how they fit together. *Data stewardship: An actionable guide to effective data management and data governance* içinde (ss. 1-21). <https://doi.org/10.1016/B978-0-12-410389-4.00001-5>
- 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). Bandung, Indonesia, 050002. <https://doi.org/10.1063/1.4941160>
- PwC. (2019). *Global and industry frameworks for data governance: Data Governance Knowledge Series - Topic 3 December 2019*. <https://www.pwc.in/assets/pdfs/consulting/technology/data-and-analytics/govern-your-data/insights/global-and-industry-frameworks-for-data-governance.pdf>
- Ridzuan, F. ve Zainon, M. N. (2024). A review on data quality dimensions for big data. *Procedia Computer Science*, 234, 341-348. <https://doi.org/10.1016/j.procs.2024.03.008>
- Salerno F. F. ve Maçada A. C. G. (2025). The effect of data governance on data-driven culture: The mediating effect of data quality. *The TQM Journal*. <https://doi.org/10.1108/TQM-08-2024-0304>
- Savona, M. (2026, 24 Şubat). *Data value and data governance*. Research Center for European Analysis and Policy. https://leap.luiss.it/wp-content/uploads/2026/02/WP3.26-Data-value-and-data-governance_FINAL.pdf
- SAS. (2018). *The SAS® Data governance framework: A blueprint for success*. SAS white paper. <https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/sas-data-governance-framework-107325.pdf>
- Schubert, K. D. ve Barrett, D. (2024). Data governance, privacy, and ethics. M. C. Lacity ve L. Coon (Ed.), *Human privacy in virtual and physical worlds: Technology, work and globalization* içinde (ss. 87–110). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-51063-2_5
- Sidi, F., Shariat Panahy, P. H. Affendey, L. S., Jabar, M. A., Ibrahim H. and Mustapha, A. (2012). Data quality: A survey of data quality dimensions. *2012 International Conference on Information Retrieval & Knowledge Management* (ss. 300-304). doi: 10.1109/InfRKM.2012.6204995.
- Smith, A. M., (2025, 15 Ekim). *Data governance framework: Key elements and examples*. Dataversity. 16 Şubat 2026 tarihinde <https://www.dataversity.net/articles/data-governance-frameworks/#key-elements-of-a-data-governance-framework> adresinden edinilmiştir.
- Smith, A. M., (2026, 15 Ocak). *Data governance maturity models and assessments: 2026 guide*. Dataversity. 16 Şubat 2026 tarihinde <https://www.dataversity.net/articles/understanding-data-governance-maturity-an-in-depth-exploration/> adresinden edinilmiştir.
- Stewart, C. J. ve Cash, W. B. (2017). *Interviewing: Principles and practices* (15. baskı). McGraw-Hill Education
- The European Parliament and of The Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and*

repealing Directive 95/46/EC (General Data Protection Regulation). <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

The European Parliament and of The Council. (2018). *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>

The European Parliament ve The Council Of The European Union. (2019). *Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024&qid=1772716573669>

The European Parliament ve The Council Of The European Union. (2022). *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*. <http://data.europa.eu/eli/reg/2022/868/oj>

The Office of Parliamentary Counsel. (2024). *Data availability and transparency act 2022*. https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/daata2022312/

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2021). *Ulusal Yapay Zeka Stratejisi 2021-2025*. <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>

United States Department Of Justice. (2002). *E-Government Act of 2002*. <https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

United States Department Of Justice. (2020). *Overview of The Privacy Act of 1974 (2020 Edition)*. <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>

UNDP (2021). *Digital strategy 2022-2025*. https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-Full-Document_ENG_Interactive.pdf

UNDP (2024). *Data governance framework: Recommendation report for Türkiye*. <https://www.undp.org/turkiye/publications/data-governance-framework-recommendation-report-turkiye>

UNESCO (2021, 23 Kasım). *Recommendation on the ethics of artificial intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

UNICC (2021). *UNDP data strategy – Microsoft and UNICC help accelerate delivery*. <https://www.unicc.org/news/2021/10/11/undp-data-strategy-microsoft-and-unicc-help-accelerate-delivery/>

University of Akron. (2026). *UA's data governance framework*. 15 Mart 2026 tarihinde <https://www.uakron.edu/datamanagement/governance/governance-framework> adresinden edinilmiştir.

University of Denver. (2025, 27 Şubat). *Data governance newsletter*. 15 Mart 2026 tarihinde <https://www.du.edu/data-governance/news/2025-february-newsletter> adresinden edinilmiştir.

- University of Maine Systems. (2017). Welcome to data governance! 15 Mart 2026 tarihinde <https://www.maine.edu/data-governance/> adresinden edinilmiştir.
- University of Oxford. (t.y.). *Data governance*. 15 Mart 2026 tarihinde <https://governance.admin.ox.ac.uk/data-governance> adresinden edinilmiştir.
- University of Tennessee. (2017). *Data central decision support resources for the UTK community: Data governance*. 15 Mart 2026 tarihinde <https://data.utk.edu/governance/> adresinden edinilmiştir.
- University of Wisconsin. (2023). *Data governance*. 15 Mart 2026 tarihinde <https://data.wisc.edu/data-governance/> adresinden edinilmiştir.
- U.S. Department of Labor. (2025). *Enterprise data strategy*. <https://www.dol.gov/sites/dolgov/files/Data-Governance/DOL-Enterprise-Data-Strategy.pdf>
- Verdi, U., Pinède, N. ve Melançon, G. (2024). La gouvernance des données en contexte universitaire: Proposition d'un modele de maturité. <https://hal.science/hal-04551264v1>
- Verhulst, S. G. (2021). Reimagining data responsibility: 10 new approaches toward a culture of trust in re-using data to address critical public needs. *Data & Policy*, 3, 1–11.
- 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>
- Webber, K. L. ve Zheng, H. Y. (2020). Data analytics and the imperatives for datainformed decision making in higher education. K. L. Webber ve H. Y. Zheng (Ed.), *Big data on campus: Data analytics and decision making in higher education* içinde (ss. 1–14). Johns Hopkins University Press.
- Wende, K. ve Otto, B. (2007). A contingency approach to data governance. M.A. Robert, R. O'Hare, M.L.Markus, ve B. Klein (Ed.) *Proceedings of 12th International Conference on Information Quality* içinde (ss. 163-176). <https://www.alexandria.unisg.ch/handle/20.500.14171/79975>
- Western University. (2026). Data governance framework. 15 Mart 2026 tarihinde <https://data.uwo.ca/governance/framework.html> adresinden edinilmiştir.
- Winks, E. (2023, 8 Mayıs). *Data Governance for higher educational institutions: Benefits, cautionary signs & roadmap*. Atlan. <https://atlan.com/data-governance-higher-education-institutions/>
- World Bank. (2020). *Data governance diagnostic tool*. <https://documents1.worldbank.org/curated/en/496191616486276525/pdf/Data-Governance-Diagnostic-Tool-MENA-Tech-Initiative.pdf>
- World Bank. (2021). *Data for better lives*. A World Bank Group Flagship Report. <https://www.worldbank.org/en/publication/wdr2021>
- World Economic Forum. (2021). *Articulating value from data. White paper: November 2021*. https://www3.weforum.org/docs/WEF_Articulating_Value_from_Data_2021.pdf

- Wu, Y. (2023). *Data governance in public sector: A study of U.S. municipal open data platforms* [Doktora tezi, University of Kansas].
- YÖK (2025). *2030'a doğru Türk yükseköğretiminin yol haritası*.
<https://www.yok.gov.tr/documents/documents/68e652769d934.pdf>
- Yıldırım, A. ve Şimşek, H. (2021). *Sosyal bilimlerde nitel araştırma yöntemleri* (12. baskı). Seçkin Yayıncılık

Bu referanslar APA7'ye göre düzenlenmiştir ve <https://libraryguides.vu.edu.au/apa-referencing/7SampleReferenceList> sayfasından alınmıştır.

EK1. ORJİNALLİK FORMU

	HACETTEPE ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ	Doküman Kodu Form No.	FRM-DR-21
	FRM-DR-21 Doktora Tezi Orijinallik Raporu <i>PhD Thesis Dissertation Originality Report</i>	Yayın Tarihi Date of Pub.	04.01.2023
		Revizyon No Rev. No.	02
		Revizyon Tarihi Rev. Date	25.01.2024

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI BAŞKANLIĞINA

Tarih: 27/08/2026

Tez Başlığı (Türkçe): Üniversitelerde Kurumsal Veri Yönetişimi Modelinin Geliştirilmesi
 Tez Başlığı (Almanca/Fransızca)*:.....

Yukarıda başlığı verilen tezin a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 195 sayfalık kısmına ilişkin, 27/08/2026 tarihinde şahsım/tez danışmanım tarafından Tuminin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezin benzerlik oranı % 4'tür.

Uygulanan filtrelemeler**:

- ☒ Kabul/Onay ve Bildirim sayfaları hariç
- ☒ Kaynakça hariç
- ☐ Alıntılar hariç
- ☒ Alıntılar dâhil
- ☒ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tezin herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Burcu TİĞ DEMİR

Öğrenci Bilgileri	Ad-Soyad	Burcu TİĞ DEMİR
	Öğrenim No	N20245543
	Enstitü Anabilim Dalı	Bilgi ve Belge Yönetim Anabilim Dalı
	Programı	Bilgi ve Belge Yönetim Bölümü
	Statüsü	Doktora ☒ Lisans Derecesi ile (Bütünleşik) Dr ☐

DANIŞMAN ONAYI

UYGUNDUR.
Prof. Dr. Özgür KÜLCÜ

*Tez **Almanca** veya **Fransızca** yazılıyor ise bu kısımda tez başlığı **Tez Yazım Dilinde** yazılmalıdır.

**Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları İkinci bölüm madde (4)/3'te de belirtildiği üzere: Kaynakça hariç, Alıntılar hariç/dâhil, 5 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit match size to 5 words) filtreleme yapılmalıdır.

	HACETTEPE ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ	Doküman Kodu Form No.	FRM-DR-21
		Yayın Tarihi Date of Pub.	04.01.2023
	FRM-DR-21 Doktora Tezi Orijinallik Raporu <i>PhD Thesis Dissertation Originality Report</i>	Revizyon No Rev. No.	02
		Revizyon Tarihi Rev. Date	25.01.2024

TO HACETTEPE UNIVERSITY GRADUATE SCHOOL OF SOCIAL SCIENCES DEPARTMENT OF INFORMATION MANAGEMENT		Date: 27/08/2026
Thesis Title (In English): Development of Institutional Data Governance Model in Universities		
According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 27/08/2026 for the total of 205 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled above, the similarity index of my thesis is 4%.		
Filtering options applied**:		
1. ☒ Approval and Declaration sections excluded		
2. ☒ References cited excluded		
3. ☐ Quotes excluded		
4. ☒ Quotes included		
5. ☒ Match size up to 5 words excluded		
I hereby declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.		
I respectfully submit this for approval.		
Burcu TİĞ DEMİR		

Student Information	Name-Surname	Burcu TİĞ DEMİR	
	Student Number	N20245543	
	Department	Information Management	
	Programme	Information Management	
	Status	PhD ☒	Combined MA/M Sc-PhD ☐

SUPERVISOR'S APPROVAL

APPROVED
Prof. Dr. Özgür KÜLCÜ

**As mentioned in the second part (article (4)/3) of the Thesis Dissertation Originality Report's Codes of Practice of Hacettepe University Graduate School of Social Sciences, filtering should be done as following: excluding reference, quotation excluded/included, Match size up to 5 words excluded.

EK 2. ETİK KURUL İZNİ

Tarih: 23/07/2024 16:40
Sıra: E-66777242-300-00003671817



00003671817



HACETTEPE ÜNİVERSİTESİ SOSYAL VE BEŞERİ BİLİMLER ARAŞTIRMA ETİK KURULU

<u>TOPLANTI TARİHİ</u>	<u>TOPLANTI SAYISI</u>
23 Temmuz 2024	2024/13

İlgi : 18.07.2024 tarihli ve E-12908312-300-00003656506 sayılı yazınız.

Enstitünüz Bilgi ve Belge Yönetimi Anabilim Dalı Doktora Programı öğrencilerinden **Burcu Tığ DEMİR**'in, **Prof. Dr. Özgür KÜLCÜ** danışmanlığında yürüteceği "*Üniversitelerde Kurumsal Veri Yönetimi Politikalarının Geliştirilmesi*" başlıklı tez çalışması Üniversitemiz Sosyal ve Beşeri Bilimler Araştırma Etik Kurulunun **23 Temmuz 2024** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan **uygun** bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. İsmet KOÇ
Kurul Başkanı

EK 3. ÜNİVERSİTELERDE KURUMSAL VERİ YÖNETİMİ POLİTİKALARININ GELİŞTİRİLMESİ GÖNÜLLÜ KATILIM FORMU VE GÖRÜŞME SORULARI

Gönüllü Katılım Formu

Sayın Katılımcı:

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Ana Bilim Dalında “Üniversitelerde Kurumsal Veri Yönetimi Politikalarının Geliştirilmesi” adlı bir doktora tezi hazırlıyorum (Danışman: Prof. Dr. Özgür Külcü). Bu araştırmada, Türkiye’deki üniversitelerin veri yönetimi konusundaki durumunu tespit etmek, karşılaştıkları problemlere çözüm önerileri sunmak ve veri yönetimi politikası modeli geliştirmek amaçlanmaktadır. Bu kapsamda veri yönetimi birimi olan üniversitelerle veri yönetimi konusunda ne noktada olduklarını belirlemek amacıyla durum tespiti, veri yönetimi konusundaki karşılaştıkları problemlere yönelik yarı yapılandırılmış görüşmeler yapılacaktır. Görüşme sorularından elde edilen veriler, sadece doktora tez çalışması kapsamında kullanılacaktır. Bu araştırma için Hacettepe Üniversitesi Sosyal ve Beşerî Bilimler Araştırma Etik Kurulundan gerekli izinler alınmıştır.

Görüşmede veri yönetimine yönelik 12 soru sorulacaktır. Görüşmenin yaklaşık 45 dakika sürmesi beklenmektedir. Araştırmaya katılım gönüllülük esasına dayanmaktadır. Kişisel verileriniz ve sorulara vereceğiniz cevaplar kimseyle paylaşılmayacak, sadece araştırma amacıyla kullanılacaktır. Araştırmaya katılmaktan istediğiniz zaman hiçbir sorumluluk getirmeden vazgeçebilirsiniz.

Araştırmaya katılmayı kabul ettiğiniz için şimdiden teşekkür ederim. Görüşme bittikten sonra bana sormak istediğiniz sorular varsa olursa telefon numarası ya da burcutigdemir@hacettepe.edu.tr adresinden benimle iletişime geçebilirsiniz.

İzin verirseniz sadece araştırma amacıyla kullanılmak üzere görüşme kayıt altına alınacaktır. Araştırmaya katılmayı kabul ediyorsanız lütfen aşağıdaki alanı doldurarak imzanızı atınız.

Tarih:

Katılımcının:

Adı Soyadı:

Adres:

Telefon:

İmza:

Araştırmacı:

Adı Soyadı: Arş. Gör. Burcu TIĞ DEMİR

Adres: H.Ü. Bilgi ve Belge Yönetimi Bölümü

Görüşme Soruları

1. Üniversitenizdeki veri yönetimi birimi teşkilatlanması hakkında bilgi verebilir misiniz? Birimde kaç kişi çalışmaktasınız? Görev tanımlarınız nelerdir? Üniversitede veri yönetimi uzmanı var mıdır? Hangi yapıya bağlısınız? Biriminize ait bütçeniz var mıdır? Veri yönetimine yönelik danışma kurulunuz var mıdır? Veri yönetimi için geliştirdiğiniz ya da geliştirmeyi planladığınız program, düzenleme, strateji ya da politika var mıdır? Veri yönetimi çalışmalarınızı rapor ettiğiniz herhangi bir yapılanma var mıdır?

2. Sizce üniversiteniz personelleri veri yönetimi konusunda eğitime ve farkındalığa ihtiyaç duymakta mıdır? Veri yönetimi ile ilgili hem birim içindeki hem de birim dışındaki eğitim faaliyetleri konusundaki düşüncelerinizi paylaşabilir misiniz?

3. *Yurt dışı üniversiteler incelendiğinde üniversite verilerinin şu şekilde sınıflandığı karşımıza çıkmıştır. Kamu verisi (public data), dahili veri (internal data), özel veri (private data), kısıtlanmış veri (restricted data) gibi verilerden oluşabilir.*

Kamu verisi: Erişim veya yönetim kısıtlaması olmayan, kamu kullanımına yönelik kurumsal veriler.

Dahili veri: Üniversitenin iş ve operasyonlarını yürütmek için kullanılan kurumsal veriler. Aksi belirtilmediği sürece dahili, kurumsal veriler için varsayılan düzeydir.

Özel veri: Yasal, düzenleyici, idari veya sözleşmeye bağlı gereklilikler nedeniyle özel olarak sınıflandırılan kurumsal veriler; fikri mülkiyet veya etik hususlar, stratejik veya özel değer; ve/veya bu tür verilerin diğer özel yönetimi.

Kısıtlanmış: Yasal, düzenleyici, idari, sözleşmeye bağlı, kural veya politika gereklilikleri nedeniyle en üst düzeyde koruma gerektiren kurumsal veriler.

Belirtilen sınıflamalar hakkındaki düşünceleriniz nelerdir? Sizce verileri sınıflandırılmaya ihtiyacı var mıdır? Üniversitenizde veri yönetimi esnasında bu şekilde bir sınıflandırma yapılandırmasının sizce ne gibi faydaları ya da zararları olabilir? Üniversitenizdeki verilerin sınıflandırılması çalışmaları hakkında ne düşünmektesiniz?

4. Üniversitelerde verilerin değer yaratabilmesi için kapsamlı (eksiksiz, sürekli ve güncel), yüksek kalitede (doğru, karşılaştırılabilir ve ayrıntılı), kullanımı kolay (erişilebilir, anlaşılır ve birlikte çalışabilir) ve güvenli (tarafsız, gizli ve uygun) olması veri kalitesi ile ilgilidir. Veri kalitesi üniversitelerdeki bilgi ihtiyacı ve gereksinimleri karşılayan **nitelikli veriler** olarak değerlendirilmektedir. **Veri kalitesinin temeli üst verilere**¹⁵³ dayanmaktadır. **Üst veriler** doğru tanımlandığında veriye **erişim** sağlanmaktadır. Veri kalitesinin belirli **standartlarda** olmaması, **veri yaşam döngüsü** olarak adlandırılan, verinin üretimi, düzenlenmesi, erişimi, kullanımı, ayıklanması, saklanması ve yeniden kullanılması aşamalarında problemlere yol açmaktadır.

Yukarıdaki metin kapsamında üniversiteniz tarafından veri kalitesi geliştirmeye yönelik gerçekleştirilen ya da gerçekleştirilecek çalışmaları nasıl bulmaktasınız? Metinde bahsedilene benzer bir problemle karşı karşıya kaldıysanız bizimle paylaşabilir misiniz?

5. Üniversitelerin iş süreçleri kapsamında üretilen **kurumsal veriler**, (institutional data) yönetilmesi ve korunması gereken önemli varlıklar olarak tanımlanır. Üniversite çalışanlarının iş süreçlerindeki veri ihtiyaçlarını ve veri akışını sağlayabilmek amacıyla **veri mimarisi ilkeleri** geliştirilir. Veri mimarisi ilkeleri geliştirilirken üniversitelerin **mantıksal ve fiziksel veri varlıklarını** tanımlayıcı ve veri yönetimi yapısını belirleyici nitelikte olmasına dikkat edilmektedir. Veri mimarisi, üniversite verilerinin varlık, hacim, çeşitlilik, hız, doğruluk ve değer gibi açılardan ele alan araç ve tekniklerden oluşmaktadır. Veri mimarisi, toplu verilerin toplanması, depolanması, işlenmesi, entegrasyonu, dönüşümü, analizi, görselleştirmesi, güvenliği ve gizliliği ile ilgili adımları yöneten standart, kural ya da modeldir.

Üniversitenizdeki verilerin toplanması, depolanması, işlenmesi, entegrasyonu, dönüşümü, analizi, görselleştirmesi, güvenliği ve gizliliği adımlarını gerçekleştirebilmek için yaptığınız çalışmalardan bahsedebilir misiniz?

6. Veri katalogları veri sözlükleri veri mimarisinin oluşmasını sağlamaktadır. Verileri varlık olarak tanımlayan ve gerçek hayattaki ilişkilerini kurmayı sağlayan araçlardır.

Veri kataloğu: Veri kataloğu, bir üniversitenin topladığı ve işlediği tüm verilerin envanteridir. Yasal gereklilikler, üniversitelerin veri toplamadan veri tüketim sürecine kadar daima veri güvenliğini sağlamasını ve verileri korumasını sağlamaktadır. Varlık adı, varlık türü, varlık açıklaması, öznitelik/sütun adları, öznitelik/sütun veri türleri, öznitelik/sütun açıklaması gibi bilgileri tanımlamaktadır.

¹⁵³ Örneğin bir kitabın üst verisi başlık, yazar, yayın tarihi, ISBN numarası ve konusunu kapsayabilir.

Veri sözlüğü: Verinin tanımı, farklı veri türleriyle olan ilişkisini, kökeni, kullanımı ve biçimine göre sınıflandırmaya yarayan bir gösterimdir. Örneğin tablo adı PERSON, T_KISI karşılığında veri sözlüğünde yer alacak olan kavram “Kişi” veri kümesidir.

Sizce üniversitenizde veri yönetimi için veri kataloğu ve veri sözlüğü gerekli midir? Üniversitenizin geliştirmiş olduğunuz veri kataloğu veya veri sözlüğü bulunmakta mıdır? Konu hakkındaki görüşleriniz nelerdir?

ÖRNEK:**Bilgi paylaşım şartları**

MADDE 6- (1) İş bu Protokol kapsamında bilgilerin paylaşımı aşağıda yer alan esaslar dahilinde gerçekleştirilir.

- a) Taraflar web servisi ile bu Protokol kapsamında belirlenen verilere erişim sağlayacaktır.
- b) Belirlenen web servise bağlanacak olan sunucuların dış IP adreslerini taraflar birbirlerine bildireceklerdir.
- c) Oluşturulacak web servise bildirilen IP'ler ve sınırlandırılmış SSL güvenlik sertifikası ile KamuNet ortamında erişim sağlanacaktır.
- ç) Taraflar, veri erişim ve paylaşımının doğru, hızlı, kesintisiz ve güvenli olarak sağlanması için gerekli tedbirleri alacak ve gerekli yatırımları yapacaktır.

7. Yukarıda örneği sunulan “Bilgi Paylaşım Şartları” konusundaki görüşleriniz nelerdir? Üniversitenizde veri paylaşımı ve erişimine yönelik geliştirilen veya geliştirilmesi düşünülen bir çalışma varsa bizimle paylaşabilir misiniz?

8. Kurumsal verilere erişim, bu verileri kullanma, ifşa etme veya oluşturma izni, veri kullanıcılarına yalnızca meşru üniversite amaçları doğrultusunda verilmektedir. Veri kullanıcıları rollerine, üniversitenin politikaları ve yasal gereklilikleri esas alınarak **yetkilendirme** yapılmaktadır.

Üniversitenizde yukarıdaki ifadeye benzer bir yetkilendirme çalışması hakkındaki düşüncelerinizi bizimle paylaşabilir misiniz? Sizce veri kullanıcıları rollerine dair yetkilendirme üniversite içindeki veri yönetimi çalışmaları nasıl etkiler?

ÖRNEK:**Gizlilik ve güvenlik**

MADDE 7- (1) İşbu Protokol kapsamında edinilen bilgilerin gizliliğinin ve güvenliğinin sağlanması veriye erişim sağlayan tarafın sorumluluğundadır. Buna göre;

- a) Protokol kapsamında elde edilen verilerin gizliliği ve güvenliği ile verilerin kullanılmasının hukuki sonuçlarından (hukuki, cezai, idari, mali) veriye erişim sağlayan taraf sorumludur. Veriye erişimi sağlanan taraf kendi sistemine transfer ettiği bilgileri, amacı çerçevesinde kullanacak, bilgilerin mahremiyetini korumak için gerekli tedbirleri alarak gizli tutulmasını sağlayacaktır.
- b) Taraflar elde ettiği bilgileri kendi sistemlerindeki diğer bilgiler ile bütünleştirebilir. Görev ve sorumlulukları ile yerine getirmesi gereken yükümlülüklerin ifası için kullanabilirler.
- c) Erişim için verilen kullanıcı adı ve parolaların gizliliğinden, ilgili taraf sorumludur.

9. Yukarıda örnek metni paylaşılan verilerin gizliliği, güvenliği ve mahremiyeti konularındaki düşüncelerinizi bizimle paylaşabilir misiniz? Üniversitenizde bu konularla ilgili yapılmış ya da yapılması düşünülen çalışmalardan bahsetmeniz mümkün müdür?

10. Üniversitenizde üretilen verilerin korunması ve saklanması konusundaki düşünceleriniz nelerdir? Sizce verilerin korunması ve saklanması konusunda özellikle dikkat edilmesi gereken noktalara dair tecrübelerinizi paylaşabilir misiniz?

11. Sizce üniversitenizdeki verilerin üretimi, erişimi, kullanımı, saklanması, paylaşımı, bütünlüğü ve imhası aşamaları için ne gibi düzenlemeler yapılabilir? Veri yönetimi politikası ile bu aşamalarda yaşanan problemlerin çözüme kavuşacağını düşünüyor musunuz? Sizce kurumsal veri yönetimi politikası yapılandırabilmek için hangi adımları izlemek daha doğru olabilir?

12. Üniversiteniz ya da diğer kamu/özel kurum ve kuruluşlarındaki veri yönetimi ile ilişkili yasal düzenlemeleri nasıl buluyor musunuz? Bizim için genel bir değerlendirme yapabilir misiniz?

EK 4. VERİ YÖNETİŞİMİ DÜZENLEMESİ OLAN ULUSAL ÜNİVERSİTELER

No	Üniversite / Kurum	Belge Türü	Belge Adı
1	Ankara Üniversitesi	Yönerge	Kurumsal Veri Yönetimi Koordinatörlüğü Yönergesi
2	Dokuz Eylül Üniversitesi	Yönerge	Kurumsal Veri Yönetim Koordinatörlüğü Çalışma Yönergesi
3	Erciyes Üniversitesi	Yönerge	Kurumsal Veri Yönetimi ve Analitiği Koordinatörlüğü Yönergesi
4	Fatih Sultan Mehmet Vakıf Üniversitesi	Yönetmelik	Yapay Zeka ve Veri Bilimi Uygulama ve Araştırma Merkezi Yönetmeliği
5	Gazi Üniversitesi	Yönerge	Kurumsal Veri Yönetimi Koordinatörlüğü Yönergesi
6	Hacettepe Üniversitesi	Politika	Kurumsal Veri Yönetişimi Politikası
7	Isparta Uygulamalı Bilimler Üniversitesi	Yönetmelik	Veri Yönetimi Uygulama ve Araştırma Merkezi Yönetmeliği
8	İstanbul Üniversitesi-Cerrahpaşa	Yönerge	Kurumsal Veri Yönetim Ofisi Yönergesi
9	İzmir Kâtip Çelebi Üniversitesi	Yönetmelik	Yapay Zeka ve Veri Bilimi Uygulama ve Araştırma Merkezi Yönetmeliği
10	Osmaniye Korkut Ata Üniversitesi	Yönetmelik	Veri Analizi Uygulama ve Araştırma Merkezi Yönetmeliği
11	Pamukkale Üniversitesi	Yönetmelik	Kalite Yönetimi ve Veri Değerlendirme Uygulama ve Araştırma Merkezi Yönetmeliği
12	Sakarya Uygulamalı Bilimler Üniversitesi	Yönetmelik	Yapay Zeka ve Veri Bilimi Uygulama ve Araştırma Merkezi Yönetmeliği
13	Trabzon Üniversitesi	Yönerge	Büyük Veri ve Yapay Zeka Koordinatörlüğü Yönergesi
14	Üsküdar Üniversitesi	Yönetmelik	Veri Analizi Uygulama ve Araştırma Merkezi Yönetmeliği
15	Zonguldak Bülent Ecevit Üniversitesi	Yönerge	Dijital Veri Yönetim Koordinatörlüğü Yönergesi

EK 5. ULUSLARARASI ÜNİVERSİTELERİN VERİ YÖNETİŞİMİ POLİTİKALARINA DAİR BİLGİLER

No	Üniversitenin Adı	Politikanın Adı	Ülke	Yılı
1	Adelphi University	Research and Data Management Procedure	ABD	2017
2	Alabama A&M University	Data, Information Access, and Security Policy	ABD	2024
3	Andrews University	Data Governance Policy	ABD	2021
4	Antioch University	Data Governance Policy	ABD	2024
5	Appalachian State University	Data Governance Policy	ABD	2020
6	Arcadia University	Data Governance Policy	ABD	2021
7	Athens State University	Data Governance Policy	ABD	2023
8	Augusta University	Data Management and Classification Policy	ABD	2021
9	Australian Catholic University	Data and Information Governance Policy	Avustralya	2024
10	Australian National University	Data Governance Policy	Avustralya	2022
11	Baldwin Wallace University	Data Governance Policy	ABD	2024
12	Bates College	Data Governance Policy	ABD	2017
13	Binghamton University	Data Governance Policy	ABD	2023
14	Boise State University	Data Governance Policy	ABD	2022
15	Brandeis University	Data Governance Policy	ABD	2021
16	Bucknell University	Data Classification and Management	ABD	2018
17	California State University, Fullerton	Data Governance Guidelines	ABD	
18	California Health Sciences University	Data Governance Policy	ABD	2024
19	Cardiff Metropolitan University	Data Management and Governance Policy	BK	2024
20	Central Michigan University	Data Stewardship Policy	ABD	2019
21	Cleveland State University	Administrative Data Policy	ABD	2015
22	Colorado State University	Central Administrative Data Governance	ABD	2018
23	Columbia International University	Data Governance Policy	ABD	2023
24	Concord University	Data Governance, Accessibility & Classification Policy	ABD	2024
25	Concordia University	Policy On Data Governance	ABD	2020
26	Connecticut College	Data Governance Policy	ABD	2019
27	Cornell University	Data Stewardship and Custodianship Policy	ABD	2018
28	Danville Area Community College	Data Governance Policy	ABD	2019
29	Drake University	Stewardship And Custodianship of Institutional Data Policy	ABD	2014
30	Duquesne University	Data Governance Service Requirements	ABD	2024
31	East Stroudsburg University	Data Governance Charter	ABD	2023
32	Edmonds College	Data Governance Policy	ABD	2024
33	Emerson College	Data Governance Policy	ABD	2020
34	Florida International University	Data Stewardship Policy	ABD	2024
35	George Mason University	Data Stewardship Policy	ABD	2024
36	Georgia State University	Data Governance Policy	ABD	2023
37	Griffith University	Data Governance and Management Protocol	Avustralya	2024

38	Grand Valley State University	University Data Management Policy	ABD	2022
39	Harris–Stowe State University	Data Governance Policy	ABD	2024
40	Haverford College	Data Governance and Management Policy	ABD	2024
41	Hudson County Community College	Institutional Data Governance Policy	ABD	2023
42	Indiana State University	Data Security and Management	ABD	2022
43	Indiana University	Standards for Management of Institutional Data	ABD	2020
44	James Cook University	Data Governance Policy	Avustralya	2022
45	John Carroll University	Data Governance Charter	ABD	2019
46	Kansas State University	Institutional Data Policy	ABD	2024
47	King's College	Data Governance Policy	ABD	2024
48	Lamar University	Data Governance Policy	ABD	2024
49	La Trobe University	Data Governance Policy	Avustralya	
50	Limestone University	Data Governance Policy	ABD	2024
51	Lower Columbia College	Data Governance Policy	ABD	2022
52	Louisiana State University	Data Governance Committee Charter	ABD	2024
53	Loyola University	Data Governance Structure Proposal	ABD	2024
54	Lynn University	Data Classification and Data Governance Policy	ABD	2021
55	Michigan State University	Institutional Data Policy	ABD	2017
56	Middle Georgia State University	Data Governance Policy	ABD	2020
57	Minnesota State University	Enterprise Data Governance	ABD	2018
58	Montana State University	Enterprise Data Stewardship Policy	ABD	2020
59	Montana State University	Data Stewardship Standards	ABD	2023
60	New Mexico State University	Data Governance Policy	ABD	2020
61	New South Wales College	Data Governance Policy	Avustralya	2023
62	New York University	Administrative Data Management Policy	ABD	2024
63	Northeastern Illinois University	Data Governance Policy	ABD	2023
64	Northeastern University	Data Governance Policy	ABD	2024
65	Northern Arizona University	Information Technology and Data Governance Trustees Charter	ABD	2024
66	Northern Kentucky University	Data Governance and Security Policy	ABD	2019
67	Northwest Missouri State University	Data Governance Policy	ABD	2024
68	Oakwood University	Data Management and Information Security Policy	ABD	2021
69	Ohio State University	Institutional Data Policy	ABD	2021
70	Old Dominion University	Data Administration Policy	ABD	2022
71	Olympic College	Data Governance Policy	ABD	2019
72	Oregon State University	University Data Management, Classification, and Incident Response	ABD	2017
73	Queen Mary University of London	Information/Data Governance Policy	BK	2022
74	Purdue University Northwest	Data Governance Policy	ABD	2020
75	Rhode Island College	Data Governance Policy	ABD	2024
76	Rochester Institute of Technology	Institutional Data Governance Policy	ABD	2017
77	Royal College of Art	Data Governance Framework	BK	2024
78	St. Mary's University	Data Governance Policy	BK	2023
79	Sam Houston State University	Data Governance Policy	ABD	2024

80	Salt Lake Community College	Data Governance Policy	ABD	2022
81	Southern University	Data Governance Policy	ABD	2020
82	Southern Methodist University	Institutional Data Governance Policy	ABD	2023
83	Southern Utah University	Data Governance and Protection Policy	ABD	2019
84	Southern Wesleyan University	Data Governance Policy	ABD	2024
85	Southwestern University	Data Governance Policy	ABD	2024
86	Snow College	Data Governance Policy	ABD	2024
87	Tennessee Wesleyan University	Data Policy	ABD	2024
88	Texas Agricultural and Mechanical University	University Data Governance and Management Policy	ABD	2024
89	Texas Christian University	Data Governance Charter	ABD	2019
90	Texas Tech University	Data Management and Data Governance	ABD	2023
91	Towson University	Data Governance Policy	ABD	2021
92	Tulane University	Data Governance Policy	ABD	2023
93	University at Buffalo	Data Governance Policy	ABD	2014
94	University of Alabama	Data Governance Program Charter	ABD	2025
95	University of Alaska	Data Governance Policy	ABD	
96	University of Arkansas	Data Management, Use and Protection	ABD	2014
97	University of Arkansas at Little Rock	Data Governance Policy Framework	ABD	2018
98	University of Baltimore	Institutional Data Management Policy	ABD	2020
99	University of California	Data Governance Task Force	ABD	2016
100	University of Central Arkansas	Data Management, Use and Protection	ABD	2023
101	University of Chicago	Managing University Data	ABD	2020
102	University of Cincinnati	Data Governance and Classification Policy	ABD	2021
103	University of Delaware	Data Governance Policy	ABD	2018
104	University of Denver	Data Governance Committee Charter	ABD	2024
105	University of Hertfordshire	Data Management Policy	BK	2023
106	University of Maryland	Policy on Data Management Structure and Procedures	ABD	2013
107	University of Michigan	Institutional Data Resource Management Policy	ABD	2022
108	University of Montana	Data Classification and Management Standard	ABD	2024
109	University of Nebraska	Institutional Data Use Policy	ABD	2022
110	University of Nevada	Data Governance Policy	ABD	2010
111	University of Nevada Las Vegas	Institutional Data Governance and Management Policy	ABD	2010
112	University of New England	The Data and Information Governance and Strategy Committee	ABD	2015
113	University of New Mexico	Data Governance Policy	ABD	2023
114	University of North Carolina at Chapel Hill	University Data Governance Policy	ABD	2018
115	University of North Carolina at Greensboro	Data Governance Structure	ABD	2022
116	University of North Carolina at Wilmington	Data Governance and Management Policy	ABD	2025
117	University of North Georgia	Data Governance and Management Policy	ABD	2023
118	University of North Texas	Data Governance Insights	ABD	
119	University of Northern Iowa	Institutional Data Policy	ABD	2023
120	University of Nottingham	Data Governance and Quality Policy	BK	2024

121	University of Oklahoma	Data Governance Policy	ABD	2024
122	University of Richmond	Administrative Data Management Policy	ABD	2023
123	University of Rochester	Institutional Data Governance Policy	ABD	2017
124	University of St Andrews	Data Governance Policy	BK	2021
125	University of St Francis	Data Governance Policy	ABD	2022
126	University of St Thomas	Data Management Policy	ABD	2023
127	University of South Carolina	Data and Information Governance Policy	ABD	2019
128	University of South Florida	Data Management Policy	ABD	2023
129	University of Suffolk	Data Management Policy	BK	2024
130	University of Southern California	External Surveys and Rankings Data Management Policy	ABD	2023
131	University of Texas Arlington	Data Governance Program Charter	ABD	2016
132	University of Texas at Austin	Data Governance Policy	ABD	2021
133	University of Utah	University Institutional Data Management Policy	ABD	2020
134	University of Wisconsin	Institutional Data Policy	ABD	2025
135	University of Wollongong.	Data Governance Policy	Avustralya	2024
136	Vincennes University	Data Governance Policy	ABD	2023
137	Virginia Commonwealth University	Data and Information Governance	ABD	2020
138	Washburn University	Data Management Policy	ABD	2014
139	Washington University St. Louis	Data Governance Policy	ABD	
140	Wayne State University	Data Governance Core Committee	ABD	
141	Wesleyan College	Data Governance Policy	ABD	2024
142	West Chester University	Data Governance Policy	ABD	2019
143	Western Michigan University	Data and Systems Governance Policy	ABD	2024
144	Wichita State University	Data Governance Policy	ABD	2014
145	William Paterson University	Data Governance Policy	ABD	2017
146	Williams College	Data Governance Policy	ABD	2025

EK 6. ULUSLARARASI VE ULUSAL ÜNİVERSİTELERİN TEMATİK KODLAMALARI

Sıra	Ana Tema	Alt Tema	%
1	Veri Yönetişimi Birimleri ve Personeli	Organizasyon Yapısı, Roller ve Sorumluluklar, İnsan Kaynağı, İş Birliği ve Koordinasyon	43,8
2	Veri Standartları	Veri Standardizasyonu, Üst Veri Yönetimi, Veri Kalitesi, Referans Veri Yönetimi	32,6
3	Veri Güvenliği ve Gizlilik	Erişim Yönetimi, Veri Paylaşımı, Veri Entegrasyonu, Dış Paylaşım	11,9
4	Veri Erişimi ve Paylaşımı	Veri Depolama, Veri Yedekleme, Veri Güvenliği, Gizlilik ve Mahremiyet, Teknik Koruma Önlemleri	6,9
5	Veri Kültürü	Veri Kültürü, Veri Okuryazarlığı, Eğitim ve Farkındalık, Veri Temelli Karar Alma, Değişim Yönetimi	4,8
Toplam			100

EK 7. GÖRÜŞME BULGULARI İLE MODEL BİLEŞENLERİNİN KARŞILIKLARI

	Ana Tema	Görüşme bulgusu	Modelde karşılığı
Stratejik Katman	Veri Yönetişimi Birimleri ve Personel	Koordinatörlük ve ofisler kurumsal veri yönetimi, raporlama ve karar desteğine odaklanmaktadır.	Karar alma mekanizmalarının kurulması ve veri yönetişiminin kurumsal hedeflerle ilişkilendirilmesi.
	Veri Yönetişimi Birimleri ve Personel	Birimler doğrudan rektörlük veya rektör yardımcılığına bağlıdır.	Liderlik ve stratejik sahiplik. Veri Yönetişimi Ofisinin üst yönetimle doğrudan ilişkili konumlandırılması.
	Veri Yönetişimi Birimleri ve Personel	Birimler üst yönetime düzenli raporlama yapmaktadır.	İzleme, geri bildirim ve performans raporlaması.
	Veri Yönetişimi Birimleri ve Personel	Bazı kurumlarda rol, yetki ve sorumluluklar resmî çalışma esaslarıyla belirlenmektedir.	Rol ve sorumluluk matrisi, karar hakları ve hesap verebilirliğin tanımlanması.
	Veri Yönetişimi Birimleri ve Personel	Veri yönetişimi görevleri çoğunlukla akademisyenler tarafından ek görev olarak yürütülmektedir. Faaliyetler personelin kalan zamanında sürdürülmektedir.	Uzman insan kaynağı planlaması, rollerin kurumsallaştırılması ve sürekli çalışan profesyonel ofis yapılması.
	Veri Yönetişimi Birimleri ve Personel	Veri yönetişimi ve veri bilimi uzmanı sayısı sınırlıdır.	Uzman insan kaynağı planlaması (Kültür Katmanında rol bazı eğitimle desteklenir).
	Veri Yönetişimi Birimleri ve Personel	Birimler çoğunlukla YÖK ve üst yönetimin raporlama taleplerini karşılayan operasyonel yapılar olarak çalışmaktadır.	Veri yönetişiminin raporlama işlevini aşarak kurumsal değer, karar ve performans yönetimiyle ilişkilendirilmesi.
	Veri Standartları	Üniversiteler veriyi kurumsal bir varlık olarak tanımlama ihtiyacının farkındadır.	Verinin stratejik kurumsal varlık olarak kabul edilmesi ve veri stratejisine bağlanması.
	Veri Erişimi ve Paylaşımı	Veri paylaşımı sıralama, performans, kalite ve akreditasyon süreçlerine yöneliktir.	Veri paylaşımının kurumsal hedefler, performans ve değer yönetimiyle ilişkilendirilmesi.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Ticari yazılımlara bağımlılık ve dış kaynak kullanımı konusunda çekinceler bulunmaktadır.	Risk ve uyum çerçevesinin oluşturulması.
Yönetişim Katmanı	Veri Kültürü	Yönetim değişiklikleri veri yönetişimi tercihlerini ve teknik stratejileri değiştirmektedir. Önceki çalışmalar terk edilebilmektedir.	Yönetim dönemlerinden bağımsız veri stratejisi, yol haritası ve politika geliştirme süreci.
	Veri Kültürü	Üniversitelerde veriye dayalı karar alma kültürü henüz tam yerleşmemiştir.	Karar alma mekanizmaları ve değer yönetimi (Kültür Katmanındaki veri güveni ve veri kalitesiyle desteklenir).
	Veri Yönetişimi Birimleri ve Personel	Veri yönetişimi birimleri koordinatörlük, ofis, birim ve araştırma merkezi gibi farklı biçimlerde yapılandırılmıştır; en yaygın yapılanma koordinatörlüktür.	Ortak, esnek ve koordinasyon odaklı Veri Yönetişimi Ofisi yapılması.
	Veri Yönetişimi Birimleri ve Personel	Veri yönetişimi kurumsal yapıları henüz standartlaşmamıştır.	Veri Yönetişimi Kurulu, Ofisi, rol yapısı ve karar mekanizmalarının tanımlanması.

	Veri Yönetişimi Birimleri ve Personel	Yönetim ve danışma kurullarında rektörlük, genel sekreterlik, strateji, kalite ve bilgi işlem temsil edilmektedir.	Çok paydaşlı Veri Yönetişimi Kurulu.
	Veri Yönetişimi Birimleri ve Personel	Her akademik ve idari birimde veri yöneticisi ve veri sorumlusu görevlendirilmektedir.	Veri sahipleri, veri sorumluları ve veri alan liderlerinden oluşan federatif rol yapısı.
	Veri Yönetişimi Birimleri ve Personel	Birim personelinin görev ve sorumlulukları birçok kurumda tanımlı değildir.	Veri sahibi, veri sorumlusu, teknik veri sorumlusu ve kullanıcı rollerinin açık görev tanımlarıyla düzenlenmesi.
	Veri Yönetişimi Birimleri ve Personel	Veri yönetişimi birimleri az sayıda personelle çalışmaktadır.	Merkezi ofis ile birimlere dağıtılmış rollerin birlikte kullanıldığı hibrit yapılanma.
	Veri Yönetişimi Birimleri ve Personel	Kurumsal veriler öğrenci, akademik, araştırma ve yönetim verisi gibi alanlara ayrılmaktadır.	Veri alan liderleri ve veri sahipleri aracılığıyla alan bazlı sorumluluk dağılımı.
	Veri Erişimi ve Paylaşımı	Verilerin nerede tutulduğu, kimlerin eriştiği ve sorumlularının kim olduğu belirlenmeye çalışılmaktadır.	Veri sahipleri ve veri sorumlularının belirlenmesi (Süreç Katmanında yaşam döngüsüyle desteklenir).
	Veri Erişimi ve Paylaşımı	Kurum içi veri paylaşımı rektörlük, strateji, kalite ve genel sekreterlik arasında gerçekleşmektedir.	Veri Yönetişimi Kurulu aracılığıyla kurum içi koordinasyon.
	Veri Erişimi ve Paylaşımı	Veri erişimi ve paylaşımı çok aktörlü bir yapıda yürütülmektedir.	Kurul, Ofis, veri sahipleri ve teknik birimler arasında karar ve sorumluluk dağılımı.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Güvenlik politikasını koordinatörlük, teknik uygulamayı Bilgi İşlem yürütmektedir.	Politika ve uygulama sorumluluklarının ayrıştırılması.
	Veri Yönetişimi Birimleri ve Personel	Bilgi İşlem ile veri yönetişimi birimi arasında yakın çalışma gerekmektedir.	Veri Yönetişimi Ofisi–BT koordinasyon mekanizması.
	Veri Yönetişimi Birimleri ve Personel	Veri temsilcilerinin görevlerini yanlış anlaması uygulamayı zorlaştırmaktadır.	Açık rol tanımları ve rol bazlı yönetim düzeni (Kültür Katmanında eğitimle desteklenir).
Süreç Katmanı	Veri Yönetişimi Birimleri ve Personel	Veri giriş ve veri onay sorumluları ayrı kişiler olarak belirlenmektedir.	Veri üretme, doğrulama ve onay iş akışlarının ayrıştırılması.
	Veri Standartları	Veri envanteri oluşturulması üniversitelerin öncelikli hedeflerinden biridir.	Veri yaşam döngüsü kapsamında veri envanteri ve üst veri süreçleri.
	Veri Standartları	Veri doğrulama için ortak yazılı standart bulunmamaktadır.	Kurumsal veri doğrulama standardı ile yaşam döngüsü içinde doğrulama/denetim adımlarının tanımlanması.
	Veri Standartları	Bazı kurumlar henüz veri envanteri aşamasındadır.	Veri yaşam döngüsünün başlangıç aşamalarında envanter ve kalite kontrolünün kurulması.
	Veri Erişimi ve Paylaşımı	Veri göstergeleri merkezi birimin onayına sunulmaktadır.	Veri yaşam döngüsünde doğrulama, onay ve yayımlama iş akışları.
	Veri Erişimi ve Paylaşımı	YÖK, TÜBİTAK, THE, QS ve URAP gibi dış kuruluşlarla düzenli veri alışverişi yapılmaktadır.	Veri yaşam döngüsünde paylaşım ve yayımlama süreçlerinin tanımlanması (Yasal ve Etik Katmanla desteklenir).
	Veri Erişimi ve Paylaşımı	Yetkilendirme doğrultusunda açık arşiv ve diğer sistemlere erişilmektedir.	Veri yaşam döngüsünde erişim, paylaşım ve yayımlama süreçleri.

Teknik Katman	Veri Erişimi ve Paylaşımı	Veri talepleri çoğunlukla yönetsel gereksinime göre ve süreç içinde ortaya çıkmaktadır.	Standartlaştırılmış veri talebi, değerlendirme, onay ve erişim iş akışları.
	Veri Kültürü	Yeni veri süreçleri çalışanlar tarafından ek iş yükü olarak algılanmaktadır.	İş akışlarının mevcut görevlerle bütünleştirilmesi (Kültür Katmanında değişim yönetimiyle desteklenir).
	Veri Yönetişimi Birimleri ve Personel	Araştırma merkezleri veri bilimi, büyük veri, yapay zekâ ve Ar-Ge faaliyetlerine ağırlık vermektedir.	Veri ambarı, iş zekâsı ve ileri analitik bileşenleri.
	Veri Standartları	Yönetmeliklerde veri kalitesi, sınıflandırma, sahiplik ve üst veri bileşenleri sistematik biçimde tanımlanmamıştır.	Veri kalitesi, sınıflandırma, veri mimarisi ve üst veri yönetiminin ayrı teknik bileşenler olarak tanımlanması.
	Veri Standartları	Bazı yönergelerde veri sözlüğü, veri haritası ve veri kataloğu oluşturulması öngörülmektedir; bazı kurumlarda çalışmalar tamamlanamamıştır.	Veri sözlüğü, veri kataloğu ve üst veri yönetimi.
	Veri Standartları	Veri kalitesi doğruluk, bütünlük, güncellik, geçerlilik, gizlilik ve erişilebilirlik boyutlarıyla ele alınmaktadır.	Veri kalitesi yönetimi, kalite ölçütleri ve izleme araçları.
	Veri Standartları	Veri standardizasyonu büyük ölçüde ticari yazılımlar aracılığıyla yürütülmektedir.	Kurumsal veri mimarisi ile veri modelleme ve tasarımı.
	Veri Standartları	Akademik personelin kurumsal kimlikle sisteme tanımlanması veri bütünlüğünü desteklemektedir.	Veri entegrasyonu ve birlikte çalışabilirlik.
	Veri Standartları	Veri sınıfları fiilen kullanılmakta, ancak çoğu kurumda yazılı sınıflandırma politikası bulunmamaktadır.	Kurumsal veri sınıflandırma standardı (Yasal ve Etik Katmanla desteklenir).
	Veri Standartları	Birim veri temsilcileri, sahip oldukları verilerin üst verisini merkezi birime iletmektedir.	Merkezi üst veri yönetimi.
	Veri Erişimi ve Paylaşımı	Erişim uygulamaları rol temelli yürütülmekte ancak sınıflandırma politikasıyla desteklenmemektedir.	Erişim yönetimi ve teknik yetkilendirme mekanizmaları.
	Veri Standartları	Ortak veri tanımları ve üst veri, kurumsal olarak aynı dili konuşmanın aracı olarak görülmektedir.	Veri modelleme, veri mimarisi ve üst veri yönetimi.
	Veri Standartları	Manuel girilen veriler doğrulanmış veri olarak kabul edilmemekte ve ayrıca kontrol edilmektedir.	Veri kalitesi kuralları ve doğrulama statüsü.
	Veri Standartları / Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Farklı sistemlerin entegrasyonu önemli bir sorun alanıdır; veriler çok sayıda bilgi sisteminde tutulmaktadır.	Kurumsal veri mimarisi, entegrasyon/ETL/ESB ve birlikte çalışabilirlik.
	Veri Erişimi ve Paylaşımı	Kurumsal veri erişimi henüz merkezi bir platform üzerinden yürütülmemektedir.	Veri depolama ve operasyonlar; merkezi erişim mimarisi.
	Veri Erişimi ve Paylaşımı	Üniversiteler bütün kurumsal verileri tek gösterge panelinde izlemeyi planlamaktadır.	Veri ambarı, iş zekâsı, veri depolama ve operasyonlar.
	Veri Standartları	Yıllar arasındaki büyük veri sapmaları kontrol edilmektedir.	Veri kalitesi, anomali ve eğilim kontrolleri.

	Veri Erişimi ve Paylaşımı	Veri erişimi görev ve yetkiye göre farklılaştırılmaktadır; IP blokları erişim kontrolünde kullanılmaktadır.	Erişim yönetimi ve veri güvenliği.
	Veri Erişimi ve Paylaşımı	Dış veri tabanlarından ORCID, YÖKSİS, PubMed, Web of Science ve Scopus verileri alınmaktadır.	Veri entegrasyonu, birlikte çalışabilirlik ve üst veri yönetimi.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Sistemler arası birlikte çalışabilirlik hedeflenmektedir.	Veri entegrasyonu ve uyumluluk.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Verilerin tek merkezde veya bütünleşik yapıda izlenmesi amaçlanmaktadır; dağıtık sistemler bütünleşik platformlarda bir araya getirilmeye çalışılmaktadır.	Kurumsal veri ambarı, iş zekâsı, veri depolama ve operasyonlar.
	Veri Kültürü	Kurumsal hafıza eksikliği veri toplama süreçlerinde sorun yaratmaktadır.	Veri kataloğu, arşiv ve kurumsal kayıt sistemleri.
Kültür Katmanı	Veri Kültürü	Kurum kültürünün dönüşümü veri yönetişiminin en kritik zorluklarından biridir.	Kurumsal kültürel dönüşümün bağımsız bir model bileşeni olarak ele alınması.
	Veri Kültürü	Veri yönetişimi birimlerinin görevleri arasında veri farkındalığı oluşturmak bulunmaktadır.	Eğitim ve farkındalık programları.
	Veri Kültürü	Tüm çalışanların veri yönetimi konusunda bilinçlendirilmesi hedeflenmektedir.	Kurum geneline yayılan veri okuryazarlığı programı.
	Veri Kültürü	Yeni üniversitelerde deneyim ve kurumsal hafıza eksikliği bulunmaktadır.	İletişim, iş birliği ve kurumsal öğrenme.
	Veri Kültürü	Üst yönetim desteği en önemli kolaylaştırıcı unsur olarak görülmektedir.	Liderlik desteği.
	Veri Kültürü	Akademik ve idari birimler veri toplama ve giriş süreçlerine direnç göstermektedir.	Değişim yönetimi, eğitim, farkındalık ve çalışan katılımı.
	Veri Standartları	Ortak veri tanımları ve üst veri, kurumsal olarak aynı dili konuşmanın aracı olarak görülmektedir.	Veri paylaşımı, veri güveni ve iş birliği.
Yasal ve Etik Katman	Veri Yönetişimi Birimleri ve Personel	Birimlerin hukuki ve idari kuruluş dayanakları farklılaşmaktadır.	Ortak düzenleyici ve stratejik politika çerçevesinin oluşturulması.
	Veri Erişimi ve Paylaşımı	Veri kümelerinin araştırmacılarla paylaşılmadan önce kişisel verilerden arındırılması öngörülmektedir.	KVKK, mahremiyet, anonimleştirme ve kontrollü paylaşım ilkeleri.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Veri güvenliği ve mevzuata uyum yönergelerin temel amaçları arasındadır.	Düzenleyici uyum ve kurumsal politika çerçevesi; teknik güvenlik kontrolleriyle bütünleşme.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	KVKK ve veri mahremiyeti kurumsal amaçlar arasında açıkça belirtilmektedir.	KVKK uyumu, mahremiyet ve sorumlu veri kullanımı.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	Veri kullanım politikalarının geliştirilmesi öngörülmektedir.	Veri kullanımı, erişim ve paylaşım politikalarının oluşturulması.
	Veri Depolama, Yedekleme, Güvenlik ve Gizlilik	ISO/IEC 27001 gibi bilgi güvenliği standartlarına uyum sağlanmaktadır.	Standart ve mevzuat uyumu; veri güvenliği kontrolleriyle bütünleşme.

Veri Erişimi ve Paylaşımı	Veri sınıflandırması ve erişim uygulamalarını destekleyen yazılı politika eksikliği bulunmaktadır.	Veri sınıflandırma, erişim ve paylaşım hükümlerini içeren politika çerçevesi.
Veri Kültürü	Yönetim değişiklikleri teknik stratejileri ve önceki uygulamaları etkileyebilmektedir.	Kurumsal sürekliliği sağlayacak onaylı politika ve düzenleyici çerçeve.

EK 8. ULUSLARARASI VERİ YÖNETİŞİMİ POLİTİKALARI VERİLERİNİN MODEL BİLEŞENLERİ KARŞILIĞI

	Politika bulguları	Modelde karşılığı
Stratejik Katman	Üst yönetimin politika onayı, kaynak tahsisi ve stratejik karar alma süreçlerindeki rolü Loglama, denetim ve şeffaf raporlama uygulamaları	Liderlik desteği, stratejik sahiplik, veri stratejisi, kaynak yönetimi, karar ve performans yönetimi Veri güveni, hesap verebilirlik ve yönetim performansının izlenmesi
Yönetişim Katmanı	Veri yönetişimi birimlerinin üst yönetime bağlı, çok katmanlı ve rol temelli yapılandırılması Veri standartlarının düzenli olarak gözden geçirilmesi ve güncellenmesi Rol temelli erişim kontrolü ve veri sahibi onay mekanizmaları Akademik, idari ve teknik birimler arasında koordinasyonun sağlanması	Veri Yönetişimi Kurulu, Veri Yönetişimi Ofisi, Veri Sahipleri, Veri Sorumluları, Teknik Veri Sorumluları, Veri Alan Liderleri ve Veri Kullanıcılarından oluşan yönetim yapısı Standartlara uyum, izleme, denetim ve sürekli iyileştirme Rol temelli erişim, veri sahipliği ve yetkilendirme süreçleri İş birliği ve katılımcı yönetim
Süreç Katmanı	Veri standartlarının düzenli olarak gözden geçirilmesi ve güncellenmesi Verinin oluşturulduğu anda sınıflandırılması ve yaşam döngüsü boyunca yönetilmesi Veri oluşturma, doğrulama, paylaşma, saklama, arşivleme ve imha süreçlerinin tanımlanması Kurum içi ve kurum dışı veri paylaşımının politika ve prosedürlerle düzenlenmesi Veri saklama, arşivleme, imha ve veri öznesi haklarının tanımlanması	Standartlara uyum, izleme, denetim ve sürekli iyileştirme Veri yaşam döngüsü yönetimi Veri yaşam döngüsü süreçleri Veri paylaşım süreçleri, kurum dışı paylaşım mekanizmaları Veri saklama ve imha politikaları, veri öznesi hakları
Teknik Katman	Ortak veri tanımları, veri sözlüğü, üst veri katalogları ve veri standartlarının kullanılması Veri bütünlüğü, birlikte çalışabilirlik ve ortak veri modelleri Veri kalitesinin doğruluk, bütünlük, tutarlılık ve güncellik ölçütleriyle izlenmesi Rol temelli erişim kontrolü ve veri sahibi onay mekanizmaları Hassas veriler için şifreleme, loglama, kimlik doğrulama ve erişim kontrolleri Merkezi veri depolama, veri ambarı ve analitik altyapının kullanılması Düzenli yedekleme, felaket kurtarma ve iş sürekliliği uygulamaları Loglama, denetim ve şeffaf raporlama uygulamaları	Veri mimarisi, veri modelleme ve tasarımı, veri sözlüğü, üst veri yönetimi Veri entegrasyonu ve uyumluluk, ana veri yönetimi, referans veri yönetimi Veri kalitesi yönetimi ve kalite performans göstergeleri Rol temelli erişim, veri sahipliği ve yetkilendirme süreçleri Veri güvenliği, kimlik ve erişim yönetimi Veri depolama ve operasyonlar, veri ambarı ve iş zekâsı Yedekleme, iş sürekliliği ve felaket kurtarma Veri güveni, hesap verebilirlik ve yönetim performansının izlenmesi
Kültür Katmanı	Etik veri kullanımı, şeffaflık ve hesap verebilirlik ilkelerinin benimsenmesi Veri yönetişimi eğitimlerinin kurumsal düzeyde yürütülmesi Ortak veri dili ve standart terminolojinin kullanılması Akademik, idari ve teknik birimler arasında koordinasyonun sağlanması	Etik ve sorumlu kullanım Veri okuryazarlığı, eğitim ve farkındalık Standartlaşma ve kurumsal öğrenme İş birliği ve katılımcı yönetim

	Loglama, denetim ve şeffaf raporlama uygulamaları	Veri güveni, hesap verebilirlik ve yönetim performansının izlenmesi
Yasal ve Etik Katman	GDPR, FERPA, HIPAA vb. düzenlemelere uyum	Düzenleyici çerçeveler ve stratejik politika çerçeveleri
	Veri saklama, arşivleme, imha ve veri öznesi haklarının tanımlanması	Veri saklama ve imha politikaları, veri öznesi hakları
	Etik veri kullanımı, şeffaflık ve hesap verebilirlik ilkelerinin benimsenmesi	Etik ve sorumlu kullanım