Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Ana Bilim Dalı

KAMUSAL BİLGİ VE VERİ YÖNETİMİ POLİTİKALARI ÇERÇEVESİNDE ÖZEL GÜVENLİK GEREKTİREN BELGELERİN YÖNETİMİ

Ahmet KAYMAK

Yüksek Lisans Tezi

Ankara, 2024

KAMUSAL BİLGİ VE VERİ YÖNETİMİ POLİTİKALARI ÇERÇEVESİNDE ÖZEL GÜVENLİK GEREKTİREN BELGELERİN YÖNETİMİ

Ahmet KAYMAK

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Anabilim Dalı

Yüksek Lisans Tezi

Ankara, 2024

KABUL VE ONAY

Ahmet KAYMAK tarafından hazırlanan “Kamusal Bilgi ve Veri Yönetimi Politikaları Çerçevesinde Özel Güvenlik Gerektiren Belgelerin Yönetimi” başlıklı bu çalışma, 07.06.2024 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Prof. Dr. Fahrettin ÖZDEMİRCİ (Başkan)

Prof. Dr. Özgür KÜLCÜ (Danışman)

Doç. Dr. Şahika EROĞLU (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Uğur ÖMÜRGÖNÜLŞEN

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin 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 metinleri 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)

07/06/2024

Ahmet KAYMAK

"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

*(1) Madde 6. 1. Lisansüstü tezle 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 çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Prof. Dr. Özgür KÜLCÜ** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Ahmet KAYMAK

TEŞEKKÜR

Bu tezin tamamlanması sürecinde birçok kişiden destek aldım. Bu vesileyle, öncelikle tez danışmanım Prof. Dr. Özgür KÜLCÜ'ye en içten saygılarımı ve sonsuz teşekkürlerimi sunarım. Kıymetli hocamın yönlendirmeleri, önerileri ve sabrı olmadan bu çalışmayı tamamlamam mümkün olmazdı.

Tez çalışmasının gelişimine yönelik değerli eleştiri, görüş ve önerilerini bildiren kıymetli jüri üyeleri Prof. Dr. Fahrettin ÖZDEMİRCİ ve Doç. Dr. Şahika EROĞLU'na çok teşekkür ederim.

Ayrıca, bu tez çalışmasının gerçekleştirilmesindeki destekleri için aileme ve sevdiklerime minnettarım. Bana her zaman destek olan, cesaret veren ve inancını kaybetmemem için yanımda olan değerli eşim Behiye KAYMAK'a çok teşekkür ederim. Yaşam kaynağım olan çocuklarımın sevgi ve neşeleri bana büyük motivasyon kaynağı oldu, en büyük teşekkürü canım kızım Sare'ye ve canım oğlum Mustafa Doğan'a ediyorum. Her zaman yanımda olup sevgi ve desteğini esirgemeyen annem Seher KAYMAK ile her zaman doğruları söyleyen ve ilham veren ablam Şerife ATEŞ'e çok teşekkür ederim.

ÖZET

KAYMAK, Ahmet. *Kamusal Bilgi ve Veri Yönetimi Politikaları Çerçevesinde Özel Güvenlik Gerektiren Belgelerin Yönetimi*, Yüksek Lisans Tezi, Ankara, 2024.

Kurumsal bilgi sistemlerinde çok çeşitli ve farklı özelliklere sahip veri, bilgi ve belge oluşturulmakta veya sağlanmaktadır. Bu özelliklerin en önemlisi olan gizlilik, veri, bilgi ve belgelere yetkisiz erişimlerin engellenmesi amacıyla kullanılan özel bir güvenlik tedbiridir. Özel güvenlik gerektiren belgeler başarılı bir şekilde yönetilemediğinde, gerekli olan güvenlik önemlerinin alınamamasına, kişisel mahremiyet ile ulusal güvenliğin, ulusal ve uluslararası menfaatlerin zarar görmesine, belge süreçlerinin iş yükünün ve maliyetinin artmasına ve etkinliğinin azalmasına, bilgi edinme hakkının engellenmesine neden olmaktadır. Bu araştırmanın amacı, kamu kurumlarında gizlilik dereceli belge yönetimi çerçevesinin oluşturulması, belge gizliliği ve güvenliğinin sağlanması için politika ve prosedürlerin belirlenmesi, farklı ortamlarda gerçekleştirilen gizlilik dereceli belge yönetim süreçlerine ait gerekliliklerin tespit edilmesi, gizlilik dereceli olmayan fakat özel güvenlik gerektiren belgeleri de kapsayan, özel güvenlik gerektiren belge yönetimine ilişkin bir model önerisinin sunulmasıdır.

Doküman analizi yöntemiyle elde edilen araştırma verileri betimsel analiz tekniği kullanılarak analiz edilmiştir. Araştırmada sonucunda "*Türkiye'de, kamu kurumlarında kamusal bilgi ve veri yönetimi politikaları çerçevesinde özel güvenlik gerektiren belgelerin yönetimine dönük bütünsel (holistic) politikalar oluşturulmadığı için ilgili belge serilerine dönük gizlilik derecelerinin tanımlanması, bu belgelerin düzenlenmesi, kullanımı, arşivlenmesi, korunması ve süreçlerde teknolojik araçların kullanımında belirsizlikler yaşanmaktadır*" şeklinde belirlenen hipotez doğrulanmıştır. Gizlilik dereceli belge yönetiminin farklı kurumsal düzlemlerde ilgili gizlilik derecesine göre fiziki veya elektronik ortamlarda gerçekleştirildiği tespit edilmiştir. Gizlilik dereceli belgelerin oluşturulacağı ve muhafaza edileceği birimler ile gizlilik derecesinin değerlendirilmesi, gizlilik derecesinin düşürülmesi, kaldırılması veya belgenin imha edilmesi ve bilgi talebi itirazları kapsamında farklı yapıların oluşturulduğu görülmüştür. Araştırma bulguları doğrultusunda özel güvenlik gerektiren belgelere yönelik bir model geliştirilmiştir. Kamu kurumlarının mevcut gizlilik dereceli belge yönetimi uygulamalarının iyileştirilmesine, daha etkili gizlilik politikalarının ve prosedürlerinin oluşturulmasına ve denetim süreçlerinin geliştirilmesine yönelik önerilerde bulunulmuştur.

Anahtar Sözcükler

Veri Yönetimi, Belge Yönetimi, Devlet Sırrı, Gizlilik Derecesi, Gizli Belge

ABSTRACT

KAYMAK, Ahmet. *Management of Records Requiring Special Security within the Framework of Public Information and Data Management Policies*, Master's Thesis, Ankara, 2024.

In enterprise information systems, data, information and records with various and different characteristics are created or provided. Confidentiality, which is the most important of these features, is a special security measure used to prevent unauthorised access to data, information and records. When records requiring special security cannot be managed successfully, it leads to failure to take the necessary security measures, damage to personal privacy and national security, national and international interests, increase in the workload and cost of records processes and decrease in effectiveness, and prevention of the right to information. The purpose of this research is to establish a framework for confidential document management in public institutions, to determine policies and procedures for ensuring document confidentiality and security, to determine the requirements for confidential document management processes carried out in different environments, and to propose a model for document management that requires special security, including documents that are not confidential but require special security.

The research data obtained by document analysis method were analysed using descriptive analysis technique. As a result of the research, the hypothesis determined as '*Since holistic policies for the management of records requiring special security have not been established within the framework of public information and data management policies in public institutions in Turkey, there are uncertainties in defining the degree of confidentiality for the relevant records series, organizing, using, archiving and protecting these records and using technological tools in the processes*' has been confirmed. It has been determined that confidential records management is carried out at different organisational levels in physical or electronic environments according to the degree of confidentiality. It has been observed that different structures have been established within the scope of the units where confidential records will be created and maintained, the evaluation of the degree of confidentiality, the reduction, removal or destruction of the degree of confidentiality, and information request objections. In line with the research findings, a model has been developed for records requiring special security. Recommendations have been made to improve the existing confidential records management practices of public institutions, to establish more effective confidentiality policies and procedures, and to improve audit processes.

Keywords

Data Management, Records Management, State Secret, Security Classification, Secret Records

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AIIM	the Association for Intelligent Information Management
BGYS	Bilgi Güvenliği Yönetim Sistemi
BTK	Bilgi ve İletişim Kurumu
BTYK	Bilim ve Teknoloji Yüksek Kurulu
DAA	Devlet Arşiv Ağı
DAVM	Devlet Arşivi Veri Merkezi
DCMI	Dublin Core Metadata Initiative
DETSİS	Devlet Teşkilatı Merkezi Kayıt Sistemi
EBYS	Elektronik Belge Yönetim Sistemi
ETL	Extract, Transform, Load
IEC	the International Electrotechnical Commisson
ISCAP	the Interagency Security Classification Appeals Panel
ISO	the International Organization for Standardization
ISOO	the Information Security Oversight Office
HEYS	Hizmet Envanteri Yönetim Sistemi
KAYSİS	Elektronik Kamu Bilgi Yönetim Sistemi
KEP	Kayıtlı Elektronik Posta
KEPHS	Kayıtlı Elektronik Posta Hizmet Sağlayıcıları
KİY	Kurumsal İçerik Yönetimi
KMS	Kamu Mevzuat Sistemi
MSR	Management System for Records
NAA	National Archives of Avustralia
NARA	National Archives and Records Administration
NDC	the National Declassification Center
NFPA	the National Fire Protection Association
PIDB	the Public Interest Declassification Board
UKEVM	Ulusal Kamu Entegre Veri Merkezi
XLM	Extensible Markup Language

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

1. BÖLÜM

GİRİŞ

1.1. KONUNUN ÖNEMİ

Bilgi ve iletişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla bilginin elde edilmesi, işlenmesi ve paylaşılması eskiye oranla daha kolay ve hızlı bir şekilde yapılmaktadır. Bu değişimle birlikte, kamu kurum ve kuruluşları iş süreçlerinin ve faaliyetlerinin büyük bir bölümünü elektronik ortamda sürdürmeye başlamıştır. Bu sayede veri, bilgi ve belgelerin yönetimini birbirleriyle ilişkili şekilde daha hızlı ve sürdürülebilir olarak gerçekleştirmektedirler. Bu sebeple kurum ve kuruluşlar, bilgi varlıklarını etkin bir şekilde yönetebilmek için değişen koşullara uyum sağlayarak bilgi yönetimi altyapılarını bilgi teknolojileri çerçevesinde geliştirilmişlerdir (Eroğlu ve Çakmak, 2020a, s. 59; Külcü ve diğerleri, 2015, s. 25). Bilgi ve belgelerin e-devlet modeli kapsamında elektronik süreçlerde yönetilmesi ile bunların doğrudan ve geniş ölçekli olarak paylaşılması yetkisiz erişim ihlali risklerinin artmasına neden olabileceği düşünülmektedir (Özdemirci ve Torunlar, 2015, s.52). Bu bağlamda, ulusal ve kişisel menfaatlerin korunması çerçevesinde, hassas bilgileri içeren belgelerin diğer belgelerden farklı işleme tabi tutulması gerektiği ifade edilmektedir (Odabaş, 2008, s.126).

Kamu kurum ve kuruluşlarında bulunan ve özel güvenlik gerektiren veri, bilgi ve belgelerin yetkisiz olarak açıklanması, kişisel, kurumsal, ulusal ve uluslararası menfaatlerin farklı önemlilik düzeylerinde zarar görmesine neden olabilmektedir. Bu ihtimalleri doğuracak yetkisiz erişimin engellenmesi maksadıyla veri, bilgi ve belgelere yönelik gizlilik sınıflandırılması yapılmaktadır (Diri ve Gülçiçek, 2012, s. 499). Hassas bilgileri içeren veri, bilgi ve belgelerin sistemli olarak yönetilmesinin ilk adımı olan gizlilik sınıflandırılması, uygun iş ve güvenlik süreçlerinin belirlenmesinde en önemli bileşendir. Gizlilik derecesinin doğru kullanımı belge yönetimi süreçlerinin verimli bir şekilde yönetilmesini, hesap verilebilir ve şeffaf bir yönetim anlayışının etkin bir şekilde sürdürülebilmesini ve bilgi edinme taleplerinin doğru bir şekilde karşılanmasını sağlayacaktır. Gizlilik derecesinin yanlış kullanımı (belgenin gereğinden fazla ya da düşük gizlilik derecesiyle sınıflandırılması) ise iş süreçlerinin yoğunluğunun ve maliyetinin artmasına, yerine getirilen faaliyetlerin gecikmesine, güvenlik ve hak ihlallerinin yaşanmasına sebep olabilecektir.

Kamu kurum ve kuruluşları faaliyetlerini şeffaflık ilkesi ile devletin ve vatandaşların güvenliğini sağlayarak yerine getirmektedir. Kurum ve kuruluşlar tarafından oluşturulan bazı belgeler, ulusal güvenliği ve kişisel mahremiyeti etkileyen hassas bilgileri içerebilmektedir. Hassas bilgileri içeren belgelerin korunması, kamu kurum ve kuruluşlarının ulusal ve uluslararası menfaatlerin ve kişisel mahremiyetin sağlanmasındaki rolünün kritik bir parçasını oluşturmaktadır. Türkiye'de gizlilik dereceli belgelerin yönetimi ile ilişkili (doğrudan veya dolaylı olarak) birçok yasal ve idari düzenleme geliştirilmiştir (Arşivlerden Yararlanma Usul…, 2021; Bilgi Edinme Hakkı…, 2003; Cumhurbaşkanlığı Bilgi…, 2019; Cumhurbaşkanlığı Dijital Dönüşüm…, 2020a; Devlet Arşiv Hizmetleri…, 2019; Elektronik İmza Kanunu, 2004; Elektronik Haberleşme Kanunu, 2008; Gizlilik Dereceli Belgelerde…,2022; Gizlilik Dereceli Belgelerde…,2023; Güvenlik Soruşturması…, 2021; Güvenlik Soruşturması…, 2022; Resmi Yazışmalarda…Yönetmelik, 2020). Bu düzenlemeler, gizlilik durumunun gerekçelerini, belgelerin hassasiyetlik durumlarına göre alınacak güvenlik önlemleri amacıyla kullanılacak gizlilik sınıflandırma derecelerini, gizlilik sınıflandırılmasının hangi belgelere uygulanacağını, gizlilik dereceli belge yönetim süreçlerinin nerelerde ve nasıl gerçekleştirileceğini, belgelerin nerelerde ve hangi tedbirler alınarak muhafaza edileceğini, erişim yetki sorumlulukları ve yetkilendirilme gereklilikleri ile bilgi edinme talebine yönelik yapılacak hususları kapsamaktadır. Söz konusu düzenlemeler hassas bilgileri içeren belgelerin bir gizlilik derecesiyle ilişkilendirilerek, gizlilik dereceli belge yönetim süreçlerinin ve alınması gereken özel güvenlik önlemlerinin çerçevesini çizmekte olup, bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelerin (hukuki belgeler ile kişisel bilgileri içeren sağlık belgeleri, eğitim belgeleri, mali belgeler vb.) yönetimi kapsamında sadece bilmesi gereken prensibinin uygulanması gerektiğini belirtmektedir (Gizlilik Dereceli Belgelerde…, 2022, mad. 31).

Hassas bilgileri içeren gizlilik dereceli belgelerin yönetimi, kamu kurum ve kuruluşlarının verimliliği, güvenliği ile yasal ve idari düzenlemelere uyum açısından önemli bir rol oynamaktadır. Gizlilik dereceli belge yönetimi, belgelerin üretilmesini, muhafaza edilmesini, paylaşılmasını, teslim alınmasını, güvenliğinin alınması ile erişim düzenlemelerine yönelik süreçleri kapsamaktadır. Gizlilik dereceli belge yönetiminin önemli bileşenlerinden olan erişim yetkilendirmeleri sayesinde bilgi ve belge ihlallerinin önüne geçilebilmekte ve böylece kurum ve kuruluşlar yasal sorumluluklarını yerine getirebilmektedirler. Kamu kurum ve kuruluşları için gizlilik dereceli belge yönetimi,

stratejik bir öneme sahip olması sebebiyle sistemli ve etkili bir şekilde uygulanması gerekmektedir.

Gizlilik dereceli belge yönetimi politikaları, kamu kurum ve kuruluşlarının hassas bilgilerinin korumasına ve yasal gerekliliklere uygun şekilde yönetmesine yardımcı olmaktadır. Bu politikalar, gizlilik sınıflandırmalarını standartlaştırarak hangi belgelerin nasıl korunacağını belirlemekte ve aynı zamanda belgelerin yalnızca yetkili kişilere erişilebilir olmasını temin ederek güvenliğini sağlamaktadır. Gizlilik dereceli belge yönetimi politikaları ve prosedürleri, kurum ve kuruluşların yasal ve idari düzenlemelere uyumunu sağlamaktadır. Bu bağlamda, doğru politika ve uygulamalarla birlikte, gizlilik dereceli belgelerin güvenli ve etkin bir şekilde yönetilmesi, devletin ve kişilerin güvenliği, güvenilirliği ve hesap verilebilirliği ile bilgi edinme hakkının etkin olarak kullanılması kapsamında kritik bir öneme sahiptir.

Kamu kurum ve kuruluşları tarafından yerine getirilen faaliyetlerin hesap verebilir, adil, etkili ve güvenli bir şekilde gerçekleştirilmesi için gizlilik dereceli belge yönetim süreçlerinin yasal ve idari düzenlemelere uygun olarak gerçekleştirilmesi gerekmektedir (Gizlilik Dereceli Belgelerde…,2023; Gizlilik Dereceli Belgelerde…,2023). Gizlilik dereceli belge yönetimi ulusal ve kişisel gizliliğin korunması için gerekli olan koşulları tanımlarken, bilgiye erişimi sınırlamaktadır. Bu bağlamda, belgelerin doğru gizlilik derecesi ekseninde yönetilmesi önem taşımaktadır. Bu yönetimin ilk ve en temel aşamasını gizlilik sınıflandırma süreci oluşturmaktadır. Belgelerin doğru gizlilik derecesiyle sınıflandırılmasının belge süreçlerinin uygun ortamlarda ilgili güvenlik gerekliliklerinin yerine getirilmesini, gereksiz muhafaza ve güvenlik önlemlerini azaltarak zaman ve kaynakların verimli kullanılmasını sağlayacaktır.

Yasal ve idari düzenlemeler belgelerin gizlilik gerekçeleri ve süreleri ile belgelerin yönetim süreçlerini belirleyen en önemli değişkenlerdir. Gizlilik dereceli belgelerin yönetimi, yasal ve idari düzenlemeler kapsamında belgelerin gizlilik derecesine göre fiziksel ya da elektronik ortamlarda ve farklı güvenlik tedbirlerine göre gerçekleştirilmektedir (Elektronik İmza Kanunu, 2004). Bu sebeple kurum ve kuruluşlarda, gizlilik dereceli belgelerin yönetimi için farklı düzeylerde uygulamaların yapılandırılması gerekmektedir. Hizmete özel gizlilik dereceli belgelerin yönetimi olağanüstü durumlar haricinde sadece elektronik ortamda (EBYS), gizli gizlilik dereceli belgelerin yönetimi gerekli güvenlik önlemleri alınan fiziki ortamlarda ve çok gizli gizlilik

dereceli belgelerin yönetimi ise bu amaçla özel olarak oluşturulmuş Çok Gizli Belge Bürosu koordinatörlüğünde yönetilmesi gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022). Bununla birlikte, elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili olanlar tarafından gerekli güvenlik önlemlerinin alınması şartıyla güvenli e-imza ile onaylanan gizlilik dereceli belgelere yönelik işlemlerin elektronik ortamda yürütülmesi mümkün olabilmektedir (Kamu kurum…, 2010; Resmi Yazışmalarda… Yönetmelik, 2020). Bu bağlamda, gizlilik dereceli belgelerin farklı kamu kurum ve kuruluşlarda, farklı ortamlarda ve güvenlik düzeylerinde yönetilmesi hibrit olarak yürütülecek bir belge yönetimi süreçlerini gerektirmektedir.

Türkiye'de gizlilik dereceli belgelerin yönetimi ile bu belgelerin üretileceği ve muhafaza edileceği ortamlar, gizlilik derecesinin değerlendirilmesi, gizlilik derecesinin düşürülmesi/kaldırılması ile imha edilmesi veya bilgi talebi itirazlarına yönelik aşağıda sunulan birimler görevlendirilmiştir.

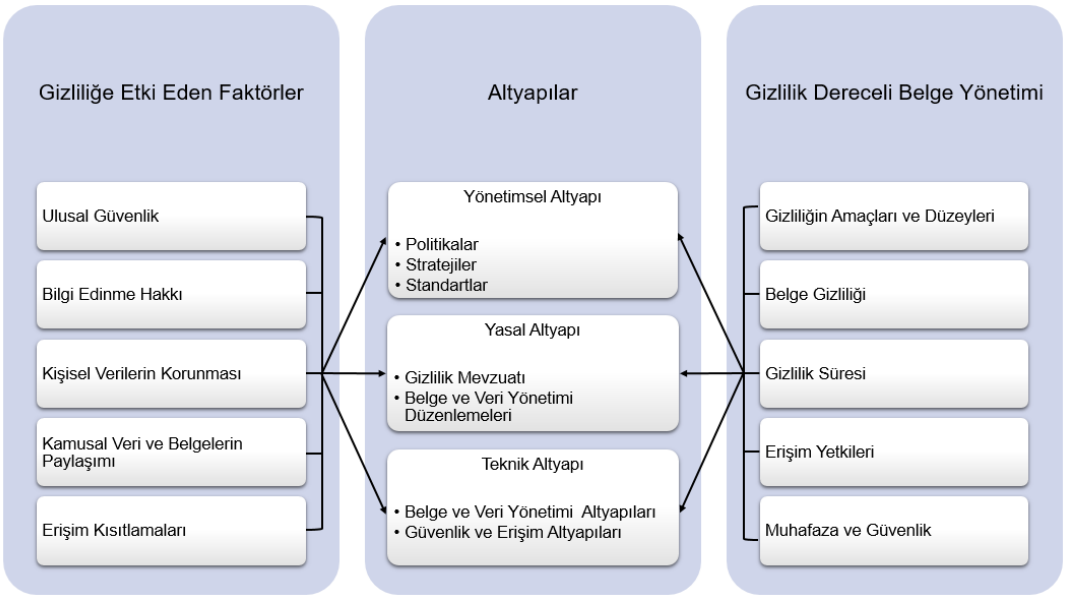
- Gizlilik Dereceli Birimler: Çok gizli ve gizli gizlilik dereceli bilgi ve belgeleri üreten ve koruyan birimler, bilgi işlem birimleri, teftiş ve denetim birimleri, personel birimleri, özel kalem müdürlükleri gizlilik dereceli birimlerdir (Güvenlik Soruşturması…, 2022).
- Gizlilik Dereceli Belgeleri Değerlendirme Komisyonları: Gizlik dereceli belgeleri üreten kurum ve kuruluşları tarafından oluşturulmaktadır (Gizlilik Dereceli Belgelerde…, 2022).
- Arşiv Belgesi Gizlilik Değerlendirme Komisyonu: Devlet Arşivleri Başkanlığı tarafından oluşturulmaktadır (Arşivlerden Yararlanma Usul…, 2021).
- Bilgi Edinme Değerlendirme Kurulu: Adalet Bakanlığı koordinesinde bulunmaktadır (Bilgi Edinme Hakkı…, 2003; Bilgi Edinme Değerlendirme…, 2023a).

Türkiye'de kişisel, kurumsal, ulusal ve uluslararası menfaatlerin korunması kapsamında birçok yasal ve idari düzenleme geliştirilmiş, standartlar kabul edilmiş, projeler yürütülmüştür. Gizlilik dereceli belgeler söz konusu düzenleme, proje ve standartlara uygun olarak yönetilmediğinde, gereğinden az veya fazla gizlilik sınıflandırılması yapılmasına, gizlilik derecesinin gerektirdiği güvenlik önemlerinin alınamamasına, kişisel, kurumsal, ulusal ve uluslararası menfaatlerin zarar görmesine, belge yönetim

süreçlerinin iş yükü ve maliyetin artmasına ve etkinliğinin azalmasına, bilgi edinme hakkının kullanımın engellenmesine sebebiyet verebilmektedir. Bu kapsamda çalışmada, araştırma verilerin analiz edilmesiyle elde edilen bulgular ışığında gizlilik dereceli belge yönetimi çerçevesinin oluşturulması, belge gizliliği ve güvenliğinin sağlanması için etkili politika ve prosedürlerin belirlenmesi, farklı ortamlarda gerçekleştirilen gizlilik dereceli belge yönetim süreçlerine ait gerekliliklerin tespit edilmesi, bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgeleri de kapsayan, kamu kurumlarında özel güvenlik gerektiren belge yönetimine ilişkin bir model önerisinin sunulması amaçlanmıştır. Araştırma sonuçlarının gizlilik dereceli belge yönetimi konusunda kamu kurumlarına değerli bir rehberlik sağlaması umulmaktadır. Ayrıca gerçekleştirilen çalışmanın, kamu kurumlarının mevcut gizlilik dereceli belge yönetimi uygulamalarının iyileştirilmesine, daha etkili gizlilik politikalarının ve prosedürlerinin oluşturulmasına, denetim ve değerlendirme süreçlerinin geliştirilmesine katkıda bulunabileceği düşünülmektedir.

1.2. ARAŞTIRMANIN AMACI, PROBLEMİ VE HİPOTEZİ

Bu araştırmanın amacı, kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimine yönelik hususların belirlenerek, bu konuda bir dizi uygulama önerisi geliştirmektir. Bu bağlamda, çalışma kapsamında geliştirilen araştırma modeli Şekil 1'de gösterilmiştir.



Şekil 1. Araştırma Modeli

Araştırma modeline göre gizlilik süreçleri “gizliliğe etki eden faktörler”, “altyapılar” ve “gizlilik dereceli belge yönetimi” olmak üzere üç temel unsur ve bu unsurlara ait bileşenlerin birbirleriyle ilişkileri çerçevesinde modellenmiştir. Araştırma modelinde belirtilen bu unsurlar:

- Gizliliğe etki eden faktörler: Veri, bilgi ve belgelerin gizliliğine ilişkin kavramsal düzlemde farklı olguların ilişkileri ve birleşimi çerçevesinde bulunmaktadır. Bu kapsamda, gizliliğe etki eden faktörler temel olarak ulusal güvenlik, bilgi edinme hakkı, kişisel verilerin korunması, kamusal veri ve belgelerin paylaşımı ve erişim kısıtlamaları olguları kavramsal düzlemde şekillenmektedir. Bu kavramsal olgular birbirleri ile ilişkili olup, veri, bilgi ve belgelerin gizliliği bilgi edinme hakkının engelleyicisi olabilmektedir.
- Altyapılar: Modelin bu bölümünde, veri, bilgi ve belgelerin gizliliğine ilişkin altyapı süreçleri bulunmaktadır. Yönetimsel altyapılar, kurumsal ve ulusal zeminde gizlilik yönetimine yönelik politikalar, stratejiler ve standartlar oluşturabilecek bileşenlerden oluşmaktadır. Yasal altyapı, veri, bilgi ve belgelerin gizliğinin meşruluğu ile kişilerin bilgi edinme hakkının korunmasına temel olan gizlilik mevzuatı, belge ve veri yönetimi düzenlemeleri bileşenlerinden oluşmaktadır. Teknik Altyapı ise, ulusal ve kurumsal çapta uygulanan belge ve veri yönetimi altyapıları ile güvenlik ve erişim altyapıları bileşenlerinden oluşmaktadır.
- Gizlilik dereceli belge yönetimi: Kamu kurum ve kuruluşlarının faaliyet ve hizmet alanlarıyla ilgili olarak yürüttükleri iş süreçleri ve kurum içi/dışı iletişimlerinde kullandıkları belgeler yetkisiz olarak paylaşıldığında, kişisel mahremiyet ile kurumsal ve ulusal güvenliğe farklı önemlilik düzeylerinde zarar verebilmektedir. Araştırma modelinin bu bölümünün bir bileşeni olan gizlilik amaçları ve düzeyleri, veri, bilgi ve belge bağlamında, kişisel, kurumsal, ulusal ve uluslararası menfaatlerin korunmasına yönelik gizlilik amaçlarının belirlenmesi ve bu amaçlara yönelik gizlilik düzeylerinin oluşturulmasıdır. Belge gizliliği bileşeni, belgelerin belirlenen amaçlar ve gizlilik düzeylerinde güvenliğinin sağlanmasına yönelik ilgili gizlilik derecesiyle ilişkilendirilmesi süreçlerini kapsamaktadır. Gizlilik süresi bileşeni, gizliliğin korunma süresi ve bu gizliliğin güncellenme veya ortadan kaldırılması süreçlerini kapsamaktadır. Erişim yetkileri bileşeni, gizliliğin etkin ve güvenli bir şekilde sürdürülebilmesi amacıyla, bilmesi gereken prensibi (Güvenlik Soruşturması…, 2022, mad. 4)

çerçevesinde kurum, kuruluş ve kişilerin veri, bilgi ve belgelere erişimlerine yönelik ilgili düzenlemeleri içermektedir. Muhafaza ve güvenlik bileşeni, gizlilik dereceli veri, bilgi ve belgelerin nasıl muhafaza edilmesi gerektiği ve bunların güvenliğine yönelik alınması gereken tedbirlerin neler olduğunu ortaya koymaktadır.

Araştırmanın modeli ve amaçları doğrultusunda çalışmanın problemi "*Türkiye'deki kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimi konusunda yasal ve idari düzenlemelerin sadece gizlilik dereceli belgelere odaklandığı, gizlilik sınıflandırılması yapılmayan ancak özel güvenlik gerektiren belgeler için standart uygulama ve politikaların eksikliği bilgi güvenliği açısından potansiyel bir zafiyete sebep olabilecektir*" şeklinde belirlenmiştir.

Araştırmanın problemi doğrultusunda oluşturulan temel araştırma sorusu; kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimi nasıl yapılmalıdır? Çalışmanın temel sorusu bağlamında aşağıdaki alt araştırma sorularına yanıt aranacaktır:

- Gizlilik sınıflandırılmasının farklı düzeylerde yapılmasının amacı nedir?
- Hangi makam ya da kişiler gizlilik sınıflandırması yapmaya yetkilidir?
- Gizlilik dereceli belgelere nasıl erişim sağlanmaktadır?
- Gizlilik sınıflandırılması yapılan belgelerin gizliliği ne zamana kadar korunmaktadır?
- Gizlilik derecesinin düşürülmesi, kaldırılması veya belgenin imha edilmesi kararı hangi makam ya da kişiler tarafından verilmektedir?
- Gizlilik dereceli belgelerin yönetimi kapsamında hangi yapılar oluşturulmuştur?
- Gizlilik belgelerin yönetim süreçleri hangi ortamlarda yapılmaktadır?

Araştırma problemi ve soruları kapsamında araştırmanın temel hipotezi "*Türkiye'de, kamu kurumlarında kamusal bilgi ve veri yönetimi politikaları çerçevesinde özel güvenlik gerektiren belgelerin yönetimine dönük bütünsel (holistic) politikalar oluşturulmadığı için ilgili belge serilerine dönük gizlilik derecelerinin tanımlanması, bu belgelerin düzenlenmesi, kullanımı, arşivlenmesi, korunması ve süreçlerde teknolojik araçların kullanımında belirsizlikler yaşanmaktadır"* şeklinde oluşturulmuştur. Bu hipotez bağlamında oluşturulan alt hipotezler aşağıda yer almaktadır.

- Veri, bilgi ve belgelere yönelik yapılan gizlilik sınıflandırılması, ulusal güvenlik ve uluslararası menfaatler ile kişisel mahremiyetin korunması amacıyla yetkisiz erişimin engellenmesi ile ilgili düzenlemeler yetersizdir.
- Gizlilik sınıflandırılmasının yapılması ve personelin erişim yetkilendirilmesi sürecindeki tutarsızlıkların önüne geçilebilmesi için belgeyi üreten birim düzeyinde tüm kurumsal yapılarda süreçlerin tanımlanması, gizlilik düzeylerine göre kişi ve makamların yetkilendirmelerinin yapılması gerekmektedir.
- Uygulamada gizlilik sınıflandırılması yapılan belgelerin gizliliğinin en fazla ne kadar süre devam edeceği belirsizdir.
- Türkiye'de, belgelerin gizlilik derecesinin düşürülmesi, kaldırılması veya belgenin imha edilmesine yönelik, belgeyi oluşturan kamu kurumunu merkeze alan bir politika bulunmaktadır.
- Gizlilik dereceli belgelerin yönetimi ile gizlilik dereceli arşiv belgelerinin gizliliğinin kaldırılması ve bilgi edinme hakkının kullanılması kapsamında, ulusal boyutta bir koordinasyon kurulu oluşturulmamıştır.
- Gizlilik dereceli belgelerin yönetim süreçlerinin gizlilik derecesinin gerektirdiği farklı ortamlarda ve güvenlik önlemleriyle yapılmasına dönük hibrit belge yönetim uygulamaların geliştirilmesi gerekmektedir.

1.3. ARAŞTIRMANIN YÖNTEMİ VE KAPSAMI

Araştırmada kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimine ilişkin yaklaşımları tespit edebilmek, araştırmanın hipotezlerine yönelik analizleri yapabilmek için betimleme yöntemi kullanılmıştır. Betimleme yöntemi, analiz edilen olayın, vaziyetin, gerekliliklerin ne olduğunu veya bunların özelliklerini belirten ya da tanımlayan incelemelerdir (Kaptan, 1995, s.59). Bu bağlamda, araştırmanın kapsamını oluşturan konu alanlarının temel özellikleri ve araştırmaya temel oluşturan olgular elde edilen verilerle betimlenerek ifade edilmek istenilen hususların anlaşılması amaçlanmıştır (Arıkan, 2013, s. 27).

Araştırma verileri doküman analizi tekniği ile toplanmıştır. Belgesel tarama olarak da bilenen doküman analizi tekniği (Sak ve diğerleri, 2021, s. 230) belirlenen bir hedefe ulaşmak için kayıt ve belgelerin bulunması, okunması, incelenerek verilerin toplanması, not alınması ve değerlendirilmesi süreçlerini kapsamaktadır (Karasar, 2015, s. 183). Doküman analizi tekniği, daha önceden oluşturulmuş kaynak ve belgelerin sistemli

olarak incelenmesi ve değerlendirilmesiyle araştırma verilerinin toplanması sürecidir (Bayter, 2023, s. 69). Literatür araştırmasına dayanan çalışmalarda kullanılan bu teknikle, araştırmanın amacına uygun olarak belge türleri ve kaynaklar belirlenmiş, belirlenen kaynaklardan uygun olan belgeler seçilmiş ve seçilen belgeler çözümlenerek araştırma verileri toplanmıştır (Akgün ve Çiçek, 2022; Bayter, 2022; Cırıkoğlu, 2023; Değer, 2021; Öztürk, 2021; Şenay ve Güneş, 2021). Araştırma amacına yönelik durum veya durumlar hakkında bilgilere sahip olan belge ve kayıtlardan veri elde edilebilmesini mümkün kılan doküman analizi tekniği, birbirleriyle ilişkili olan ve peşi sıra gerçekleştirilen iki tekniği içermektedir (Ekici, 2021, s. 4). Bunlardan ilki, araştırma konusunun haritalandırılmasına, mevcut durumun tematik ve tarihsel perspektifleriyle değerlendirilmesine olanak sağlayan literatür taraması tekniğidir (Köroğlu, 2015, s. 61). İkincisi olan içerik analizi tekniği ise "*belli bir metnin, kitabın, belgenin belli özelliklerini sayısallaştırarak belirleme amacına hizmet etmektedir*" (Hasar, 2017).

Araştırmanın amacını gerçekleştirmek maksadıyla, Türkiye Cumhuriyeti'nde yürürlükte bulunan yasal ve idari düzenlemeler, ulusal ve uluslararası standartlar, kamu kurumları oluşturulan rehberler araştırmanın veri kaynağı olarak kullanılmıştır. Veri, bilgi ve belgelerin gizliliği ve bunların yönetim süreçlerinin güvenliği ile doğrudan veya dolaylı olarak ilişkili olan araştırma belgelerini elde etmek maksadıyla;

- T.C. Mevzuat Bilgi Sistemi Arama Motorunda içerek kriteri düzeyinde "Gizli", "Devlet Sırrı", "Mahremiyet", "Gizli Veri", "Gizli Bilgi" ve "Gizli Belge" anahtar kelimeleri kullanılarak tarama yapılmıştır. Yapılan taramada toplam 1862 adet belgeye ulaşılmıştır. Veri, bilgi ve belgelerin gizlik nedeni, gizlilik sınıflandırması ile bunların yönetim ve güvenlik süreçlerini içermeyen belgelerin elenmesi sonucunda 17 adet yasal ve idari düzenleme,
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından oluşturulan 1 adet rehber,
- Ulaşılabilir nitelikte olan ve içeriği hakkında bilgi sahibini olunabilen toplam 10 adet ulusal ve uluslararası standart araştırma kapsamında yer almıştır.

Araştırma kapsamında bulunan belgelerden içerik analizi tekniği ile sağlanan kamu kurumlarında gizlilik süreçlerine ilişkin veriler, geliştirilen yöntem ve kategoriler kullanılarak sayısallaştırılmıştır. Araştırma verilerin sayısallaştırılması yapılırken önceden belirlenen kategorilerin belgede olup olmadığı dikkate alınmaktadır (Sak ve

diğerleri, 2021, s. 237). Belgelerden sistematik olarak veri elde edilmesi, verilerin bu sistematik yapı içerisinde değerlendirilmesi amacıyla geliştirilen, 3 bileşen ve 13 kategori ve 68 kavramdan oluşan yöntem Tablo 1'de sunulmuştur.

Tablo 1. Araştırmanın Amacı Kapsamında Geliştirilen Veri Elde Yöntemi

Bileşenler	**Kategoriler**	**Kavramlar**	**Kavram Sayısı**
Gizlilik Süreçleri	Gizlilik nedenleri	Gizli, devlet sırrı, kişisel veri, mahremiyet, ulusal güvenlik, ulusal menfaat vb.	7
	Gizlilik sınıflandırma düzeyleri	Gizlilik derecesi, çok gizli, hizmete özel, özel ve tasnif dışı vb.	10
	Sınıflandırılabilecek veri, bilgi ve belge türleri	Harp planı, istihbarat, istihbari faaliyet, milli teknoloji vb.	6
	Sınıflandırma yetkileri	Üst yönetici, birim yöneticisi vb.	3
	Gizlilik süresi	Gizlilik süresi, süreli gizlilik vb.	3
	Gizliliğinin değerlendirilmesi	Gizliliğin düşürülmesi, gizliliğin kaldırılması vb.	3
Gizlilik Dereceli Belgelerin Yönetimi	Gizlilik dereceli belgelerin yönetimiyle ilişkili yapılar	Gizlilik dereceli birim, çok gizli belge bürosu, değerlendirme komisyonu vb.	5
	Gizlilik dereceli belge süreçleri	Belgenin oluşturulması, gönderilmesi, havale edilmesi, çoğaltılması vb.	8
	Belge süreçlerinin gerçekleştirileceği ortamlar	Fiziki ortam, elektronik ortam	2
Güvenlik Önlemleri	Belge güvenliği	Güvenlik önlemi, güvenlik tedbiri, belge ihlali, ağ bağlantısız ortam vb.	6
	Fiziksel güvenlik	Doğal afet, yangın, su baskını, hayvan zararı vb.	6
	Personel güvenliği/güvenirliliği	Arşiv araştırması, güvenlik soruşturması, gizlilik sözleşmesi vb.	4
	Teknoloji güvenliği	Bilgisayar, yazılım, sunucu	5

Tablo 1'de gösterilen gizlilik süreçleri, gizlilik dereceli belgelerin yönetimi ve güvenlik önlemleri bileşenleri farklı süreçleri içermekle birlikte, bu bileşenler birbirleriyle ilişkilidir. Dolayısıyla bu bileşenlerin kavramları arasında net bir sınır bulunmamaktadır. Bu kavramların araştırma belgelerinde geçme durumları ve ifade edilmiş biçimleri

incelenmiştir. Bu bağlamda sağlanan veriler, yöntem kapsamında belirlenen kategoriler çerçevesinde sunulmuştur. Bu kapsamda aşağıda ifade edilen yol izlenmiştir.

- Araştırma belgelerinin her birine bir kod verilmiştir. Örneğin, 651 Sayılı Devlet Memurları Kanunu (1965) için Kanun-1, Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik (2021) için Yönerge-1 belge kodu kullanılmıştır.
- Araştırma belgelerinin her biri satırda, kategori ve kavramlar sütunlarda olacak şekilde Excel dosyası oluşturulmuştur.
- Araştırma belgelerinde geçen kavram ve bu kavramların belirlenen kategoriler için anlam ifade edilip etmediği incelenmiş ve Excel dosyasına işlenmiştir. Araştırma belgesinde geçen fakat kategorilere ilişkili olmayan içermeyen kavramlar yok sayılmıştır.
- Bu yöntemle sağlanan araştırma verilerinin belge özelinde bulunup bulunmadığı oluşturulan tablolarda kategori sütunlarında gösterilmiştir. Sonrasında kategorilerde bulunan olgular belgelerde ifade edildiği şekilde açıklanmıştır.

1.4. ARAŞTIRMANIN DÜZENİ

Bu araştırma toplam sekiz bölümden oluşmaktadır. İlk bölümde araştırma konusunun önemine ve sorularına, araştırmanın amacı, yöntemi, kapsamı ve düzeni ile araştırmada yararlanılan kaynaklar hakkında bilgilere yer verilmiştir.

İkinci bölümde kamu kurum ve kuruluşlarına ait veri, bilgi ve belgelerin varlık bulduğu bilgi sistemleri, kurumsal içerik yönetim sistemleri, belge yönetimi ve elektronik belge yönetimi uygulamalarının yapıları, işlevleri, bileşenleri ve kullanım alanları ele alınmıştır.

Üçüncü bölümde kamu kurum ve kuruluşları tarafından gerçekleştirilen faaliyetler ile kurumsal kararın alınmasında önemli rol oynayan verilerin kullanım amaçları ile yapısal ve karakteristik özellikleri kapsamında sınıflandırma tanımlamaları açıklanmış ve veri yönetiminin çerçevesi ortaya konulmuştur. Bu bölümde ayrıca, veri yönetiminin devamlı olarak iyileştirilmesine yönelik mevcut yeteneklerin ölçülerek güçlü ve zayıf yönlerin değerlendirilmesi kapsamında veri yönetimi olgunluk modelleri incelenmiştir.

Dördüncü bölümde gizlilik ve mahremiyet kavramları odağında veri, bilgi ve belge yönetimine ilişkin ulusal ve uluslararası standartlar, yasal ve idari düzenlemeler ile projelere yer verilmiştir. Ayrıca kamu kurum ve kuruluşlarının bu standartlara ve mevzuata uyum sağlama süreçleri, yürütülen projelerin amaçları, kapsamı ve sonuçları ele alınmıştır.

Beşinci bölümde ABD'de ve Türkiye'de gizlilik dereceli belge yönetim uygulamaları ile bu amaçla oluşturulmuş yapılar incelenerek, gizlilik gereklilikleri, gizlilik derecelerinin seviyeleri, gizliğin süresi gibi olgular ile gizlilik dereceli belge yönetim süreçlerinin (üretme, muhafaza etme, gönderme, teslim alma, çoğaltma, imha etme vb.) hangi ortamlarda ve nasıl gerçekleştirildiği ortaya konulmuştur.

Altıncı bölümde araştırma kapsamında doküman analizi tekniğiyle elde edilen araştırma verilerin analizlerine ilişkin bulgulara ve değerlendirmelere yer verilmiştir.

Yedinci bölümde araştırma çerçevesinde incelenen konular ve yapılan analizler doğrultusunda kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimine ilişkin bir model önerisi kapsamında değerlendirilmiştir.

Sekizinci bölümde ise araştırmanın sonuçları ile Türkiye'de özel güvenlik gerektiren belge uygulamalarına yönelik geliştirilen önerilere yer verilmiştir.

Bu araştırma, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre düzenlenmiştir. Kaynak gösterme biçimi olarak APA 7 kullanılmıştır.

1.5. ARAŞTIRMADA YARARLANILAN KAYNAKLAR

Araştırmanın kurumsal çerçevesinin oluşturulması ve amacının gerçekleştirilmesi için yapılan literatür taramasında aşağıda listelenen arama motorları ve bilgi kaynaklarından yararlanılmıştır.

Hacettepe Üniversite Kütüphanesi Kataloğu
Google Akademik Veritabanı
Proquest Veritabanı
Scopus Veritabanı
TR Dizin Veritabanı

Web Archive Veritabanı
Web Of Science Veritabanı
Ebsco Discovery
Dergi Park
Bilgi Dünyası Dergisi
Library Management Dergisi
Türk Kütüphaneciliği Dergisi
T.C. Mevzuat Bilgi Sistemi Kataloğu
YÖK Tez Kataloğu

Araştırma çerçevesinde yapılan literatür taramasına ilave olarak kamu kurumlarının kurumsal web sayfaları da incelenmiştir. Gerçekleştirilen taramalarda kullanılan anahtar kelimeler aşağıda sunulmuştur.

Devlet Sırrı (State Secret)
Gizlilik (Confidentiality)
Mahremiyet (Privacy)
Ulusal Güvenlik (National Security)
Gizlilik Sınıflandırması (Security Classification)
Gizli Veri (Secret Data)
Gizli Bilgi (Secret Information)
Gizli Belge (Secret Records)
Veri Yönetimi (Data Management)
Belge Yönetimi (Records Management)

2. BÖLÜM

KAMU KURUMLARINDA BİLGİ SİSTEMLERİ VE BELGE YÖNETİMİ

2.1. KURUMSAL BİLGİ SİSTEMLERİ

Bilgi ve iletişim teknolojisinde yaşanan gelişmeler ile birlikte, bilginin elde edilmesi, işlenmesi ve paylaşılması eskiye oranla daha kolay ve hızlı bir şekilde gerçekleştirilmektedir. Bu değişim, iş süreçlerini ve şekillerini, ürünlerin ve hizmetlerin niteliklerini, tüketicilerin beklentilerini ve sonuç olarak kurumların bilgiyi yönetme yapısını değiştirmiştir. Kurumlar, faaliyet alanlarıyla ilgili iş süreçlerini bilgi teknolojileri çerçevesindeki altyapılarla ve bunların efektif kullanımıyla yerine getirmektedir (Külcü ve diğerleri, 2015, s. 25). Bilgi sistemlerinin insanlara ve kurumlara sağladığı imkan ve kabiliyetlerin yanı sıra literatürde farklı tanımları bulunmakta olup, bu tanımlar Tablo 2'de gösterilmiştir.

Tablo 2. Bilgi Sistemi Tanımları

Yazar/Yazarlar	Tanım
Alberghini ve diğerleri (2014, s. 164)	Kurumlar ve karar destek mekanizmaları için önemli olan bilişim yönetim sistemlerinin bir çeşididir.
Ehie ve Madsen (2005)	Kurumların iş süreçlerinin entegre edilmesi, kurum içerisinde ve kurum paydaşları arasında bilgi paylaşımının yapılması için stratejik bir araçtır.
Mesquita ve diğerleri (2013, s. 1291)	Kurumsal kaynak planlamanın (ERP) süreçlerini optimize etmenin yolu olarak, kurumlar tarafından uygulanan entegre yönetim sistemleridir.
Özata ve Sevinç (2011, s. 25)	Kişiler arasında bilginin aktarılma aracı veya kurumların kullanabileceği bir biçimde verilerin bilgiye dönüştürülmesi ve aktarılmasını sağlayan bir sistemdir.

Stair ve Reynolds (2005, s. 4)	Hedeflere ulaşmak için otonomi mekanizmaları elde etmek amacıyla veri ve bilgileri toplayan, işleyen ve yayan, birbiriyle ilişkili bir dizi bileşendir.
Turban ve diğerleri (2008, s. 17)	Özel bir gereksinim maksadıyla bilginin toplanması, işlenmesi, depolanması, analiz edilmesi ve dağıtılması sürecini kapsayan sistem olarak tanımlanmakla birlikte, bilgi sistemlerine girdi olan veri ve bilgiler işlenerek diğer sistemlerce kullanılabilecek çıktılar üretmektedirler.

Yukarıda ifade edilen tanımlar çerçevesinde, bilgi sisteminin; iş süreçlerinin yerine getirilmesi, kurum içi ve dışı paydaşlar ile bilgi alışverişinin yapılması, karar destek ihtiyacının karşılanması için veri ve bilgilerin sağlanması, depolanması, işlenmesi, anlamlı hale getirilmesi, paylaşılması ve gerektiğinde bulunabilmesi maksadıyla oluşturulan sistematik araç olduğu söylenebilir.

Bilgi sisteminin, işlenmemiş veri veya bilgiyi içerisine alan ve dönüşüm süreçleri sonrasında ürün olarak bilgiyi ortaya çıkaran bir sistem olduğu dikkate alındığında, bir bilgi sistemi kuruluş ve kuruluşun çevresi ile ilgili şu işlevsel unsurlardan oluşmaktadır (Adeoti-Adekeye, 1997, s. 321):

- Algı: Üretilen veya elde edilen verilerin kuruluşa ilk girişinin yapılması.
- Kayıt: Verilerin fiziksel olarak kaydedilmesi.
- İşleme: Kuruluşun belirli gereksinimlerine göre bilginin dönüştürülmesi.
- Aktarma: Bilginin kuruluş içerisinde veya dış paydaşlara iletimi.
- Depolama: Bilginin gelecekteki kullanımı kapsamında depolanması.
- Geri Çağırma: Kaydedilen verilerin aranması.
- Sunum: Gereksinim duyulan bilgilerin ilgili paydaşlara iletimi ve rapor oluşturulması.
- Karar Verme: Kuruluşun tüm personelin alacağı kararlara destek sağlanması.

Çeşitli hizmet alanlarında faaliyet gösteren kuruluşların, farklı çalışma biçimleri ve iş süreçlerinin çeşidine bağlı olarak farklı özellikte bilgilere ihtiyaç duyması, kuruluş genelinde değişik özelliklerde bilgi sistemlerinin kurulmasına sebep olmaktadır (Özata

ve Sevinç, 2011, s. 36). Bu bağlamda kurumsal bir yönetiminin gerçekleşmesine imkân sağlayan bilgi sistemleri Şekil 2'de gösterilmektedir.

Şekil 2. Kurumsal Bilgi Sistemleri (Karagül, 2006, ss. 21-34; Külcü ve diğerleri, 2015, s. 25)

Kurumsal bilgi sistemleri, bilginin kuruluş geneline dağıtılmasını ve birimlerin bilgi ihtiyaçlarının arzu edilen biçimde sunulmasının önemli yardımcıları (Çevre ve Orman Bakanlığı, 2009, s.11) olmakla birlikte, küreselleşen ekonomide kuruluşlara önemli bir rekaket avantajı sağlamaktadır (Watson, 2007, p. 77). Bu bağlamda, bilgi sistemlerinin ihtiyaç duyulan türde bilgiyi doğru olarak üretmesi, kurumsal bilgiye hızlı bir şekilde erişim sağlaması, stratejik, yönetimsel ve karar verme süreçlerinde performans ve zaman kazanımını artırması ve iş süreçlerine ait maliyetleri azaltma yeteneği bu sistemlerin kurumlar tarafından kullanılma gerekçeleri olarak gösterilebilir.

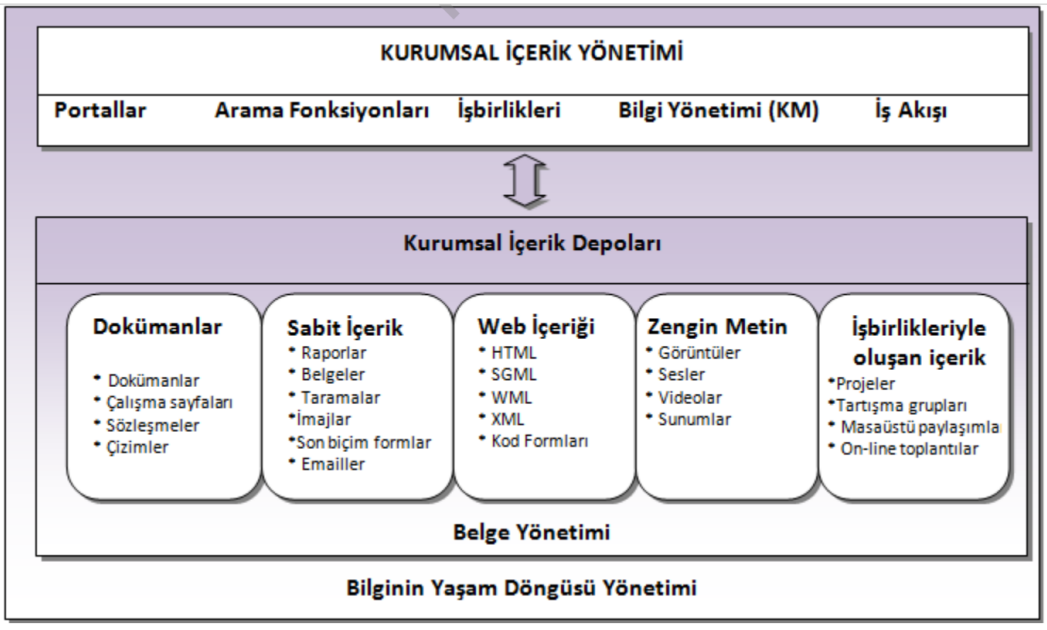
2.2. KURUMSAL İÇERİK YÖNETİMİ

Kurumlar, sahip oldukları altyapı, kaynak ve teknoloji imkânları vasıtasıyla içerik üreterek kurumsal bilginin hacmini artırmaktadırlar. Söz konusu içeriğin yönetilmesine ilişkin uygulamalar kurumsal içerik yönetimi (KİY) olarak tanımlanmaktadır (Külcü ve diğerleri, 2015, s. 29). Kurumsal içerik yönetimi (Enterprise Content Management-

ECM) terimi ilk defa 2000 yılında AIIM (the Association for Intelligent Information Management) tarafından yapılmıştır (Franks, 2013, s.35).

KİY, kurum ve kurum paydaşlarınca kullanılacak bilgilerin sistematik olarak toplanması ve düzenlenmesi olarak ifade edilebilmekle birlikte, yaşam döngüsü çerçevesinde temel kurumsal süreçleri destekleyen bilgilerin elde edilmesi ve sağlanması, depolanması, yönetilmesi, korunması ve sunulması için kullanılan araç, yöntem ve stratejilerin dinamik bir bileşimidir (AIIM, 2023a). Söz konusu bileşenler, kurumsal bilgi sistemlerinde bulunan unsurların tümleşik bir yapıdan yönetimini sağlamakta ve iş süreçlerinde kullanıcıların etkinliğini artırmaktadır (Külcü ve diğerleri, 2015, s. 32).

KİY, yazılım kodlarının, kurumsal bilginin (yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış) ve üst veri öğelerinin yönetimi ile mevcut içeriğin yayınlanması, saklanması, dağıtımı ve kurumsal gayelerde kullanımına ilişkin çözümleri tanımlamaktadır (Külcü, 2010, s.309). KİY sistemleri, kağıt belgeler, elektronik formlar ve e-postalar ile anlık mesajlar, metin belgeleri ve elektronik tablolar gibi yapılandırılmamış elektronik veriler dahil olmak üzere çeşitli biçimlerdeki içeriğin tüm yaşam döngüsünü yönetmektedir (Franks, 2013, s.36). Bu bağlamda, KİY uygulamaları farklı katmanlardan meydana gelen bir yapı olduğu söylenebilir (Alsup, 2004, s. 5). KİY uygulama ve katmanlı yapısı Şekil 3'de gösterilmiştir.



Şekil 3. Kurumsal İçerik Yönetimi Yapısı (Alsup, 2004, s. 5; Külcü ve diğerleri, 2015, s. 30)

KİY yapısı, bilgi yaşam döngüsü yönetimi prensiplerine dayanan bilgi yönetimi prosedürlerinin temel aldığı üç ana katmandan oluşmaktadır. İş akışı, arama fonksiyonları, işbirlikleri, portallar ve bilgi yönetimi uygulamalarının kullanılmasıyla kurumsal içerik depolarında bulunan bilgi varlıkları kullanıcıya iletilmektedir. Kurumsal içerik depolarında bulunan içerik öğeleri KİY tarafından teknik uygulamalar ile bütünleştirilerek kullanıcıya aktarılmaktadır (Külcü ve diğerleri, 2015, s. 30). KİY uygulamaları kapsamında bulunan kurumsal bilgi sistemlerinin genel hatları aşağıda çizilmiştir.

- Web İçerik Yönetimi: Web içerik yönetimi, web sayfalarında içerik oluşturmak, yönetmek, depolamak ve görüntülemek için kullanılmaktır. İçerik çoğunlukla bir veri tabanında tutulmakta ve XML gibi esnek bir dil kullanılarak birleştirilmektedir. Bir web içerik yönetim sisteminin temel özelliklerini; ilgili ve güncel içeriğe verimli ve etkili erişim sağlamak için web siteleri tasarlama ve düzenleme becerisi, web sitesinde yayınlanmadan önce içerik değerlendirmesinin ve onayının düzenlenmesi ve kontrol edilmesi dahil olmak üzere içeriği yayın için kontrol etme ve hazırlama becerisi ve yayınlama sürecinin önemli bölümlerinin otomasyonu oluşturmaktadır (AIIM, 2023c). Web içerik yönetimi, kuruma ait doküman ve bilgilerinin web sayfalarında oluşturulması, yayınlanması ve yönetimi süreçlerini kapsamakla birlikte kurumsal amaçlar çerçevesinde çok yönlü olarak kullanılabilmektedir (Külcü ve diğerleri, 2015, s. 32).
- Doküman Yönetimi**:** Kurumsal içerik unsurlarından biri olarak yoğunlukla kullanılan dokümanlar, kurumların iş süreçlerin oluşturduğu standartlar, teknik raporlar, eğitim notları gibi dokümanlardan oluşmaktadır. Dokümanlar, kurumsal süreçlerde delil özelliği taşıması sebebiyle çoğunlukla doküman yönetim sistemleriyle yönetilmektedir. Doküman yönetim sistemleri, dokümanların yaşam döngüleri boyunca izin verme, üst veri hizmetleri, arama, versiyon kontrolü, yol bulma, dizinleme vb. işlemleri gerçekleştirmektedir (Jenkins ve diğerleri, 2005, s.24; Külcü ve diğerleri, 2015, s.33; O'Callaghan ve Smiths, 2005).
- Belge Yönetimi: Belgeler, kurumsal faaliyetlerde ve iş süreçlerinde üretilen, kanıt özelliğine sahip olan bilgi varlıklardır. Kurumsal iletişimin temelini oluşturulan belgeler, resmi işlemlerin ve kurum içi/dışı yazışmalarını yerine getiren önemli unsurlardır. Bilgi ve iletişimin teknolojisinde yaşanan gelişmeler

ve kurumsal yapıların buna evrilmesiyle birlikte belgeler elektronik olarak üretilmekte ve yönetilmektedir. KİY çerçevesinde elektronik belgelerin yönetimi, belgelerin yaşam döngüsü çerçevesinde yapılmaktadır (Külcü ve diğerleri, 2015, s.33).

- E-posta Yönetimi: Bilgi ve iletişim teknolojisindeki gelişmeler ile birlikte e-postalar kurumsal iletişimin en önemli unsuru haline gelmiştir. Kurumsal iletişimin büyük birçoğunun e-postalar ile yapılması sebebiyle, e-posta uygulamasının en önemli bilgi yönetim sistemlerinden biri olduğu söylenmektedir (Stephens ve Wallece, 2003). E-posta yönetimi, kurum tarafından gönderilen ve alınan elektronik iletilerin nitelik ve niceliğinin sistematik bir şekilde kontrolünü içermektedir (AIMM, 2023d). Kurumların KİY uygulamaları çerçevesinde artarak önemli hale gelen e-postaların yönetimine ilişkin, elektronik postaların kurumsal iş akışlarında depolanması, uzun vadeli saklanması ve imha edilmesi işlemlerini içeren uygulamalar bulunmaktadır (Külcü ve diğerleri, 2015, s.33).
- Dijital Varlık Yönetimi: Kurumların faaliyetlerinde ve iş süreçlerinde üretilen veya sağlanan doküman ve belgelerin haricinde, fotoğraf, video gibi görsel ortamlarla birlikte elektronik ortamlarda bulunan diğer unsurlar kurumların dijital varlıklarını oluşturmaktadır (Wilkoff ve diğerleri, 2001). Gelişen bilgi ve iletişim teknolojisiyle birlikte kurumlarda bulunan dijital varlıkların sayısı giderek artmakta ve bu sebeple söz konusu varlıkların sistemli bir şekilde yönetilmesine ihtiyaç duyulmaktadır. Dijital varlık yönetimi, dijital varlıkların izlenmesi, dijitalleştirilmesi ve depolanması süreçlerini içermektedir (Çakmak ve Özel, 2013). Bununla birlikte, dijital içerik ve üst veri, kurallar, haklar, izinler ve teknik altyapı dijital varlık yönetiminin unsurları arasında bulunmaktadır (İnceoğlu ve Şentürk, 2014, s.363).
- İş Akışı ve İş Süreçleri Yönetimi: İş akışı, kurumsal faaliyetlerin yapılan bir planlama ve belirli bir düzen çerçevesinde yeri getirilmesidir. İş akışları, kurumsal faaliyetlerin çoğunlukla ihtiyaç duyduğu transfer işlemleri ve belge işlemleri gibi süreçlerde kullanılmaktadır (Günay, 2018, s.115). İş süreci ise kurum personeli ile içerik öğeleri arasındaki ilişkiyi sağlayan unsurlardır. İş süreçleri yönetimi, personelinin ortak çalışmalarına ilişkin yapılandırılmamış ve yapılandırılmış ortamların yaratılması ve personelin içerik unsurları ile etkileşim halinde olmasını temin eden bir yapıdır (Jenkins ve diğerleri, 2005, s.24; Külcü, 2015, s.33).

2.3. BELGE YÖNETİMİ

Belge, genel manada, kayıt altına alınmamış sözlü ifaden farklı olarak, kayıt altına alınan bilginin herhangi bir formu, tüzel kuruluş ya da kişiler tarafından üretilen ve paylaşılması gerekli olan bilgi olarak tanımlanabilmektedir (Diamond, 1995, s.2; Külcü, 2018, s. 21). Belge, kurumsal veya bireysel görevlerin gerçekleştirilmesi maksadıyla alınan ya da söz konusu görevlerin gerçekleştirilmesiyle üretilmiş olan ve içerik, ilişki ve yapısıyla bahse konu işlev için delil oluşturan kayıtlı bilgidir (TS 13298, 2015). Belge, kurumlarda resmi iletişimi ve kurum içi bilgi paylaşımını kolaylaştıran, geçmiş uygulamaları aydınlatan, yasal/idari inceleme ve onaylama prosedürlerine yönelik delil sağlayan ve yönetim tercihleri için gerekli bilgileri tutan, önceden belirlenmiş biçim ve içerikteki belgesel kaynaklardır (Külcü ve diğerleri, 2015, s.1). Bu bağlamda belgeler, kurumsal yapıların en değerli bilgi varlıklarındandır (Torunlar ve Özdemirci, 2019, s. 139).

Belgeler hangi formatta (kağıt, kartografik, optik veya elektronik) üretilirse üretilsin, önemli olan belgelerin oluşturulma amaçlarına uygun kullanım imkanlarına haiz olması ve kanıt özelliğini koruyabilmesidir (Külcü, 2018, s. 21). Kişi veya kuruluşlar tarafından yapılan işlemlerin hukuki sonuçlara sebebiyet verme ihtimali kapsamında, belgelerin söz konusu kanıt özelliği bir ispat aracı olarak görülmektedir (Çiçek, 2015, s.44). Bununla birlikte, belgelerin kağıt veya elektronik olarak varlık bulması hesap verilebilirlik yükümlüğünü değiştirmemektedir (Franks, 2013, s.32). Kurumların iş süreçlerini gerçekleştirebilmeleri için üretilen belgeler, kurumun geçmiş faaliyetlerinin incelenmesi kapsamında kullanılan temel varlıklardır. Yukarıdaki tanımlardan da anlaşılacağı üzere, belgenin iki temel özelliği bulunmaktadır. Bunlardan ilki belgenin kanıt niteliğine sahip olması, diğeri ise belgenin kurumsal iletişim ve karar alma süreçlerinde bilgi kaynağı olmasıdır. Kurumların faaliyet alanları ve iş süreçleri kapsamında üretilen belgeler; yazışma, rapor, talimat ve form yapılarında vücut bulmaktadırlar (Külcü, 2018, s.33).

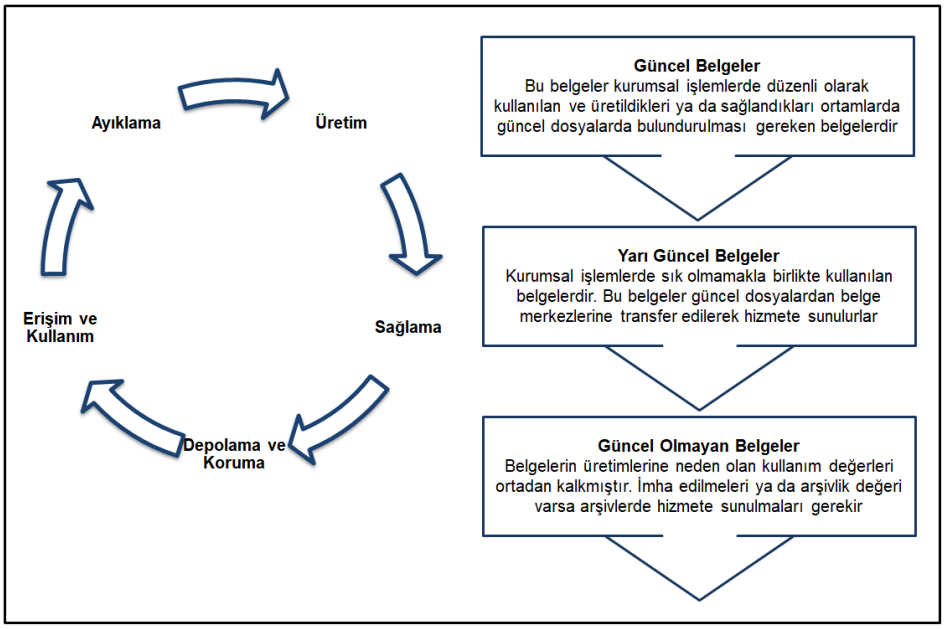
Kurumsal faaliyetlerin organik bir parçası olan belgeler, iş sürekliliği, iş verimliliği, hesap verilebilirlik ve risk yönetimi uygulamalarının temel bilgi ve iletişim kaynağını oluşturmaktadır. Bu sebeple, kurumların ihtiyaçlarına dayalı bir belge politikası ve hedeflerinin belirlenerek uygulaması gerekmektedir. Söz konusu belge politikası ve hedeflerin uygulanması, iş faaliyetleri hakkında yetkili ve doğru bilgilerin üretilmesi, bu

bilgilere ait kanıtlarının geliştirilmesi, yönetilmesi ve gerekli olduğu sürece ihtiyaç duyanlar için erişilebilir olmasını mümkün kılmaktadır (ISO 30301, 2019).

Günümüzde belge yönetimi çözümleri, kurumlarda oluşturulan bilgi kaynaklarının çoğunu yönetmektedir (Odabaş, 2008, s.122). Belge yönetimi, kuruluşların faaliyetlerinin ve işlemlerinin bir kanıtı olarak bilgilerin oluşturulması, kullanımı, bakımı, dağıtımı ve imha edilmesinin sistematik olarak sürdürülmesi için yerine getirilmesi gereken faaliyetleri ifade etmektedir (Özdemirci, 1999). Uluslararası Belge Yönetim Standardı (ISO 15489-1, 2016) belge yönetimini "*iş faaliyetleri ve işlemlerine ilişkin kanıtların ve bilgilerin kayıt biçiminde toplanması ve muhafaza edilmesi süreçlerini içine alan, kayıtların üretilmesi, sağlanması, bakımı, kullanımı ve elden çıkarılmasının etkin ve sistemli bir şekilde kontrol edilmesinden sorumlu yönetim alanı*" olarak tanımlanmaktadır. Bu standartta belgelerin yasal geçerlilikleri ile kanıt özelliklerinin üzerine durulmaktadır (Külcü ve diğerleri, 2015, s.18). Odabaş'a (2008, s.123) göre belge yönetimi, kurumların faaliyetleri kapsamında belgelerin üretilmesi, dağıtılması, dosyalanması, erişim sağlanması ve ayıklanması ya da imha edilmesine kadar yürütülen tüm işlemlerin kontrol altında tutulmasını sağlayan uygulama ve ilkelerdir. Bu bağlamda belge yönetimi, kurumlarda yürütülen faaliyetlere ilişkin bir denetim mekanizması olarak hizmet etmektedir.

Kurumlar için çok önemli bilgi varlıkları olan belgelerin yönetimi, Amerika Ulusal Arşivi (National Archives and Records Administration-NARA) tarafından 1934 yılında yapılan çalışmalar neticesinde ortaya çıkan yaşam döngüsü (life cycle) kavramıyla ifade edilmektedir. Yaşam döngüsü; belgelerin üretilmesi, dosyalanması, dağıtımı, saklanması ile imhası veya arşive transfer edilmesi süreçlerini içeren bir yapı olarak tanımlanmakla birlikte, kurumlarda belge ve arşiv faaliyetleri kapsamında yaşanan sorunların yaşam döngüsü süreçlerinin bir bütün halinde uygulanmasıyla çözülebileceğine dayanmaktadır (Hare ve McLeod 1997, s.2; Külcü ve diğerleri, 2015, s.1; Penn ve diğerleri, 1994). Bu yaklaşımının kullanımına ilişkin iki farklı yönelim vardır. Çoğunlukla İngiltere merkezli olan yaklaşım çerçevesinde belgeler üç aşamalı yaşam döngüsünde betimlenmekte olup, güncel dönem, yarı güncel dönem ve güncel olmayan dönem aşamalarından oluşmaktadır. Genellikle Kuzey Amerika'da kabul gören diğer yönelimde ise, belgeler beş aşamada ele alınmakta olup, üretim, sağlama, depolama, kullanım, ayıklama süreçlerinden oluşmaktadır. Söz konusu yönelimlerden ikincisi daha fazla kullanılmaktadır (Külcü, 2018, ss.62-63, Shepherd, 2003, s.5).

Belgelerin yaşam döngüsünü tanımlayan söz konusu yönelimler Şekil 4'de sunulmaktadır.



Şekil 4. Belge Yaşam Döngüsü Modelleri (Külcü, 2018, s.63; Shepherd, 2003, s.6)

Külcü (2018, s.63) idari ve yasal düzenlemelerin belgelerin yaşam sürelerini belirleyen en önemli değişkenler olduğunu ifade etmektedir. Bu bağlamda, belge yaşam döngüsü süreçlerinin doğru bir şekilde tanımlaması ile belge yönetim sisteminin yönetimi ve sürdürülebilirliğinin sağlanması için ihtiyaç duyulan idari ve yasal düzenlemelerin yapılması gerekmektedir. Bununla birlikte, belge yönetimi süreçlerinde ulusal ve uluslararası standart ve düzenlemelerin dikkate alınması önemlidir. Belge yönetimi programları kurumun bağlı olduğu sektöre, kurumun kültürüne ve büyüklüğü ile yürürlükteki yasal düzenlemelere bağlı olarak değişiklik göstermesine rağmen, bazı ortak hususların yerine getirilmesi gerekmektedir. Bu bağlamda, bir belge yönetim programının unsurları şunlardır (Franks, 2013, s. 39):

- Politika ve yönerge geliştirme,
- Belge envanteri, saklama, değerlendirme ve elden çıkarma,
- Aktif dosya yönetimi (kağıt ve elektronik),
- Aktif olmayan dosyaların yönetimi ve kontrolü (kayıt merkezi ve dijital arşivleme),
- Koruma (dijital ve fiziksel),

- Önemli belgelerin korunması, iş sürekliliğinin ve risklerin planlanması,
- Eğitim ve destek programları.

2.4. ELEKRONİK BELGE YÖNETİMİ

Kurumsal faaliyetlerin elektronik ortamlarda yürütülmesiyle birlikte, belge yönetim uygulamaları da elektronik ortamlarda vücut bulmaya başlamıştır. Teknolojik ilerlemelerle hayatın içine taşınan elektronik belge yönetimi ve uygulamaları geniş bir zeminde varlık bulmaktadır. Elektronik ortamlarda üretilen belgelerin özgünlüğü ve güvenilirliğinin sağlanmasına ilişkin yapılan yasal düzenlemeler ve standartlar kapsamında geliştirilen uygulamalar sonucunda tespit edilen performans iyileştirmeleri, kurumların elektronik belge yönetimi uygulamalarına odaklanmasına neden olmuştur (Külcü ve diğerleri, 2015, s.3).

Elektronik belgelerin ortamı, fonksiyonu, muhteviyatı, fiziksel ve entelektüel biçimi, yasal ve idari gerekliliklerle arşivsel değer unsurları, belgeleri elektronik mecrada üretilen dokümanlardan ayıran özelliklerdir (Duranti, 2001, s.4; Külcü ve diğerleri, 2015, s.19). Kurumsal yapılarda bir dokümanın belge olarak varlık bulması için, söz konusu belgenin yönetsel, teknik ve yasal prosedürlere göre üretilmesi, kullanılması ve saklanması gerekmektedir. Söz konusu gereklilikler elektronik belgeler içinde geçerli olmakla birlikte, elektronik belgelerin belge olarak nitelendirilebilmesi için belgenin özgünlük, güvenilirlik, bütünlük ve kullanılabilirlik özelliklerine sahip olması gerekmektedir (Odabaş, 2008, s. 129; Wallace, 2001, ss. 4-6).

Elektronik ortamlarda bulunan belgeler, basılı belgelerin kanıt özelliğine haiz olan ve sayısal olarak oluşturulmuş elektronik verilerden meydana gelmektedir (Külcü ve diğerleri, 2015, s. 19). Güvenli e-imza ile imzalanan elektronik belgeler, el yazısıyla imzalanan fiziki belgelerle aynı delil değerine sahip olmaktadırlar (Elektronik İmza Kanunu, 2004, mad. 5). EBYS'nin temel unsuru olan zaman damgası, güvenli e-imzalı olarak üretilen belgelerin kanıt değerinin doğrulanmasını sağlamaktadır (Özdemirci, 2019, s. 6). Ayrıca, dijitalleştirilen fiziki belgelerin elektronik belge olarak değerlendirilebilmesi ve delil kapsamında gerçekliğinin olabilmesi için söz konusu fiziki belgelerin dijitalleştirme esnasında değiştirilmediğine ilişkin bir zaman damgasıyla damgalanması gerekmektedir (Aydın ve Özdemirci, 2011, s. 106).

Elektronik belge yönetimi, iş süreçlerinde oluşturulan ya da temin edilen ve kurumların faaliyetlerine yönelik delil teşkil eden elektronik belgelerin içerik, format ve ilişkisel niteliklerinin korunarak ve söz konusu belgelerin sağlanmasından imhasına kadar süreç içerisinde yönetilmesidir. Elektronik belge yönetimi çok karmaşık ve geniş bir alan olması sebebiyle, elektronik belge yönetiminin bir sistem yaklaşımıyla sürdürülmesi ve bu sistemi oluşturan bileşenlerin birbiriyle sorunsuz bir şekilde etkileşimde olması gerekmektedir. Bu bağlamda, Elektronik Belge Yönetim Sistemi (EBYS) söz konusu sistemi oluşturan unsurların başında gelmektedir (TS 13298, 2015). Aydın ve Özdemirci (2011, s. 107) elektronik belgelerin etkili olarak yönetilmesi kapsamında, belgelerin elektronik olarak üretilmeden önce, belge ve arşiv yönetim gereksinimleri ile yasal gereklilikler çerçevesinde bir EBYS'nin tasarlanmasını gerektiğini belirtmektedirler. Elektronik belgelerin yönetimine ilişkin yasal mevzuat, standart, proje ve uygulamalar çalışmanın sonraki kısımlarında ele alınacaktır.

2.4.1. Elektronik İmza (E-imza)

Kamu kurum ve kuruluşları, bilgi ve iletişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla faaliyetlerinin ve iş süreçlerinin büyük bir bölümünü elektronik ortamda sürdürmektedirler. Bu faaliyetlerde üretilen elektronik belgelerin delil değeri taşıması için elektronik imza (e-imza) gibi güvenilir araca ihtiyaç duyulmuştur. Söz konusu teknolojilerin gelişmesi ve kurumların belge yönetim uygulamaları elektronik ortamlarda sunması ile birlikte belgelerin kanıt özelliğini sağlayan e-imza uygulaması, kişilere ve kurumlara önemli kolaylıklar sağlamaktadır (Kaya Bensghir ve Topcan, 2010). Çoğu ülkede kullanılmakta olan e-imza uygulaması, Türkiye'de 2004 yılında yürürlüğe giren Elektronik İmza Kanunu ile kullanılmaya başlanmıştır.

5070 Sayılı Elektronik İmza Kanunu'nda (2004) e-imza, "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*" olarak tanımlanmaktadır. E-imza, elektronik belgelerin yetkili kişilerce üretilmesi, gönderilmesi, kullanılması, saklanması ve imha edildiğini belirten bir işarettir (TS 13298, 2015). Kurumların faaliyetleri ve iş süreçleri kapsamında kullandıkları resmi yazışmaların çerçevesini belirleyen Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'e (2020) göre güvenli e-imza ise, "*Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli*

elektronik sertifikaya dayanarak imza sahibinin kimliğinin ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza" olarak tanımlanmaktadır. Bu tanımlardan yola çıkarak e-imza, elektronik belgelerinin yetkili kişiler tarafından imzalanmasına ve imza sahibinin kimliğinin belirlenmesine olanak sağlayan elektronik ortamda kullanılan veri olarak tanımlanabilir.

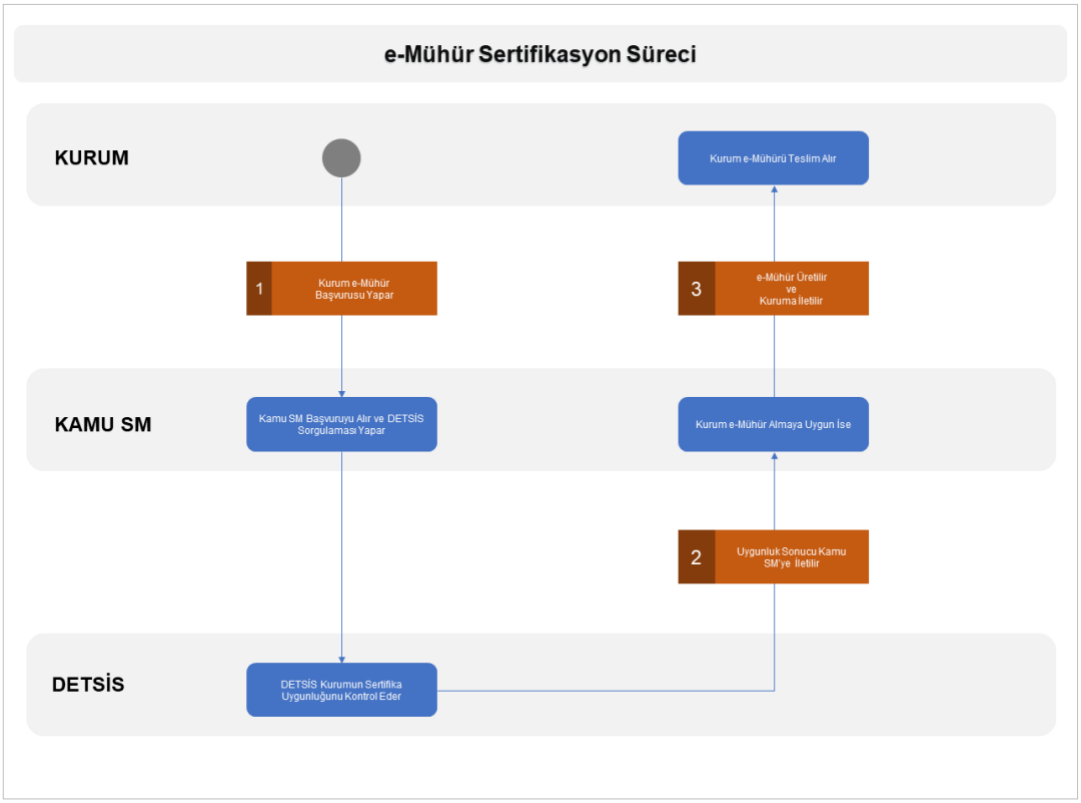
Belgelerin yetkili kişiler tarafından onaylanması çerçevesinde, fiziki belgelerin el yazısıyla imzası ile elektronik belgelerde kullanılan e-imza arasında hukuki bir fark bulunmamaktadır (Odabaş, 2009). Bu bağlamda, belge yönetim süreçleri, kişilerin el yazısıyla gerek duyulmadan, mekân ve zaman kavramına bağlı kalınmadan e-imza sayesinde kolaylıkla sürdürülebilmektedir.

2.4.2. Elektronik Mühür (E-mühür)

Elektronik ortamlarda faaliyetlerini ve iş süreçlerini yerine getiren kurumlarda, el yazısıyla imzalanan belgelerin yerini e-imzalı elektronik belgeler, mühür işlemlerinin yerini ise elektronik mühür (e-mühür) uygulamaları almaktadır. 5070 Sayılı Elektronik İmza Kanunu'nda (2004) e-mühür "*elektronik belgenin veya verinin mühür sahibi tarafından oluşturulduğunu, belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kaydı*" olarak tanımlanmaktadır. E-mühür, hukuki anlamda resmi mühür de dahil olmak üzere tüm fiziki mühürlerle aynı niteliğe sahiptir (E-İmza Kanunu, 2004, ek mad. 1). E-mührün amacı imzalanan belgenin bütünlüğünün ve kaynağının ispatlanması olup, bahsi geçen belgenin kaynağı ise belgeye sahip olan kuruma ait bilgidir (Çelik ve diğerleri, 2017, s. 114).

Elektronik olarak varlık bulan resmi bir yazının, kurumda yetkili bir kişisi tarafından imzalanıp imzalanmadığı şüphesinin ortadan kaldırılması amacıyla, tüzel kişiyi temsil eden ve kuruma özgü oluşturulan imzanın "e-mühür" olduğu, belgelerin mühürlenmesi (imzalanması) sürecinde uygulanan sertifikanın "e-mühür sertifikası" olduğu ifade edilmektedir (Çelik ve diğerleri, 2017, s.114). Bir kişiye ait olma yapısında olan e-imza kapsamında sadece gerçek kişilere nitelikli elektronik sertifika verilmekte, yapılan işlemlere kurumsal aidiyet kazandıran e-mühür ise sadece tüzel kişilerin kimlik bilgilerine haiz olan elektronik mühür sertifikası ile oluşturulmaktadır. Bu durum, e-imza ile e-mühür arasındaki en önemli farkı göstermektedir.

e-Yazışma Projesi Genelgesi (Başbakanlık, 2017/21) ile e-mühür düzenlemesi yapılmış ve TÜBİTAK bünyesindeki Kamu Sertifikasyon Merkezi (Kamu SM) e-mühür ile ilgili sertifikaların üretilmesi için yetkilendirilmiştir (Kamu SM, 2023). e-Yazışma Teknik Rehberi çerçevesinde, e-mühür sertifikası edinilmesine ilişkin sertifikasyon süreci Şekil 5'de gösterilmiştir.



Şekil 5. E-Mühür Sertifikasyon Süreci (E-Yazışma Teknik Rehberi, 2023, s.9)

2.4.3. Kayıtlı Elektronik Posta (KEP)

Kurumsal iletişim, bilgi ve belge paylaşımı büyük oranda e-posta hizmeti üzerinden yapılmaktadır. E-postalar bilgi ve belgelerin hızlı ve az maliyetle paylaşımına imkân sağlamasına karşın, paylaşılan içeriğin bütünlüğünü koruyan, bilgi ve belgenin yasal geçerliliğini temin eden ve hukuki delil niteliğini taşıyan bir iletişim ortamı sağlamamaktadır. Türkiye'de kurumsal iletişimin e-posta hizmeti vasıtasıyla yasal zeminde ve hukuki açıdan delil özelliğinin sağlanarak yapılabilmesine olanak sağlayan Kayıtlı Elektronik Posta (KEP) uygulamasına yönelik ilk düzenleme Türk Ticaret

Kanunu (2011) ile olmuş, devamında KEP usul ve esaslarına ilişkin bir dizi mevzuat çalışması yapılmıştır.

KEP, e-posta teknoloji altyapısını kullanan ve yasal amaçlar için elektronik mesaj gönderme ve alma kanıtı sunan bir e-posta iletim hizmetidir. KEP sistemi, kurumsal yazışmaların elektronik ortamlarda, güvenli olarak, yasalar çerçevesinde ve uluslararası standartlarda gerçekleştirilmesine olanak sağlamaktadır. KEP, e-imza ve zaman damgası kullanılmasıyla birlikte, bir e-postanın tüm ekleriyle beraber gönderildiğini, gönderici ve alıcıya ait kimlik teyidinin yapıldığını, gönderilen e-postanın içeriğinin başka bir kişi tarafından değiştirilmediğini garanti altına almakla beraber, gönderim ve alım zamanının tespitini sağlamaktadır (PTTKEP, 2023).

KEP Türkiye'de uygulanmaya başlamadan önce birçok ülkede (İtalya, PEC; Almanya, De-mail; Amerika, RPost) kullanılan ve resmi yazışmalarda tercih edilen hizmettir (Üstündağ ve Yılmaz, 2015, s.221). Türkiye'de KEP, Türk Ticaret Kanunu'nun (2011) KEP'e yönelik hükümlerine istinaden yasal zeminde yerini almıştır. Söz konusu kanunun 18'inci maddesinin 3'üncü fıkrasında KEP sistemi, tacirler arasındaki ihbar veya ihtarların yapılmasına ilişkin alternatif bir iletişim kanalı olarak ifade edilmiştir. Bununla birlikte, Kanun'un 1525'inci maddesinin 2'nci fıkrasıyla KEP sistemine yönelik usul ve esasları belirleme görevi Bilgi ve İletişim Kurumu'na (BTK) verilmiştir (Türk Ticaret Kanunu, 2011). KEP sistemi, Kayıtlı Elektronik Posta Hizmet Sağlayıcıları (KEPHS) tarafından işletilmektedir. KEPHS'lerin KEP vasıtasıyla gönderilen belgelerin güvenli bir şekilde iletilmesine ilişkin kayıtları azami olarak yirmi yıl muhafaza etmesi gerekmektedir.

3. BÖLÜM

VERİ YÖNETİMİ UYGULAMALARI

3.1. VERİ

Olaylara ilişkin gerçekler olan veriler, kurumsal amaçlar kapsamında süreçlerin yapılandırılmamış bir biçimde kayıt edilmesidir. Modern kurumlarda teknolojik sistemlerde saklanan veri, çözümlenmemiş ve yorumlanmamış gözlem, işlenmemiş gerçeklerdir (Barutçugil, 2002, s. 57). Veri, sayısal kayıtların bulunduğu durumu ifade eden nicel kayıtlardan (sayı, yaş, fiyat, nüfus, gelir, hız vb.) veya sayısal olmayan formatlardaki nitel kayıtlardan (metin, fotoğraf, video vb.) oluşmaktadır (Kitchin, 2014, s. 1). Veriler bir kuruluşta günlük karar vermeyi, kurumsal amaçların ve süreç tanımlarının oluşturulmasını desteklemek için gözlemlenebilir bir varlık ve değer olarak nitelendirilmektedir (Cleven & Wortmann, 2010, s. 1; Frické, 2018, s. 1).

Tek başına anlam ifade etmeyen veriler, enformasyon ve bilginin yapı taşıdır (Davenport ve Prusak, 1998, s. 3; Krishnan, 2013, s. 3; Külcü, 2000, s. 409; Yılmaz, 1998, s. 98). Veri, enformasyon ve bilgi farklı anlamsal kavramları olmasına rağmen ilişkisel olarak birbirlerine bağlı kavramlardır. Verinin enformasyonun ham bir yapı taşı olduğu, enformasyonun veri setlerinden organize edildiği ve bilginin ise anlamlı enformasyonları ifade ettiğini söylenebilir (Bhatt, 2001, s.69). Bu sebeple enformasyon ve bilginin oluşturulmasının ham maddesi olan veriler, kuruluşların iş süreçlerinin ve hizmetlerin yerine getirilmesi ve kurumsal karar verilmesi kapsamında çok önemli varlıklar olduğu söylenebilir.

3.2. VERİLERİN SINIFLANDIRILMASI

Bilginin yapı taşı olan veriler yapısal özelliklerine, karakteristiklerine, kullanım amaçlarına göre sınıflandırılabilmektedir. Jeffery'e (2014) göre veriler yapılandırılmış/yapılandırılmamış/yarı yapılandırılmış, statik/dinamik/akar, güvenli/açık, özel/halka açık, ücretli/ücretsiz, açık veri, açık kamu verisi ve büyük veri olarak gruplara ayrılarak nitelenebilmektedir. Ayrıca, her veri türü kendine özgü özellik ve ayırt edici karakteristiğine göre sınıflandırılabilmektedir. Bu bağlamda, verilerin

sınıflandırılmasında yaygın olarak kullanılan verilerin karakteristikleri ve sınıflandırma yöntemleri Tablo 3'de listelenmiştir.

Tablo 3. Verilerin Sınıflandırmaları (Sinanç, 2014, s. 15)

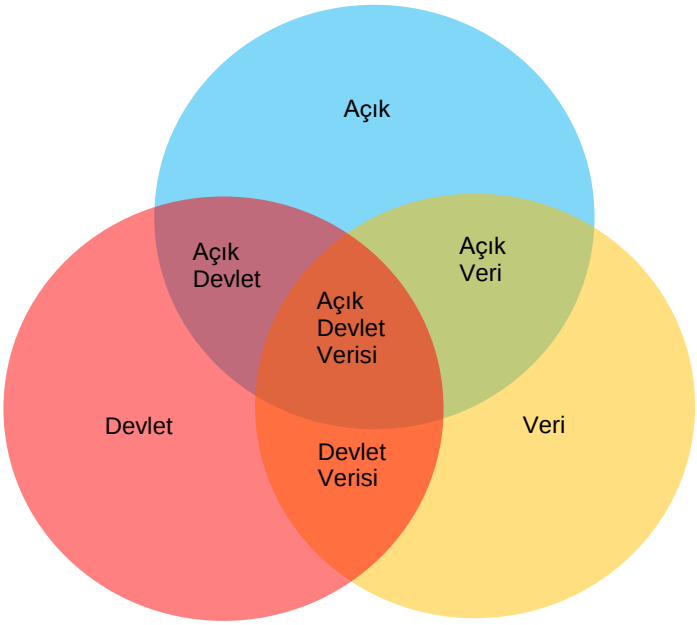
Sınıflandırma Karakteristiği	Veri Sınıflandırmaları
Veri Türü	Meta Veri, Ana Veri, Geçmiş Veri, İşlevsel Veri
Veri Biçimi	Yapısal Veri, Yarı-Yapısal Veri, Yapısal Olmayan Veri
Veri Kaynağı	Web ve Sosyal Medya, Makine Kaynaklı, Nesnelerin İnterneti (IoT), İnsan Kaynaklı, Dâhili Kaynaklar, İşlem Verisi, Veri Sağlayıcıları
Veri Frekansı	İsteğe Bağlı, Sürekli, Gerçek Zamanlı, Zaman Serileri
Veri Saklama	Sütun Tabanlı, Graf, Anahtar-Değer, Doküman Tabanlı
Veri Tüketicileri	İnsan, İş Süreci, Kurumsal Uygulamalar, Veri Ambarları
Veri Kullanımı	Endüstri, Akademi, Devlet, Araştırma Merkezleri
Analiz Türü	Analiz Türü
İşleme Metodu	Yüksek Performanslı Hesaplama, Dağıtık, Paralel, Kümeleme
Donanım	Ticari Donanım, Gelişmiş Donanım

Kamu kurum ve kuruluşlarının iş süreçleri ve faaliyetlerinde kullanılan veriler, yapılandırılmış, yapılandırılmamış ve yarı yapılandırılmış olabilmektedir. Bu kapsamda, veriler türlerine göre bu üç yapıda sınıflandırılabilir. Üretilen verilerin %80'i yapılandırılmamış veriler oluşturmakta (Inmon ve diğerleri, 2008, s. 299) ve yüksek oranda dinamik olan bu verilerin belirli bir formatları bulunmamaktadır. Bu veriler fotoğraf, pdf dokümanları, e-posta ekleri, sesli postalar, videolar tıbbi kayıtlar, X ışınları, sesler vb. şeklinde olabilmekle birlikte, yapılandırılmış olarak satır/sütun formatında depolanamamaktadır (Jaseena ve David, 2014, s. 134).

Kamu kurumlarına ait verilerin açık olarak yayınlanması olarak literatürde belirtilen "açık devlet verileri" açıklığın, devletin ve verilerin kesişim kümesi olarak tanımlanmaktadır (Zapata ve Heeks, 2015, s. 442). Açık devlet verilerinin temelleri Şekil 6'da gösterilmiştir. Kamu kurumları tarafından üretilen verilerin herhangi bir kısıtlama olmaksızın herkes tarafından kullanılabilen ve dağıtılabilen veriler olarak tanımlanmasıyla ifade edilen açık devlet verisinin açık devlet modelinin oluşturulmasının ana unsuru olduğu söylenebilir (Eroğlu, 2017). Açık devlet verisi kavramının iki temel unsuru aşağıda tanımlandığı gibidir (Ubaldi, 2013, s. 6):

- Devlet verisi (Kamu verisi): Kamu kurum ve kuruluşlarınca üretilen veya aktif hale getirilen herhangi bir veri ve bilgidir.

- Açık veri: Herkese açık, tekrar kullanılabilir ve paylaşılabilir verilerdir.



Şekil 6. Açık Devlet Verilerinin Temelleri (Zapata ve Heeks, 2015, s. 442)

Ulusal ve kişisel güvenliğin ve gizliliğin sağlanması kapsamında, gizlilik derecesine sahip, kişisel, hassas, telifli ve ekonomik değeri olan kamu verileri gerekli süreçler yerine getirilerek ve güvenlik önlemleri alınarak kurumsal faaliyetlerde kullanılmalı ve ilgilerle paylaşılmalıdır (Geiger ve Lucke, 2012, s. 272). Kamu kurum ve kuruluşlarına ait verilerin gizlilik ve mahremiyetinin sağlanması ile açık devlet sürecinin şeffaflık değerleri birbirlerinin zıt kavramları olarak önümüze çıkmaktadır (Eroğlu, 2018a, s. 144). Bu bağlamda, verilerin kamuoyuna açılarak şeffaflık, toplumun yönetime katılımı, yenilikçi uygulama ve hizmetlerin yaratılmasının sağlanması amaçlanmakta iken, diğer taraftan gizliliğe ilişkin endişeler ile kişisel, hassas, gizli, telifli ve ekonomik değeri olan veri gruplarının kötüye kullanımları ve uygun olmayan paylaşımları konusunda gerekli tedbir ve önemlerin alınmasının gerekliliği üzerinde durulmaktadır. Mevcut yasal düzenlemeler kamu verilerinin açılmasının önünde bir engel oluşturmasının yanı sıra, gerekli işlem ve tedbirlerin alınmadan şeffaflık kapsamında kamu verilerinin açılması ulusal ve kişisel güvenliği tehlikeye düşüreceği yönünde endişelere sebebiyet verebilmektedir. Bu sebeple kamu verilerinin paylaşılması kapsamında gizlilik ve güvenlik sınırlarının net bir şekilde çizilmesi, kamu verilerinin sınıflandırılması ve veri yönetim politikalarının oluşturulması ve yürütülmesi gerekmektedir (Eroğlu, 2017, s. 112).

Kamu kurum ve kuruluşlarınca üretilen veya toplanan veriler bilgi sistemleri yordamıyla başka sistemlerde paylaşılmaktadır. Bir veri grubuna ait ifadeler, farklı kurum ve kuruluşlarda çeşitli değerlerde bulunabilmektedir. Örneğin cinsiyet bilgisi için veriler; Erkek/Kadın, Bay/Bayan, E/K gibi farklı değerler kullanarak belirtilebilmektedir. Bu sebeple, verilerin nasıl anlamlandırılacağı ve saklanacağı yazılım geliştiricilerin takdirine bırakılmaktadır. Bunun sonucu olarak kurumsal hafızanın oluşturulamaması, sistemler arasında veri entegrasyonu ve paylaşılması sorunları, tekrarlı ve çelişen verilerin bulunması, sistemlerde yeknesaklığın sağlanamaması ve veri sahipliğinin belli olmaması gibi çeşitli sorunlar ortaya çıkmaktadır. Bu sorunların çözümüne yönelik Cumhurbaşkanlığı Dijital Dönüşüm Ofisi uhdesinde 2019 yılında Ulusal Veri Sözlüğü Projesi başlatılmıştır. Projenin hayata geçirilmesiyle; verilere yönelik bütün kurumlarda dil birliğinin oluşturulması, standart olarak veri tekilliğinin sağlanması ve entegrasyonun kolaylaştırılması, yenileyen, çelişen ve uyumsuz verilerin meydana gelmesinin engellenmesi, üçüncü kurum/firma/kişi gibi taraflara olan bağımlılığın ortadan kaldırılması ve bilgiye erişim kolaylığının sağlanması hedeflenmektedir. Proje ile bütün kamu kurumlarının kendi veri sözlüklerini oluşturmaları hedeflenmiştir. Bu amaçla Web tabanlı bir Üstveri Kayıt Defteri yazılımı olan “Ulusal Veri Sözlüğü Yazılımı” oluşturulmuştur (Ulusal Veri Sözlüğü…, 2019; Ulusal Veri Sözlüğü…, 2020).

Kamu kurum ve kuruluşlarında bulunan verilerin açık olarak paylaşımı; şeffaflık ile toplumun yönetime katılımını, yeni hizmet ve uygulamaların oluşturulmasını ve kamu verilerinden değer üretilmesinin geliştirilmesini artıracağı düşünülmektedir (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023b). Fakat, kurum ve toplumun mahremiyeti, güvenliği, gizliliği, menfaatinin korunması için yapılan yasal düzenlemeler verilerin paylaşımını kısıtlamaktadır. Kişisel ve hassas kişisel veriler ile verilerin gizlilik, telif ve ekonomik durumları kamu verilerinin paylaşılmasını kısıtlayan unsurlardır.

3.2.1. Yapılandırılmış Veri

Düzenli bir biçimde olması sebebiyle yapılandırılmış veriler okunabilir ve tahmin edilebilir verilerdir. Yapılandırılmış veriler hesap ve algoritmalar vasıtasıyla kolaylıkla işlenebilmekte, birleştirilebilmekte, sorgulanabilmekte, araştırılabilmekte, analiz edilebilmekte, farklı grafik ve harita formları vasıtasıyla görselleştirilebilmekte ve bilgisayar yordamıyla kolayca işlenebilmektedir (Inmon ve Linstedh, 2015, s. 336). Yapılandırılmış veriler belirli kural ve sistemler çerçevesinde depolanmaları sebebiyle

kolaylıkla erişebilir, düzenlenebilir, kategorize edilebilmektedirler (Doğan ve Arslantekin, 2016, s. 18). Yapılandırılmış veriler, güçlü bir düzenleme seviyesinde bulunmakla birlikte, ilişkisel bir veritabanına entegre edilerek kolayca ve sorunsuz bir şekilde aranabilirmektedir (Ünver, 2018, s. 15).

Tablolarda satır ve sütun olarak düzenlen bu veriler kağıt üzerinde olmasının yanı sıra, istatistik programlarındaki örüntü oluşumlarında da varlık bulabilirler (Doğan ve Arslantekin, 2016, s.18). İlişkisel veri tabanları ve benzer yapıya sahip veri ambarları, yapılandırılmış verilerin bulunduğu yaygın yerlerdir (Arslantekin, 2003, s.376). Yapılandırılmış veriler doğası gereği tanımlanmış bir düzende kayıt altına alınmakta çocuğu zaman veri tabanı yönetim sistemi tarafından yönetilmektedir (Pala, 2021, s. 32).

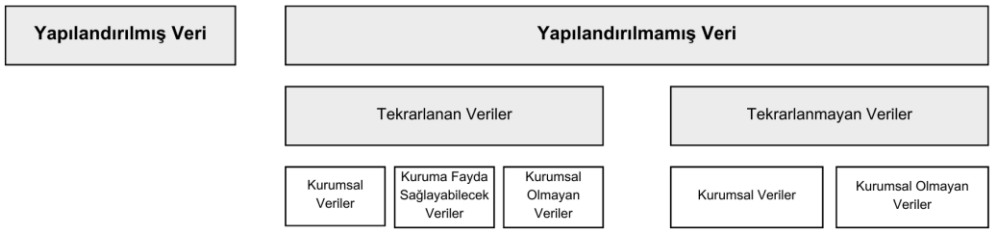
Yapılandırılmış veriler veri tabanı tabloları, yapılandırılmamış veriler e-postalar ve algılayıcılardan gelen veriler, yarı yapılandırılmamış veriler ise XML dosyaları, sosyal medya verileri vb. verilerdir (Ünver, 2018, s. 17).

3.2.2. Yapılandırılmamış Veri

Yapılandırılmış verilerin aksine, yapılandırılmamış veriler tahmin edilemeyen ve bilgisayar tarafından tanınamayan bir yapıya sahiptir. Bir çok farklı fonksiyon ve yapısı olan yapılandırılmamış veriler; kağıt üzerinde bulunan doküman, kitap ve mektup metinlerinden, e-posta, elektronik sunu dokümanları ve web sayfaları gibi elektronik ortam metinleri veya video gibi hareketli, fotoğraf gibi durağan görüntülerden ya da ses gibi medya dosyalarından oluşmaktadır (Arslantekin, 2003, s. 376; Doğan ve Arslantekin, 2016, s. 19; Inmon ve diğerleri, 2008, s. 300; Haselden ve Wolter, 2021; Yıldız, 2022, s. 363) . Yapılandırılmamış veriler insanlar tarafından kolaylıkla yorumlanabilir ve işlenebilir olmasına rağmen, bu işlemler makinelerce yapılamamaktadır (Haselden ve Wolter, 2021). Yapılandırılmamış veriler, dağınık, ilişkisel olmayan, büyük, metin ağırlıklı ve alışagelmiş tablolarda kolaylıkla temsil edilememektedir (Pala, 2021, s. 33). Dolasıyla yapılandırılmış verilerle her türlü işlem ve sorgulamanın yapılabilmesi ve bir veri tabanı yönetim sistemi vasıtasıyla ilişkilerinin kolaylıkla kurulabilmesinin aksine, bu işlemler yapılandırılmamış veriler üzerinde gerçekleştirilememektedir. Yapılandırılmamış veriler düzenli bir formda olmaması

sebebiyle, standart bir veri yönetimi sistemiyle yönetilememektedir (Inmon ve Linsted, 2015, s. 15).

Inmon ve Linsted'e (2015) göre yapılandırılmamış veriler tekrarlanan ve tekrarlanmayan veriler olarak ikiyi ayrılmaktadır. Bu veriler Şekil 7'de gösterilmiştir. Tekrarlayan yapılandırılmamış veriler, çok sık meydana gelen ve kayıtları yapı ve içerik açısından hemen hemen aynı olan verilerdir. Telefon konuşma kayıtları, ölçülü veriler ve analog veriler tekrarlanan yapılandırılmamış veri örnekleridir. Tekrarlanmayan yapılandırılmamış veriler ise, yapı veya içerik açısından kayıtların benzer olmadığı veri kayıtlarından oluşan verilerdir. Çağrı merkezi görüşmeleri, e-postalar, garanti talepleri tekrarlanmayan yapılandırılmamış veri örnekleridir. Tekrarlanan veriler çoğunlukla aynı yapı ve uygulamada olmakla birlikte, farklı zaman dilimlerine aittiler. Tekrarlanmayan verilerin her kaydı genellikle önemli ölçüde birbirinden farklıdır (Inmon ve Linsted, 2015, s.15).



Şekil 7. Veri Tipleri (Inmon ve Linstedh, 2015)

Ayrıca, kamu kurum ve kuruluşları tarafından yürütülen iş süreçleri ve hizmetlerde bazı veri setleri günlük, saatlik ve daha sık zamanlarda güncellenmektedir. Örneğin tren, uçak vb. araçların kalkış saatlerinin gerçek zamanlı olarak güncellenmesi buna örnek gösterilebilir. Bu sebeple verilerin güncellik durumu kamu verilerinin yararlığını etkilemektedir.

3.2.3. Yarı Yapılandırılmış Veri

Yarı yapılandırılmış veriler sınıflandırılarak veya belirli sıralara sokularak işaretlenebilen bir veri türü olmakla birlikte, yapılandırılmış veriler gibi veri tablolarına veya veri tabanı sistemine dahil edilecek belli bir formata sahip değildirler (Düzce Üniversitesi, 2022). Bu veriler anlamsal olarak ifadeler içerdiği halde, tipik bir biçime sahip olmayan, tanımlı olan fakat net bir düzen veya ilişki içermeyen veri tipleridir (Pala, 2021, ss. 33-34).

Bilgisayar ve insanlar tarafından rahatlıkla okunabilen dokümanlar üretilmesini sağlayan XLM (Genişletilebilir İşaretleme Dili) bu veri tipinin bir örneğidir (Inmon ve Linstedh, 2015, s. 150). Çoğu yazılım, başka yazılımlara olan veri alışverişini XML formatı üzerinden yapmaktadır. Bu sebeple, verilerin entegrasyonu kapsamında yarı yapılandırılmış veriler kullanılmaktadır.

3.2.4. Üst Veri

Üretilen veya toplanan verilerin belli standartlar ile kayıt altına alınması, bu verilerin bulunabilirliğini, paylaşılabilirliğini, birlikte çalışabilirliğini ve dolayısıyla kullanılabilirliğini etkilemektedir. Bu sebeple verilerin düzenlenmesi, aranması, erişilmesi ve yönetilmesi kapsamında verilerin tanımlanması gerekmektedir. Verilerin tanımlanabilmesine yönelik en önemli aracın ise üst veri olduğu değerlendirilmektedir (Doğan ve Arslantekin, 2016, s. 19).

Yapısal bir veri olan üst veriler, diğer veriler hakkındaki bilgileri barındırmakta ve genellikle “veriler hakkındaki veriler” olarak tanımlanmaktadır. Verilerin neyle ilgili olduğunu açıklayan üst veriler, veri içeriğinin kısa ve tutarlı bir açıklamasının yapılabilmesi için bir mekanizma sağlamaktadır. Üst veriler, veri setleri, veri tabanı, ürünler veya dokümanları tanımlamakla birlikte, olayların ne zaman, nerede ve kim tarafından gerçekleştiğini belirten detaylara sahiplerdir (Haselden ve Wolter, 2021).

Karmaşık uzman dizinleme mekanizmaları vasıtasıyla kolaylıkla taranabilen yapılandırılmış ve yapılandırılmamış verilerin bir üst veri ile bağlanmadığı durumlarda, tüm bilgi varlıklarını kapsayan bir taramanın yapılması oldukça zordur (Arslantekin, 2003, s. 376). Bu sebeple, verilerin ve veri setlerinin ihtiyaç olduğu zaman bulunabilmesi ve erişilebilir olmasının en temel unsurunun belirli standartlara göre oluşturulmuş üst veriler olduğu söylenebilir.

3.2.5. Kişisel Veri

Kamu verilerinin korunması ve güvenliğinin sağlanmasına yönelik önemli endişelerden biri de kişisel verilerdir (Eroğlu ve Çakmak, 2020b, s. 2). Kişisel veri bir bireyin kimliğini belirleyen ve bu bireyi tanımlayabilen her türlü bilgiyi ifade etmektedir (Anayasa Mahkemesi, 2014; Avrupa Konseyi, 1981, Mad.2.a.; Kişisel Verilerin Korunması…,

2016, Mad. 3.1.d). Kişilerin doğrudan veya dolaylı olarak tanınmasını ve bilinirliğini sağlayan kişisel veriler, kişilerin kimliğini doğrudan belirleyen isim, soy isim, doğum yeri gibi bilgiler haricinde, kişilerin hobileri, pasaport numarası, fotoğrafı, görüntü ve ses kayıtları, öz geçmiş, askerlik bilgisi, taşıt plakası, sosyal güvenlik numarası, kredi kartı, adres bilgileri, aile bilgileri, e-posta adresi, IP adresi, telefon numarası, parmak izi, genetik bilgiler vb. bilgilerden oluşmaktadır (Anayasa Mahkemesi, 2014; Eroğlu, 2018a, s. 134; Genç, 2019, s.43; Kişisel Verilerin Korunması…, 2016). Bireylerin yaşam hakları ve özel yaşamlarının gizliğini ihlal edebilecek olan veriler (etnik kimlik, dini inan, felsefi düşünce, cinsel yönelim, kalıtımsal veriler vb) özel nitelikli kişisel veri olarak tanımlanmaktadır (Kaya, 2011, s.318; Kişisel Verilerin Korunması…, 2016).

Kamu kurumları ve kuruluşlar tarafından toplanan ve saklanan verilerin kişisel veri olarak nitelendirilmesi ve bir kişiyi tanımlayabilmesi verilerin işlenme süreciyle ortaya çıkmaktadır (Eroğlu, 2017, s.114). Kişisel Verilerin Korunması Kanunu'na (2016, mad. 3.1.e) göre kişisel verilerin işlenmesi "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi*" olarak ifade edilmektir. Kişisel ve özel nitelikli kişisel verilerin işlenmesinde kişinin açık rızası aranmaktadır. Açık rıza kavramı, kişiye kişisel verilerin işleneceğinin bildirilmesi ve bağımsız tercihine bağlı olarak kişinin açık bir şekilde rızasının alınmasıdır. Kişisel Verilerin Korunması Kanunu'nda açık rızası aranmaksızın kişisel ve özel nitelikli kişisel verilerin işlenebilmesine olanak sağlayan durumlar tanımlanmıştır (Kişisel Verilerin Korunması..., 2016, mad. 5.2.-6.3.).

OECD tarafından 1980 yılında yayınlanan, 2013 yılında revize edilen ve 2021 yılında gözden geçirilen "Kişisel Verilerin Sınır Dışına Aktarılması ve Mahremiyetinin Korunmasının Yönetimi Rehber İlkeleri" uluslararası asgari veri koruma ve mahremiyet standardı olarak kabul edilmektedir (OECD, 2022). Kişisel verilerin korunması ve işlenmesi süreçlerine ilişkin rehberde belirtilen ilkeler aşağıda belirtilmiştir (OECD, 2021).

- Sınırlı toplama: Kişisel verilerin toplanmasında sınırlamalar olmalı, veriler uygun koşullarda yasal ve adil yollarla toplanmalı ve kişinin bilgisi veya rızası olmalıdır.
- Veri kalite: Kişisel veriler ilgili amaçlar için uygun olmalı ve bu hedeflere uygun olarak doğru, eksiksiz ve güncel tutulmalıdır.
- Amaca özgülük: Kişisel verilerin toplanma amaçları verilerin toplanma zamanından önce belirlenmesi, bu verilerin sonraki kullanımlarında bu amaçların dışına çıkılmamalıdır.
- Kullanım sınırlılığı: Veri sahibinin rızası ve mevcut yasal zorunluluk haricinde kişisel veriler toplama amacı dışında bulundurulmamalı, kullanılmamalı ve yayınlanmamalıdır.
- Güvenlik: Kişisel veriler muhtemel güvenlik risklerini (kaybolma, yetki olmayan erişim, bozulma, kullanım, dönüştürme, ifşa) önleyecek şekilde korunmalıdır.
- Açıklık: Kişisel verilere ilişkin eylem, gelişme ve düzenlemeler konusunda genel bir şeffaflık kuralı olmalıdır. Kişisel verilerin varlığı, niteliği, kullanılma amacı ile veri kontrolörünün kimliği ve olağan ikametgâhının belirlenmesi için araçlar hazır bulunmalıdır.
- Bireysel katılım: Kişiler, bir veri denetçisinin kendisiyle ilgili verilere sahip olup olmadığını teyit edebilmelidir. Kişiler kendisiyle ilgili verilere uygun bir zaman içerisinde, makul bir ücret karşılığında, uygun biçimde ve anlaşılır bir formda erişim sağlayabilmelidir. Kişiler kendisiyle ilgili verilere itiraz etmeye ve itirazları kabul olması durumunda, bu verilerin silinmesi, düzenlenmesi, tamamlanması veya değiştirilmesine yönelik talep yapabilmelidir.
- Sorumluluk: Bir veri denetleyicisi yukarıda belirtilen ilkeleri uygulayan düzenlemelere uymakla yükümlü olmalıdır.

Bilgi ve iletişim sistemlerinin kullanımının yaygınlaşması ve bilgiye erişimin kolaylaşmasının bir sonucu olarak, genellikle otomatik olarak işlenen kişisel veriler hızlı şekilde elektronik ortama aktarılmakta ve bu ortamlarda işlenmektedir. Kişisel verilerin elektronik ortama aktarılması önemli güvenlik risklerini beraberinde getirmektedir. Bu bağlamda, kişisel verilerin güvenlik risklerinin azaltılması veya ortadan kaldırılmasına yönelik alınacak tedbirler Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nin (2016) gereği olarak düzenlenen Bilgi ve İletişim Güvenliği Rehberi'nde belirtilmiştir (Cumhurbaşkanlığı Bilgi..., 2019; Cumhurbaşkanlığı Dijital Dönüşüm…, 2020a). Kişisel verilerin toplanması ve güvenliğinin sistemli bir şekilde sağlanması kapsamında, kurum

ve kuruluşlar tarafından karşılanması gereken asgari standartlar şunlardır (Vora ve diğerleri, 2018, s.1):

- Veri toplama nedeni: Verilerin toplanması için geçerli bir neden çok önemli olmakla birlikte, verilerin toplama sırasındaki gecikmenin önlenmesi için zamanında iyi bir bilgilendirme yapılmalıdır.
- Veri toplama üst sınırı: Kişisel verilerinin toplanmasında üst sınır tanımlanmalı ve sabitlenmelidir. Bunun sonucu olarak bireyler kişisel bilgilerini paylaşmasına yönelik çekincelerinden vazgeçmektedirler.
- Sınırlı erişim: Yetkilendirilmemiş kullanımların kişisel verilere erişimi sınırlandırılmalıdır. Fakat kişisel veri sahibinden önceden alınmış bir onay ve geçerli bir sebep ile verilere erişim sağlanmalıdır.
- Sınırlı kullanım: Kişisel verilerin resmi olmayan kullanımdan itina edilmelidir. Kişisel verilerin resmi kurumlarca kullanılmasına izin verilebilir, fakat bu veriler gerçek olmayan kişi veya kişilerle paylaşılmaması için kesinlikle bilgilendirilme yapılmalıdır.
- Ayrıcalıklar: Bir kişiye çeşitli ayrıcalıklar verilebilir. Yetkili otoritelere makul amaçlar çerçevesinde ve belirli zamanlarda erişim onayı verilir, reddedilen istek için uygun bir neden sunulur. Silinen, tamamlanan veya düzeltilen verilere ait yapılan taleplerde karşılaşılan zorluklara ilişkin uygun yardımlar yapılır.

3.3. VERİ YÖNETİMİNİN TARİHSEL GELİŞİMİ

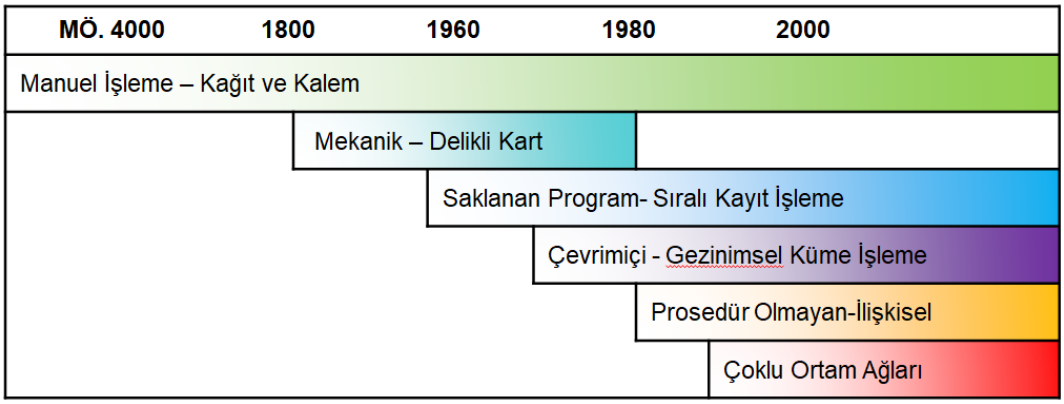
Verilerin genellikle bir bilgisayarda bulunan veri tabanı veya elektronik tabloda bulanan varlıklar olduğu düşünülmektedir. Bununla birlikte veriler, bilgisayar icat edilmeden çok önce var olan bilgi varlıklarının temel yapı taşını oluşturmuştur. Gray (1996) veri yönetimi geçmişini, M.Ö. 4000'den günümüze veri yönetimi uygulamalarını izleyen altı ayrı zaman diliminde sentezlemiştir. Veri yönetiminin manuel işleme yöntemlerinden otomatik veri yönetim aşamasına gelişimi Şekil 8'de gösterilmiştir. Veri yönetiminin tarihsel gelişimi şöyledir (Gray, 1996):

- Başlangıç aşaması (M.Ö. 4000 ile 1900): Bilgilerin kayıt altına alınması uzun bir tarihe sahiptir. Bilinen ilkyazı Sümer'de vergi ve kraliyet varlıklarının kayıtlarıdır. Veriler zaman içerisinde kil tablet, parşömen ve sonunda kâğıt

ortamında varlık bulmuştur. Verilerin sunumunda fonetik alfabe, kâğıt, defter, roman, kütüphane ve matbaanın icadı gibi birçok yenilik bulunması ile birlikte bu çağda bilgi manuel olarak işlenmektedir.

- Birinci aşama (1900-1955): 1800'lü yıllarda Jakarlı Tezgâh ile delikli kartlarla temsil edilen desenlerden kumaş üretilmesiyle ilk defa otomatik bilgi işleme süreci ortaya çıkmıştır. 1890 yılında Amerika Birleşik Devletleri (ABD) nüfus sayımında delikli kart teknolojisi kullanılmıştır. Delikli kartlar vasıtasıyla manuel olarak işlenmesi imkânsız olan milyonlarca kayıt otomatik işlenmiş ve üretilmiştir. Bu dönemde ortaya çıkan ve gelişen bilgisayarlar, 1955 ve 1970 yılları arasındaki ikinci nesle kadar veri depolama ve analiz için kullanılmamıştır.
- İkinci aşama (1955-1970): 1940'lı yıllarda geliştirilen bilgisayarlar 1950'li yılların başlarına kadar hesaplama yapmak için kullanmıştır. Bilgisayar teknolojisi veriyi depolayabilen manyetik bandı içererek şekilde gelişmesiyle yüzlerce kayıt saniyede işlenebilir hale gelmiş ve veri depolama kavramı önem kazanmaya başlamıştır. Bu dönemde, depolanan bilgileri elde etmek ve işlemek için, bilgisayar teknolojisinin önemli bir bileşeni olarak yazılımlar geliştirilmiştir.
- Üçüncü aşama (1965-1980): Borsa ticareti ve ulaşım rezervasyonlarının yapılması güncel bilgiye ihtiyaç duymaktadır. Bu dönemde bilgisayar yazılımlarının, birçok terminal kullanıcısı arasında paylaşılan bir veri tabanına karşı eşzamanlı işlemlerin yapılmasına imkân sağlayacak şekilde gelişmesiyle veriler çevrimiçi bir sisteme taşınmıştır.
- Dördüncü aşama (1980-1995): Bu dönemde her bir görev için ayrı bir yazılım dilleri yerine ortak bir dil kullanılmasıyla, verileri yönetmek için ilişkisel modeller kullanabilen bilgisayar programları ortaya çıkmıştır. Bu ilerleme, kullanıcıların karmaşık veri tabanı sorguları oluşturmasına ve verileri okunabilir, işlenebilir tablolara ve grafiklere dönüştürmesine olanak tanıyan yapılandırılmış sorgu dilinin (SQL) ve grafik kullanıcı arabirimlerinin (GUI) yolunu açmıştır.
- Beşinci aşama (1995-Günümüz): Dördüncü nesilde geliştirilen çoğu teknoloji ve görevler günümüzde hala kullanılmakla birlikte, beşinci nesilde basit sayı veya kayıt kümeleri olmayan verilerin işlenme, depolanma ve arama teknolojisinde artış görülmüştür. Günümüzde her kişi ve kuruluş tarafından

kullanılan görüntü, harita, ses dosyası gibi karmaşık veri nesnelerinin yanı sıra büyük veri kümeleri de çoklu ortamlarda saklanmaktadır.



Şekil 8. Veri Yönetiminin Gelişim Aşamaları (Gray, 1996, s. 2)

3.4. VERİ YÖNETİMİ

Bilgi hizmetlerinin sağlanmasında önemli bir kurumsal hizmet olan veri yönetimi, verilerinin tanımlanması, kalite kontrolünün yapılması ve erişilebilirliğinin sağlanması için oluşturulan mekanizmalarla ilgili süreçlerdir (Gordon, 2022). Veri yönetimi, verilerin organize ve verimli bir şekilde toplanması, saklanması, işlenmesi ve kullanılması süreçlerini ifade etmekte birlikte, kuruluşların bilinçli kararlar alması, iş süreçlerinin iyileştirmesi, yasal ve düzenleyici gerekliliklere uyulması için çok önemlidir. Bu bağlamda veri yönetimi, yaşam döngüleri boyunca veri ve bilgi varlıklarının değerini sağlayan, kontrol eden, koruyan ve artıran planların, politikaların, programların ve uygulamaların geliştirilmesi, uygulanması ve denetlenmesi süreci olarak ifade edilmektedir (DAMA International, 2017, s. 17). Veri yönetiminin amacı, kişi ve kuruluşlarca verilerin doğru amaçlar çerçevesinde kullanılmasının sağlanması maksadıyla gerekli politika ve düzenlemelerin tespit edilmesi ile güvenlik sınırlamalarının belirlenmesidir (Demir, 2021, s. 88).

Kurum ve kuruluşların değer yaratmak amacıyla maddi değeri olmayan varlıkları odaklarına almalarındaki yükseliş, veri yönetim stratejisinin kurum ve kuruluşların önemli gerekliliklerinin arasında bulunmasına neden olmaktadır. Kurum ve kuruluşlarca resmi olarak onaylanan bir veri yönetimi stratejisi, veriden değer yaratma ihtiyaçlarını, kişiler ve yöneticilerin faaliyetlerini, veri yönetimi teknolojilerinin yetkinliklerini ve yasal gereklilikleri kapsamaktadır (Oracle, 2023). Değerli ve hassas bilgiler toplayan ve

işleyen kurum ve kuruluşlar, veri varlıklarının güvenilir şekilde yönetilmesinden sorumludurlar. Bu sebeple güçlü bir veri yönetimi stratejisi, veriye dayalı karar alma süreçleri konusunda kurumsal etkinliği ve verimliliği artırmasının yanı sıra, verilerin yanlış kullanımı, veri sahipliğinin kararsızlığı veya diğer olası risklerin minimum seviyeye indirilmesine yardımcı olmaktadır (Wang ve diğerleri, 2020).

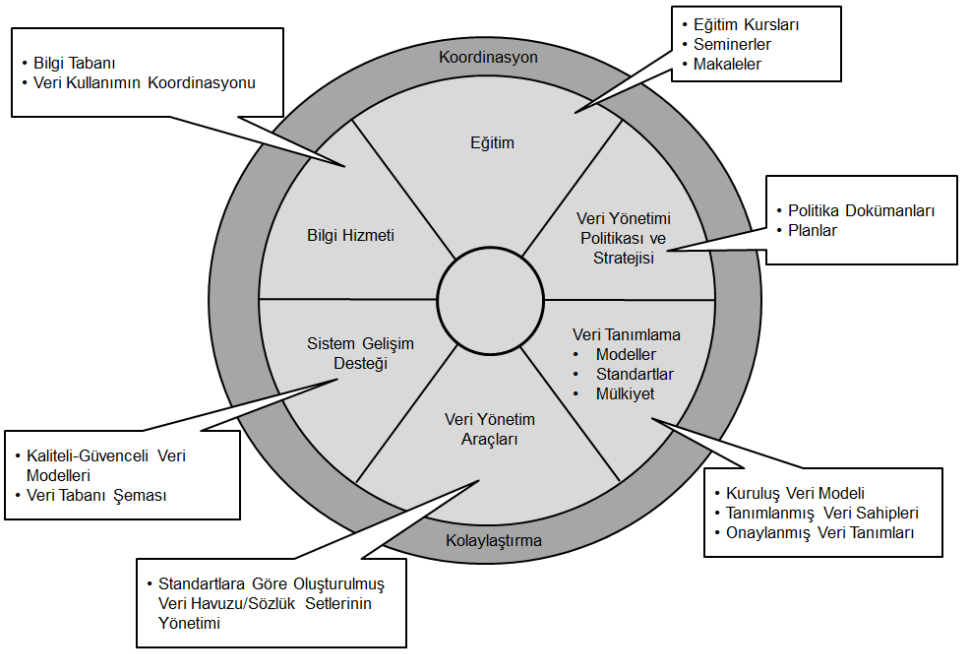
Veri yönetimi, kurum ve kuruluşlara ait verilerin tanım, kullanım ve yönetimini stratejik olarak, bilgi sistemlerinin idame ve gelişimini ise eylemsel olarak destekleme işlevine sahiptir. Kurum ve kuruluşlara stratejik ve eylemsel destek sağlama görevinin gerçekleştirilmesi kapsamında, veri yönetiminin birtakım sorumlulukları vardır. Söz konusu sorumlulukların temel alanları şunlardır (Gordon, 2022):

- Yapılandırılmış ve yapılandırılmamış verilerin önemli bir iş kaynağı olarak kabul edilmesinin sağlamasını,
- Bilgi sistemlerinde ki verilerin kalitesinin iyileştirilmesi ve bu kalitenin korunmasına yönelik süreçlerin yürütülmesi,
- Veri tanımlarının yapılması ve bu tanımların kullanımına ilişkin sistemin gelişiminde bulunan ekiplere destek sağlayarak kuruluşun bilgi iletişimini kolaylaştırılmasını,
- Kurum ve kuruluşun çeşitli yönetim düzeylerine veri tanımlarının geliştirilmesi ve sahiplenilmesi sorumluluğunun verilmesini,
- Kurum ve kuruluşun tüm bilgi sistemlerinin desteklenmesi kapsamında referans veya ana veri için tek bir kaynağın elde edilmesini sağlamaktır.

Bir kurum veya kuruluşta etkin bir veri yönetiminin uygulanması kapsamında yapılacak faaliyetlerin tanımlanması ve bu faaliyetleri gerçekleştirmek için yeterli kaynak ayrılması gerekmektedir. Veri yönetiminde yer alması gereken ana faaliyetler ve bu faaliyetlerinin çıktıları Şekil 9'da gösterilmiştir. Söz konusu faaliyetler şunlardır (Gordon, 2022):

- Eğitim: Etkin bir veri yönetiminin sağlanması için tüm personel veri yönetiminin önemi ve bu süreçlerdeki rolleri hakkında eğitilmelidir. Ayrıca, bilgi sistemi bölümün teknik personeli veri yönetimiyle sağlanan ürünlerin kullanımı ve takibi kapsamında ihtiyaç duyulacak gerekliliklerin farkında olmalıdırlar. Söz konusu eğitimler kurs, seminer ve makalelerin okunması ve yayınlanması yordamıyla yapılabilir.

- Veri yönetimi politikası ve stratejisi: Kurum ve kuruluşun veri yönetiminden beklentileri ile yöneticilerin, bilgi sistemi kullanıcılarının ve bilgi sistemi personelinin veri yönetimi kapsamındaki rolleri politika planları ve belgeleriyle düzenlenmektedir. Veri yönetimi politikaları en üst düzey yönetici tarafından onaylanarak uygulamaya sokulduktan sonra veri yönetiminin amaç ve hedeflerine ilişkin strateji geliştirilebilir. Bu aktivitenin çıktısı, politika dokümanları ve planlarıdır.
- Veri tanımlama: Kurum ve kuruluşun tüm bilgi gereksinimlerini içine alan bir veri modelinin oluşturulması için veri tanımları yapılmalıdır. Veri yönetiminin ana faaliyetlerinden biri olan bu etkinlik ile veri modellerinin geliştirilme çerçevesi, kullanılacak veri biçimleri, uygulanacak adlandırma kurallar ve standartların tanımlanmasıyla birlikte, her bir veri tanımının uygun sahibinin belirlenmesi sürecini kapsamaktadır.
- Veri yönetim araçları: Veri yönetimi karmaşık süreçleri kapsamakla birlikte, otomatikleştirilmiş araçları (otomasyon) gerektirmektedir. Bu sebeple, gerekli araçların belirlenerek satın alınmalı ve bu araçlar veri yönetimi ekibi ile kurum ve kuruluş içerisinde tutarlı şekilde kullanılmalıdır. Bu aktivitenin çıktısı, yönetilen veri havuzu/sözlük setinin belirlenen standartlara göre doldurulmasıdır.
- Sistem gelişim desteği: Veri yönetiminden sorumlu personel, bilgi sisteminin gelişiminden sorumlu olan personel ile iletişim halinde olması ve bu personeli desteklemesi gerekmektedir. Kurum ve kuruluşun veri tanımlarını da içerisine alan standartların, sistem geliştiricileri tarafından kendilerine kısıtlamalar yarattığı ve projelerin bitirilmesinde muhtemel gecikme kaynağı olduğu görülebilmektedir. Bu sebeple, sistem geliştiricileri, projelerinin geliştirilmesinde fayda elde etmek maksadıyla, veri yöneticileriyle etkileşim halinde olmalıdır. Bu aktivitenin çıktısı, kalite güvence modelleri ve veri tabanı şemalarıdır.
- Bilgi hizmeti: Bu hizmet kurum ve kuruluşta veri ve bilgi paylaşımıyla ilgilidir. Veri yöneticileri mevcut veri ve bilgilerinin neler olduğu, nelerde bulunduğu ve nasıl kullanıldığına ilişkin bilgiye sahip olması sebebiyle veri yönetiminde önemlidirler. Bu sebeple, veri yönetimi personeli kurum ve kuruluşa ve bilgi sistemi personeline kıymetli bir bilgi hizmeti verebilirler. Bu aktivitenin çıktısı ise bilgi tabanı ve veri kullanımın koordinasyonudur.



Şekil 9. Veri Yönetimi Faaliyetleri ve Çıktıları (Gordon, 2022)

Veri yönetiminin faaliyet ve disiplinleri geniş kapsamlı olmakla birlikte, söz konusu süreçlerin bazıları yazılım mimarisiyle yakından ilgili olan birden fazla alanı kapmaktadır. İş gereksinimlerinin karşılanması ve esneklik, ölçeklenebilirlik, elverişlilik, yeniden kullanılabilirlik ve güvenlik hususlarını içeren bir sistemin geliştirilmesi için, yüksek seviyeli bir yazılımın dizayn edilmesi ve oluşturulması gerekmektedir. Strengholt'a (2020) göre modern veri mimarisi çerçevesinde, veri yönetiminin boyutları şöyledir:

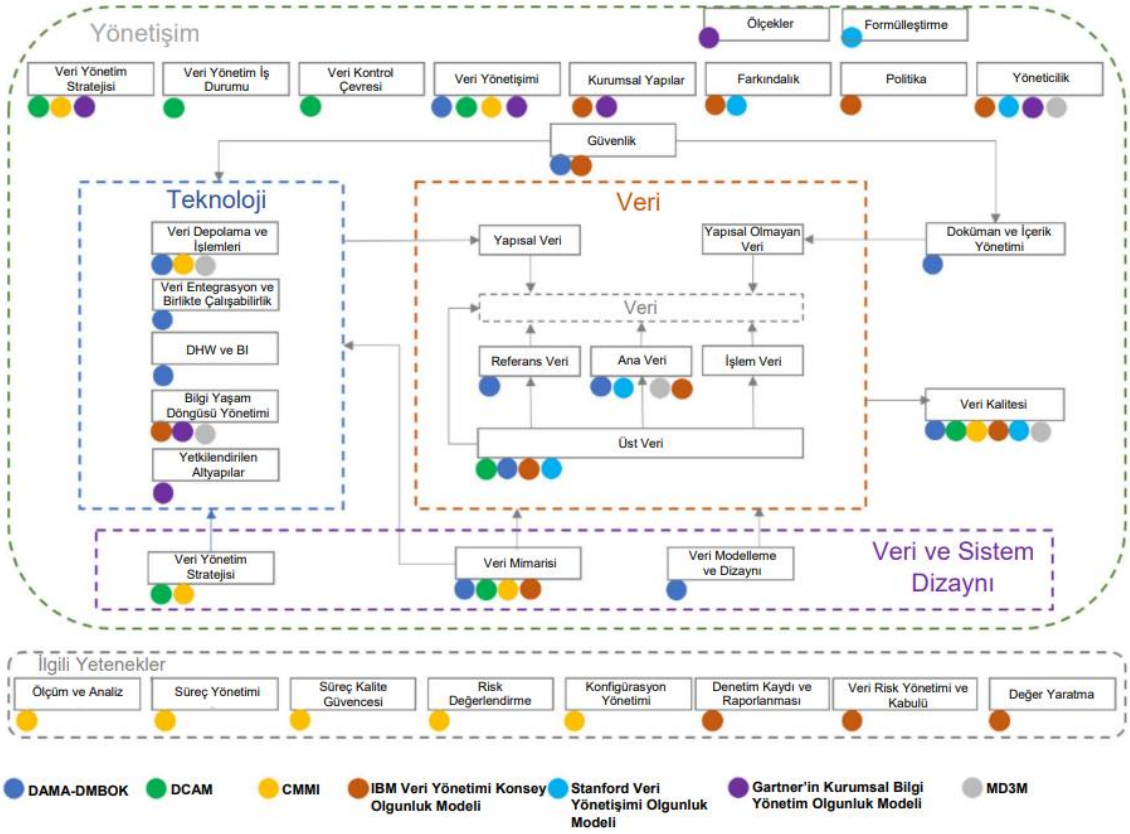
- Veri Mimarisi,
- Veri Yönetişimi,
- Veri Modelleme ve Tasarım,
- Veri Tabanı Yönetimi, Veri Depolama ve Operasyonlar,
- Veri Güvenliği Yönetimi,
- Veri Entegrasyonu ve Birlikte Çalışabilirlik,
- Referans ve Ana Veri Yönetimi,
- Veri Yaşam Döngüsü Yönetimi,
- Üst Veri Yönetimi,
- Veri Kalitesi Yönetimi,
- Veri Ambarı, İş Zekâsı ve Gelişmiş Analitik Yönetimi.

Gordon (2022) veri yönetiminin bir kurum ve kuruluşa sağlayacağı faydaların iş süreçleriyle ilgili, bilgi sistemleri ve bilgi teknolojisi ilgili olarak iki alanda değerlendirmiştir. Veri yönetiminin sağladığı ana fayda, farklı bilgi sistemleri arasında veri paylaşımıyla bilginin mevcudiyetindeki artma ve veri kalitesindeki iyileşmedir. Bu faydalar kurum ve kuruluşun etkinlik ve verimliğinin iyileşmesi, işletme ve yatırım maliyetlerinin azalması, faaliyet alanıyla ilgili yerine getirilen hizmetlerin geliştirilmesi ve rekabet gücünün artmasıdır. Veri yönetiminin bilgi sistemleri ve bilgi teknoloji ile ilgili faydaları ise; veri tanımlamalarının ve veri/bilgi analizi sonuçlarının tekrar kullanılması sistem geliştirmeye ilişkin maliyetin azalması ve verimliğinin artması, ortak veri tanımlamalarının ve veri yönetim yaklaşımlarının sonucu olarak uygulamaların bakım maliyetlerinde tasarruf sağlanmasıdır. Bununla birlikte, kurum ve kuruluş çapında etkili bir veri yönetiminin olmaması;

- Bilgi sistemlerinin birlikte çalışacak şekilde tanımlanmaması ve geliştirilmemesi sebebiyle, bu sistemler arasında ara yüz birleştirilmesinin yapılamamasına,
- Bilgi sistemleri arasında veri iletişiminin yapılamamasına,
- Veri paylaşımı engelleri sebebiyle iletişimin bozulmasına ve bilgilerin kaybolmasına,
- Uyumsuz bilgi sistemleri arasında bilgi paylaşımının sağlanması maksadıyla bir sistemdeki verilerin diğer sistem/sistemlerde yeniden gereksiz yere oluşturulmasına veya yanlış şekilde kopyalanmasına,
- Bir bilgi sistemine yönelik yapılan veri ve bilgi ihtiyacı analizi ile karşılanan veri tabanı gereksinimlerinin her yeni bilgi sistemi için tekrarlanmasına,
- Kurum ve kuruluşun rekabet gücünün azalmasına,
- Bilgi sistemi kullanıcılarının zamanında doğru bilgiye ulaşamamasına neden olmaktadır (Gordon, 2022).

Veri yönetimi çerçevesini tanımlamak için birçok yapı mevcut olmakla birlikte, the Global Data Management Community (DAMA International) ve CMMI Institute (CMMI) tarafından sağlanan yapılar yaygın olarak kullanılan ve en köklü veri yönetimi çerçeveleridir (Wallis, 2021). Defize (2020) tarafından yapılan çalışmada, 7 adet veri yönetimi modeli değerlendirilmiş ve 13'ü iki veya daha fazla modelde örtüşen toplam 32 yetenek tespit edilmiştir. Söz konusu veri yönetimi yetenekleri Şekil 10’da

haritalanmıştır. Bu bağlamda, veri yönetimi modellerinde en çok bulunan yetenekler, veri yönetişimi, veri kalitesi, üst veriler, veri mimarisi ve ana veri yönetimidir. İkiden fazla veri yönetim modelinde bulunan yetenek tanımları modele göre farklılık gösterebilmektedir.



Şekil 10. Veri Yönetimi Model Yeteneklerinin Haritalanması (Defize, 2020, s. 17).

3.4.1. Veri Yönetimi Stratejisi

Veri stratejisi, bir kuruluşun ihtiyaç ve hedeflerini karşılamak için verilerin yönetimine ilişkin süreçleri kapsamaktadır. Veri stratejisi, bir kuruluşun veri varlıklarının yönetilmesiyle birlikte veri kalitesi, veri entegrasyonu, veri güvenliği ve veri analizi gibi konuları ele almaktadır. Veri stratejisi, kurumsal hedefleri desteklenmek ve rekabet avantajı elde etmek için bilgiyi kullanmaya yönelik iş planlarını içermektedir. Veri stratejisi, bir kuruluşun hangi verilere ihtiyaç duyduğu, bu verilerin nasıl elde edileceği, nasıl yönetileceği, zaman içinde güvenilirliğinin nasıl sağlanacağı ve nasıl kullanılacağı dahil olmak üzere iş planının doğasında bulunan veri gereksinimlerinin belirlenmesiyle ortaya çıkmaktadır (DAMA International, 2017, s.32).

Veri yönetimi stratejisi, veri yönetimi programının vizyonunu, hedefleri ve amaçlarını tanımlamakla birlikte, tüm paydaşlar tarafından programın uygulanmasını sağlamaktadır (CMMI, 2019). Kuruluş tarafından veri yönetimi stratejisi belirlendikten sonra, bu strateji onaylanmalı, kurum ve kuruluşun tüm alanlarında uygulanmalı ve denetlenmelidir. Çeşitli faaliyet alanlarında hizmet gösteren kurum ve kuruluşların veri yönetimi stratejilerinin içerikleri farklı olmakla birlikte, veri yönetimi stratejisi genellikle şu konuları içermektedir (Gordon, 2022):

- Kurum ve kuruluşun rolleri ve sorumlulukları,
- Veri kalitesi,
- Veri entegrasyonu,
- Veri gizliliği ve güvenliği,
- Yapısal olmayan verileri yönetimi,
- Verilerin arşivlenmesi,
- İş zekası konuları,
- Veri modelleme standartları,
- Veri adlandırma,
- Üst veri,
- Veri tabanı yönetim sistemi seçimi,
- Yazılım uygulaması seçimi ve kullanımı,
- Masaüstü veri tabanlarının kullanımı,
- Kurum ve kuruluş dışı paydaşlar tarafından kurum ve kuruluşa ait verilerin kullanımı,
- Bulut işlem konuları,
- Verilerin iş değeri ve yatırım getirisinin belirlenmesi.

3.4.2. Veri Yönetişimi

Veri yönetişimi (data governance) sıklıkla veri yönetimi (data management) kavramı ile karıştırılmakla birlikte, veri kalitesi, ana veri yönetimi, veri güvenliği, üst veri yönetimi gibi veri yönetiminin temel bir bileşenidir. Veri yönetişimi, veri yönetimine ilişkin yetki ve kontrolün uygulanması ve bu uygulamaya yönelik faaliyetlerden oluşmaktadır (Strengholt, 2020).

Veri yönetişimi, veri kullanımında istenilen davranışların teşvik edilmesine yönelik hakların ve sorumlulukların çerçevesini oluşturmaktadır. Bu çerçeveyle kuruluşlar, misyon, norm, değer, strateji ile kültürleriyle ilişkili kuruluş genelinde veri politikaları, yönergeleri ve standartları geliştirmekte ve uygulamaktadır (Weber ve diğerleri, 2009, s.6). Veri yönetişimi, belirli modellere dayanan ve kimin ne zaman, hangi koşullarda, hangi bilgileri kullanabileceğini belirten, bilgi ile ilişkili süreçler için karar verme hakları ve sorumlulukları içeren bir sistemdir (Data Governance Institute, 2023).

Veri yönetişimi, bir kuruluşun bilgilerin etkili ve verimli bir şekilde kullanılmasına ilişkin politika, süreç, rol, standart ve metrikler topluluğudur. Veri yönetişimi, kullanılan verilerin kalite ve güvenliğinin temin edilmesi kapsamında süreç ve sorumlulukların belirlemekle birlikte, veriler üzerinde gerçekleştirilecek faaliyetlerle ilgili kişi, durum, eylem ve yöntemleri tanımlamaktadır (Talend, 2023).

Avrupa Birliği Genel Veri Koruma Tüzüğü, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, Kişisel Verilerin Korunması Kanunu gibi yasal düzenlemelerin gereği olarak, veri yönetimine ilişkin sorumlulukların belirlenmesi ve gerekliliklerin sağlanması kuruluşlar için veri yönetişimi ihtiyacını doğurmaktadır. Söz konusu yasal düzenlemeler, verilerin nereden kaynaklandığı, nerede ve ne şekilde saklandığı, ne için kullanıldığı ve nasıl kullanıldığını belirlememizi ve bunları açıkça belgelendirmemizi gerektirmektedir. Bu sebeple, kurum ve kuruluşlar tarafından yetkin ve etkin bir veri yönetişimi süreçlerinin oluşturulması gerekmektedir. Üst düzeyde uygulanan bir veri yönetişimi şu boyutları kapsamaktadır (Strengholt, 2020):

- Organizasyon boyutu: Veri sahipleri, veri kullanıcıları ve uygulama sahipleri gibi yapıların, rollerinin ve açık bir şekilde sorumluluklarının tanımlanmasıyla ilgidir. Söz konusu farklı roller çoğunlukla, veri yönetiminin uygun şekilde sağlanması için gereken sorumlulukları, rolleri, kuralları, etkinlikleri ve yönergeleri belirleyen iyi tasarlanmış bir veri yönetişimi çerçevesinde bir araya gelmektedir.
- Süreç boyutu: Süreçlerin kontrolü, denetlenmesi ve izlenmesinin nasıl yapılacağı ile ilgilidir.
- Teknoloji boyutu: Temel olarak veri yönetişiminin kontrol altında kalmasına izin veren arayüz, araç ve çerçevelerin standartlaştırılmasıyla ilgilidir.

- İnsan boyutu: Etik dengeler, yasal hususlar, sosyal ve ekonomik hususlar ile önyargılar gibi insani yönlere odaklanılmasıyla ilgilidir.
- Veri boyutu: Verilerin köken, tanım, sınıflandırma gibi veri varlıklarının kendilerine odaklanılmasıyla ilgilidir.

3.4.3. Veri Mimarisi

Bir kurum ve kuruluşta mimarlık uygulaması çeşitli seviyelerde (kurumsal, etki alanı, proje vb.) ve çeşitli odak alanlarında (altyapı, uygulama ve veri) gerçekleştirilmektedir. İş, veri, uygulama ve teknolojik alan mimarilerinin tümü kurumsal mimari alanına dahildir. Doğru şekilde yönetilen kurumsal mimari teknikleri, kurum ve kuruluşlara sistemlerinin mevcut durumunu anlamada, gelecekteki bir duruma doğru istenen değişimi teşvik etmede, mevzuata uyumu kolaylaştırmada ve verimliliği artırmada yardımcı olmaktadır. Mimari disiplinler yelpazesi boyunca birleştirici bir hedef, verilerin depolandığı ve kullanıldığı sistemlerin verimli bir şekilde yönetilmesidir (DAMA International, 2017, s.98).

Veri mimarisi, veri ana planıdır (Strengholt, 2020). Veri mimarisi, bir kurum ve kuruluşta verilerin nasıl bir araya geldiği ve verilere ait daha büyük bir resmin çizilmesi ile ilgilidir (Inmon ve diğerleri, 2019). Çoğu kurum ve kuruluşta tek bir kişinin kavrayabileceğinden daha fazla verinin bulunması sebebiyle, kurumsal verilerin anlaşılabilmesi ve kararların alınabilmesi için verilerin çeşitli soyutlama düzeylerinde tasvir edilmesi gerekmektedir. Bu sebeple veri mimarisi, veri yönetiminin temelini oluşturmaktadır (DAMA International, 2017, s.98).

Lewis ve diğerlerina (2001, s.1) göre veri mimarisi, verilerin bir sistem içinde nasıl depolandığını, yönetildiğini ve kullanıldığını tanımlamakla birlikte, bir veri mimarisi özellikle;

- Verilerin kalıcı olarak nasıl depolandığını,
- Bileşen ve süreçlerin bu verileri nasıl referans aldığı ve kullandığını,
- Verilere eski/harici sistemler tarafından nasıl erişildiğini,
- Eski/harici sistemler tarafından yönetilen verilere ilişkin arayüzleri,
- Ortak veri işlemlerinin uygulanmasını betimlenmektedir.

Veri mimarisi yapıları, hali hazırda ki durumun açıklanması, veri ihtiyaçlarının belirlenmesi, veri entegrasyonunun yönlendirilmesi ve veri varlıklarını bir veri stratejisinde ana hatlarıyla belirtildiği şekilde yönetmek için kullanılan tanımlamaları kapsamaktadır. Bir kurum ve kuruluşun veri mimarisini birlikte tanımlayan, çeşitli soyutlama düzeylerinde yazılmış, entegre bir ana tasarım belgeleri grubu, verilerin nasıl toplandığını, depolandığını, düzenlendiğini, kullanıldığını ve atıldığını kontrol eden yönergeler içermektedir. Bir kurum ve kuruluşun ihtiyaçlarını tam olarak desteklediğinde kıymetli hale gelen kurumsal veri mimarisi, kurum ve kuruluş çapında tutarlı veri standardının oluşmasını ve entegrasyonunu sağlamaktadır. Bir kurumsal veri mimarisi uygulaması genellikle sıralı veya eş zamanlı olarak yürütülen iş akışları şunlardır (DAMA International, 2017, s.110):

- Strateji: Çerçevelerin seçilmesi, yaklaşımlarının belirtilmesi ve yol haritasının geliştirilmesidir.
- Kabul ve kültür: Davranıştaki değişikliklerin bilgilendirilmesi ve motive edilmesidir.
- Organizasyon: Sorumluluk ve hesap verilebilirliğin atanmasıyla veri mimarisi çalışmalarının düzenlenmesidir.
- Çalışma yöntemleri: Kurumsal mimari ile birlikte, en iyi uygulamaları tanımlamak ve geliştirme projelerinde veri mimarisi çalışmalarını gerçekleştirmektir.
- Sonuçlar: Genel bir yol haritası kapsamında veri mimarisi yapılarının oluşturulmasıdır.

3.4.4. Veri Modelleme ve Tasarımı

Veri modelleme ve tasarımı, verileri belirli bir bağlam ve belirli sistemler içinde yapılandırmak ve temsil etmekle ilgili olup, veri gereksinimlerini keşfetmek, tasarlamak ve analiz etmek bu disiplinin bir parçasıdır (Strengholt, 2020). Veri modelleme ve tasarımı, verileri toplamak, depolamak, saklamak, arşivlemek, sorgulamak ve kullanmak için gerekli olan tüm işlemleri kapsamaktadır. Veri modelleme, veriyi algılamak için gerekli kuralların oluşturulmasını sağlamaktadır. Veri tasarımı ise, veriyi yönetmeye, erişilebilirliğini artırmaya, veriler arasındaki ilişkileri tanımlayıp bunların daha iyi anlaşılmasını sağlamaya ve daha faydalı bilgi elde etmeye yönelik stratejileri temin etmektedir.

Kurumsal yapılarda veri modeli sadece bir proje ile sınırlandırılmayarak, tüm veri gereksinimlerini kapsaması gerekmektedir. Bu sebeple, bir kurum ve kuruluşun tüm veri ve bilgi ihtiyaçlarının karşılanması amacıyla tek bir kavramsal veri modelinin tasarlanması ve geliştirilmesi gerekmektedir. Bu bağlamda, kurum ve kuruluşun ana faaliyetine dayalı olarak yukarıdan aşağıya geliştirilen bir çerçeve modeli, ayrı proje ve iş alanlarının modellemelerinde bir iskelet olarak kullanılabilmekte, söz konusu proje veya iş alanlarının modelleri bu iskeletin üzerine inşa edilmekte ve sonrasında ihtiyaç duyulduğunda kolaylıkla birleştirilebilmektedir. Bu kapsamda, kurumsal veri modellerinin geliştirilmesine ilişkin ilkeler şöyledir (Gordon, 2022):

- Modelin yukarıdan aşağıya geliştirilmesi: Faaliyetlerin ana unsurlarını ve kavramlarını temsil eden bir çekirdek veya çerçeve modelinden başlayarak kurumsal veri modelini yukarıdan aşağıya oluşturulmasıdır.
- Kuruluşun ana faaliyet alanına öncelik verilmesi: Çeşitli hizmet alanlarında faaliyet gösteren kuruluşların farklı ana işleri bulunması sebebiyle kurumsal veri modeli geliştirilirken kuruluşun temel işleri dikkate alınması gerekmektedir. Örneğin, ana faaliyeti mal satışı olan bir kuruluşun kurumsal veri modelinin çekirdeğini insan kaynakları bölümünün veri gereksinimlerinden ziyade, satışlara ve ürünlere dayalı olmaktadır.
- Modelin tüm kuruluşu kapsaması: Kurum ve kuruluşun ana faaliyeti ile ilgili olarak geliştirilen veri modeli kuruluş genelinde tüm veri ve bilgi ihtiyaçlarını desteklemesi gerekmektedir. Bu sebeple, veri modeli geliştiricilerinin kuruluşun tüm iş alanları hakkında bilgiye sahip olması gerekmektedir.
- Modelin geleceğe dönük olması: Kurumsal veri modelinin “geleceğe dayanıklı” zaman içerisinde kalıcılığının bozulmaması gerekmektedir. Bu sebeple model, veri ve bilgilerin analiz esnasında nasıl kullanıldıklarından ziyade, iş süreçlerinde kullanılan veri ve bilgilerin gerçek doğasını temsil etmelidir.
- Modelin işbirliği içinde geliştirilmesi: Kurumsal veri modelinin sadece bir veri yönetimi veya veri modelleme ekibi tarafından geliştirilmesi imkansızdır. Veri modeli ekibinin, kuruluşun ilgili uzman personeli ile mevcut ve gelecekteki bilgi sistemlerinin geliştirilmesinin sorumlu olan personel ile sürekli dirsek temasıyla çalışmalıdır.
- Fikir birliği elde edilmesi: Veri modelleme ekibinin mükemmel model geliştirmek için arayışa girmesi, etkili veri yönetiminin uygulanmasında

gecikmeye sebebiyet verebilmektedir. Bu sebeple, kuruluş genelinde tüm iş alanları için uygun görülen bir veri modeli üzerinde fikir birliğine varılmalıdır.

3.4.5. Veri Tabanı Yönetimi

Veri tabanı yönetimi, verilerin toplanması, saklanması, organize edilmesi, korunması ve verilere erişilebilmesi için veri tabanı tasarımının yönetilmesi, doğru olarak kullanılması ve desteklenmesini ifade etmektedir (Strengholt, 2020). Veri tabanı yönetimi, yazılım yönetimi ve kontrolü yordamıyla verilere erişme süreciyle ilgilidir. Kurum ve kuruluşlar tarafından verilerin kayıt altına alınması maksadıyla kullanılan veri tabanı yönetim sistemlerinin yönetim sorumluluğu çoğunlukla veri tabanı yöneticilerindedir. Veri tabanı yöneticilerin söz konusu sorumlulukları şunlardır (Gordon, 2022):

- Veri tabanı yönetimi süreçlerini belirleyen teknik standartların geliştirilmesi ve yürütülmesi: Veri tabanı yönetimine ilişkin prosedür ve süreçlerinin gerçekleştirilmesi maksadıyla, diğer iş süreçlerinde olduğu gibi veri tabanı yönetimine özgü teknik standartlara ihtiyaç duyulmaktadır. Söz konusu standartlar, kuruluş genelinde veri paylaşımı ile birlikte çalışabilirlik hususları dikkate alınarak ve son kullanıcıların verilere nasıl erişim sağlayacağını ifade edecek şekilde geliştirilmelidir.
- Fiziksel veri tabanı tasarımı: Veri tabanı tasarımları, genellikle veri tabanı yöneticileri tarafından kuruluşa ait veri standartlarına uygun olarak geliştirilmektedir. Bununla birlikte, söz konusu veri tabanı tasarımının veri tabanı yöneticilerinin haricinde, kuruluş içi uygulama geliştiricileri veya kuruluş dışı yazılım ve hizmet sağlayıcılarınca geliştirilmesi durumunda, tasarımın kuruluşa ait veri standartlarına uygunluğu kontrol edilmelidir. Veri tabanı tasarımlarının zamanla ortaya çıkacak veri gereksinimlerini karşılaması için veri yönetimi ve veri tabanı yöneticilerinin dirsek temasında bulunması gerekmektedir.
- Veri tabanı yönetim sistemine ilişkin yazılımının yönetimi: Veri tabanı yöneticisi, kullanıcıların erişim haklarının düzenlenmesi ile veri tabanı işlevselliğinin iyileştirilmesi, güvenliğinin yönetimi ve yazılım güncellemelerin yapılmasını sağlaması gerekmektedir.

- Veri tabanı yönetimi kapsamındaki eğitimler: Veri tabanı yöneticileri, veri tabanı yönetimi kapsamında mesleki yetkinliklerini sürdürebilmeleri için sürekli olarak gerekli eğitimleri almalıdırlar.

3.4.6. Veri Güvenliği

Günümüzde veri yönetiminin en önemli yönlerinden biri veri güvenliğinin sağlanmasıdır (Talend, 2023). Veri güvenliği, verilerin izinsiz veya kötü amaçlı erişimine, değiştirmesine, yok edilmesine veya ifşa edilmesine karşı alınması gereken önlemleri ifade etmektedir. Veri Güvenliği, veri ve bilgi varlıklarına yetkili erişimin sağlanması kapsamında, kimlik doğrulama, erişim yetkilendirilmesi ve erişim denetimi süreçlerini gerçekleştirmek maksadıyla güvenlik ilkelerinin ve politikalarının planlanması, geliştirilmesi ve uygulanması içermektedir. Veri güvenliği faaliyetlerinin amacı ise, koruma ve gizlilik ilkeleri ve politikalarına göre uygunluğun sağlanması, verilere yetkili erişimin sağlanması ve yetkisiz erişimin önlenmesi ile paydaşların mahremiyetlerinin sağlanmasıdır. Bir kurum ve kuruluştaki veri güvenliğinin rehber ilkeleri şunlardır (DAMA International, 2017, s. 222):

- İşbirliği: Veri güvenliği, veri yöneticilerini, bilgi teknolojileri güvenlik yöneticilerini, kurum içi ve kurum dışı denetçilerini ve hukuk kısmından oluşan ortak bir çalışmadır.
- Kurumsal yaklaşım: Veri güvenliği standartları ve politikaların kuruluş çapında tutarlı olarak uygulanmalıdır.
- Proaktif yönetim: Başarılı bir veri güvenliği yönetimi, proaktif ve dinamik olunmasına, tüm paydaşları dahil edilmesine, değişimin yönetilmesine ve bilgi teknolojisi, bilgi güvenliği, veri yönetimi ve paydaşlar arasındaki süregelen sorumluluk paylaşımı gibi kurumsal veya kültürel zorlukların üstesinden gelinmesine bağlıdır.
- Açık olarak hesap verebilirlik: Kurum ve kuruluş genelindeki veriler için “gözetim zinciri”ni de içeren roller ve sorumluluklar açıkça tanımlanmalıdır.
- Üst verilere dayalı olmak: Verilerin güvenlik sınıflandırılmasının yapılması veri tanımlarının önemli bir parçasını oluşturmaktadır.
- Maruz kalmanın indirgenerek riskin azaltılması: Üretim olmayan ortamlarda gizli/hassas veriler asgari olarak çoğaltılmalıdır.

Veri yönetiminin diğer boyutlarında olduğu gibi, veri güvenliğinin bir kurumsal girişim olarak ele alınması gerekmektedir. Bu bağlamda, kurum ve kuruluş genelinde bir veri güvenliği politikası oluşturulmalı ve bu politika farklı güvenlik korumasına sahip veri kategorilerini ve kimin hangi kategorideki verilere erişimi olması gerektiğini belirtmelidir. Veri güvenliği politikası, verilerin yönetim sürecinde bulunan tüm personel tarafından veri güvenliği konusundaki rollerinin açık ve basit bir şekilde anlayabilmelerini sağlamalıdır (Gordon, 2022).

Veri güvenliğine ilişkin çoğu strateji kimlik doğrulama, yetkilendirme ve izlenebilirlik tekniklerini içine alan üç yönlü bir yaklaşımı kullanmaktadır. Söz konusu yaklaşımla, verilere sadece yetkili kullanıcıların erişebilmeleri sağlanmaktadır. Bu üç yönlü yaklaşımın ana amacı, güvenliğin sağlanması için korunan herhangi bir kaynağın yetkisiz kullanımını önlemektir. Bu görevin yerine getirilmesine yardımcı olabilecek kimlik doğruluma ve erişim denetimi kapsamına giren unsurların bazıları Tablo 4'te gösterilmiştir. Veriye erişim, bir kullanıcının kimliği doğrulanmasının ardından, koruması sağlanan kaynağa sadece yetkili kişilerin erişilebilirliğinin garantilenmesi erişim denetimlerinin yardımıyla sağlanmaktadır (Kim ve Solomon, 2019, ss. 127-128).

Tablo 4. Kimlik Doğrulama ve Erişim Denetiminin Unsurları
(Kim ve Solomon, 2019, s. 128)

Kimlik Doğrulama Unsurları	Erişim Denetimi Unsurları
• Parola ve Kimlik Numaraları	• Kimlik Doğrulama Sunucu Kuralları ve İzinleri
• Akıllı Kartlar ve Belirteçler	• Erişim Kontrol Listeleri
• Biyometrik Cihazlar	• Saldırı Tespit ve Önleme
• Dijital Sertifikalar	• Fiziksel Erişim Kontrolü
• Meydan Okuma-Cevap El Sıkışmaları	• Bağlantı ve Erişim Politikası Filtreleri
• Kerberos Kimlik Doğrulaması	• Ağ Trafiği Filtreleri
• Bir Kerelik Şifreler	

Bir kurumda hangi verilerin korunması gerektiğinin belirlenmesi için yapılan veri sınıflandırılmaları veri güvenliğinin temel aşamasıdır. Söz konusu sınıflandırma süreci ise genellikle şu adımları içermektedir (DAMA International, 2017, ss. 220-221):

- Hassas veri varlıklarının tanımlanması ve sınıflandırılması: Kurum ve kuruluşun özelliğine bağlı olarak az veya çok sayıda varlık ve çeşitli hassas veri (kişiyi tanımlayan, tıbbi, finansal vb. veriler dahil) mevcut olabilir.

- Kuruluş genelinde hassas verilerin tespit edilmesi: Verilerin saklandığı yere göre güvenlik gereksinimleri değişkenlik gösterebilmektedir. Hassas verilerin tek bir konumda bulunması, tek bir ihlalden kaynaklanabilecek zarar sebebiyle yüksek bir risk oluşturmaktadır.
- Her bir varlığın nasıl korunması gerektiğinin belirlenmesi: Güvenliğin sağlanmasına ilişkin alınması gereken önlemler, teknolojisinin türüne ve verinin içeriğine bağlı olarak varlıklar arasında değişiklik gösterebilmektedir.
- Bu bilgilerin iş süreçleriyle nasıl etkileşime girdiğinin tanımlanması: Hangi koşullar altında hangi erişime izin verildiğinin belirlenmesi için iş süreçlerinin analiz edilmesi gerekmektedir.

Gordon (2022)'a göre veri güvenliği, veri tabanının yetkisi olmayan kişilere karşı korunmasıyla ilgili olup, gizliğin korunması için yetkisiz kişiler tarafından verilere ulaşılamaması ve verilerin kasıtlı olarak bozulmasının engellenmesidir. Bu bağlamda veri güvenliği süreçleri erişim kontrollerini, şifrelemeyi ve herhangi bir güvenlik ihlali ile karşılaşıldığında kim tarafından ne yapılacağını belirten denetim izlerini içermektedir. Söz konusu süreçler şunlardır (Gordon, 2022):

- Erişim kontrolleri: Oturum açma ve ilişkili parolalar gibi kimlik doğrulama yöntemlerine dayanmaktadır. Veri erişim hakları, oturum açma bilgilerine göre kişilere veya benzer rollere sahip kişi gruplarına verilmektedir. Erişim kontrolünün amacı, veri tabanını kullanan kişilerin sadece sahip oldukları rollerle ilgili verileri okuyabilme, oluşturabilme, güncelleyebilme veya silebilmelerine imkan sağlamaktadır.
- Şifreleme: Erişim kontrolleri atlanarak veri dosyalarına olası erişimin engellenmesi için veri tabanı şifrelenebilmektedir. Bu şifreleme, bazı verilere ya da tüm veri tabanına uygulanmaktadır. Tüm veri tabanını şifrelemek en kolay seçenek gözükmesine rağmen, verilerin okunması gerektiğinde veri tabanı şifresinin çözülmesi ve güncellenmesi gereken verilerin yeniden şifrelenmesi gerekmekte olup, bu işlemler veri tabanının performansını etkilemektedir. Bunun alternatifi ise, veri tabanında şifrelenmesi gereken sütunlardaki verilerin (kredi kartı veya kişisel bilgilerinin tutulduğu sütunlar gibi) şifrelenmesidir.
- Denetim izleri: Yetkisiz erişimi engellememekle birlikte, güvenlik ihlallerine ilişkin bilgileri sağlamaktadır. Veri tabanı yönetim sistemlerinin çoğu kim

> tarafından hangi veri tabanı varlıklarına ne zaman erişildiğini kayıt altına alarak veri tabanı işlemlerinin izlerini tutmakla birlikte, denetim izlerinin bazıları hangi verilerin değiştirildiğinin kayıt altına alınmasına olanak sağlamaktadır. Denetim izlerinin bu fonksiyonları veri güvenliğinin artırılmasına yardımcı olmaktadır**.**

Strengholt (2020)'a göre veri güvenliği yönetimi, yetkilendirme, kimlik doğrulama ve verilere erişim sağlayan tüm disiplin ve faaliyetleri içermektedir. Verilerin güvenliğinin uygulanması için önerilen yaklaşım ise güvenlik gereksinimlerinin sürecin başından itibaren mimariye dahil edilmesidir. Güvenlik risklerinin başarılı olarak incelenmesi için iki kontrol seviyesine odaklanılması gerekmektedir. Veri güvenliği kontrollerin ilk seviyesi, kimlik sağlayıcıları, veri şifreleme, veri maskeleme, veri erişimi ve veri kullanımını izlemeyi içermektedir. İkinci seviyi oluşturan altyapı seviyesinde ise güvenlik duvarları, izolasyon, ağ şifreleme gibi konulara odaklanılmaktadır.

Veri güvenliği, veri ve veri varlıklarının tanımlanması ve sınıflandırılmasıyla birlikte, kimlik doğrulama, erişim kontrolleri, şifreleme mekanizmaları, güvenlik duvarları, anti virüs yazılımları gibi çeşitli araç ve yöntemlerle sağlanmaktadır. Ayrıca, kurum ve kuruluş çalışanlarının veri güvenliği konusunda farkındalıklarının artırılması ve veri güvenliği politikalarına uygun hareket etmelerini sağlamak için sıklıkla veri güvenliği yönetimi hakkında eğitim almaları önem arz etmektedir.

3.4.7. Veri Entegrasyonu ve Birlikte Çalışabilirlik

Veri entegrasyonu ve birlikte çalışabilirlik, verilerin bir kaynaktan diğer bir kaynağa verimli bir şekilde aktarılması kapsamında, verilerin taşınması, toplanması, birleştirilmesi, kaynaştırılması ve dönüştürülmesine ilişkin tüm faaliyetleri içermektedir (Strengholt, 2020). Veri entegrasyonu, fiziksel veya görsel olan bağlantılı formların içerisinde olan verilerin birleştirilmesidir. Birlikte çalışabilirlik ise iki ve daha fazla sistemin iletişim ve veri alışverişi yeteneğidir. Veri entegrasyonu ve birlikte çalışabilirlik, ihtiyaç duyulan verilerin ihtiyaç duyulduğu zamanda, ihtiyaç duyulan yerde ve ihtiyaç duyulan biçimde elde edilmesini içermektedir. Veri entegrasyonu ve birlikte çalışabilirlik faaliyet ve çözümlerinin uygulanmasının amaçları şunlardır (DAMA International, 2017, s. 272):

- Sistem ve insanların ihtiyaç duyduğu zaman diliminde ve formatta verilerin kullanılabilir hale getirilmesi,
- Verilerin sanal ve fiziksel biçimde veri merkezlerinde birleştirilmesi,
- Çözümlerin yönetilmesi kapsamında, paylaşılan model ve arabirimler geliştirilerek en düşük maliyetin ve karmaşıklığın sağlanması,
- Fırsat ve tehditlerin belirlenmesi, uyarı ve eylemlerin otomatik bir biçimde harekete geçirilmesi,
- Ana veri yönetimi, analitik, işletme verimliğinin ve iş zekasının desteklenmesidir.

Bir kurum ve kuruluş, veri entegrasyonu ve birlikte çalışabilirlik faaliyetlerini uygularken şu ilkeleri takip etmelidir (DAMA International, 2017, s. 272):

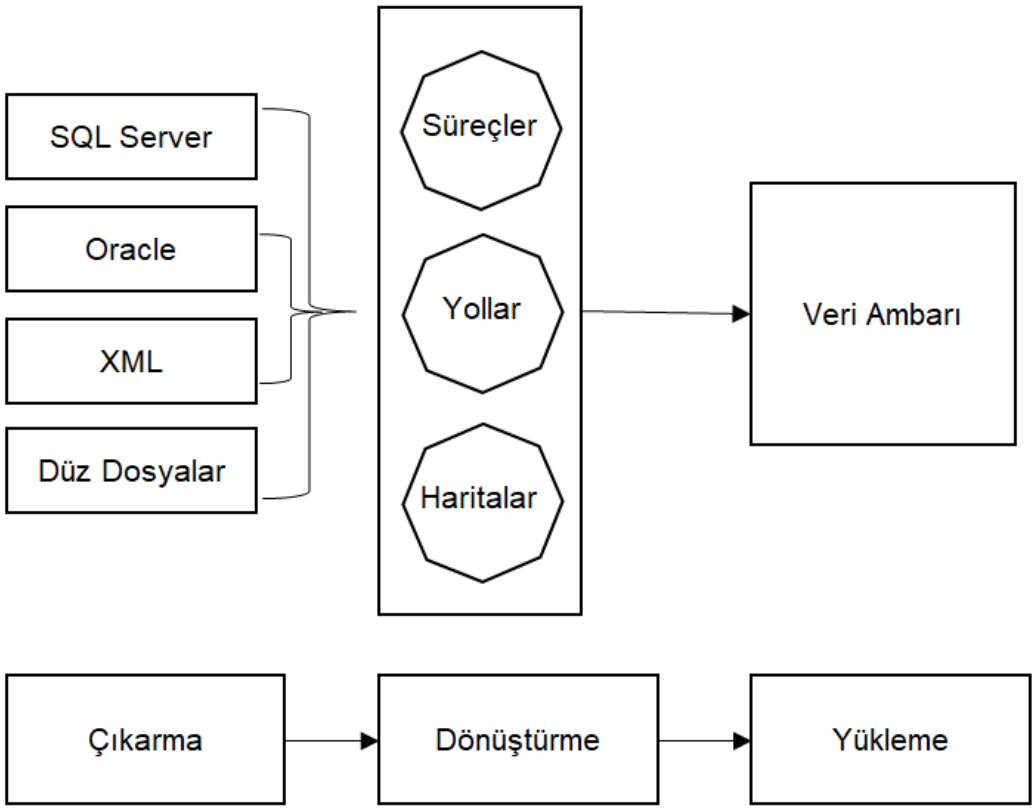
- Gelecekteki genişletilebilirliğin sağlanması kapsamında, tekrarlı ve artırımlı servis yoluyla uygulanan kurumsal bir bakış açısı benimsenmelidir.
- Destek ve bakım da dahil olmak üzere, kısmı veri ihtiyaçları kurumsal veri ihtiyaçları ile dengelenmelidir.
- Veri entegrasyonu ve birlikte çalışabilirlik faaliyetlerinin tasarımı ve etkinliği kapsamında, işletmedeki sorumluluklar belirlenmeli ve sürdürülmelidir. Bu çerçevede, işletme uzmanları veri dönüştürme kurallarının tasarım ve bu kuralların değişim süreçlerine dahil edilmelidir.

Veri entegrasyonu ve birlikte çalışabilirlik faaliyetinin tüm alanlarının merkezinde verinin çıkarılma (extract), dönüştürülme (transform) ve yüklenme (load) (ETL) süreci yer almaktadır (DAMA International, 2017, s. 273). Verilerin ambarlama süreçlerinde sıklıkla kullanılan ETL işlemleri, kaynak veri sistemlerinden (kaynak veri tabanları, dosya sistemleri vb.) verilerin çıkarılması, gerekli şekle dönüştürülmesi ve hedef veri sistemine (veri ambarı, veri tabanı vb.) yüklenmesidir. ETL süreci ve mimarisi Şekil 11'de sunulmuştur. ETL faaliyetine ilişkin süreçler şöyledir (Sreemathy ve diğerleri, 2020, ss. 1446-1447):

- Veri çıkarma: Çeşitli kaynaklardan veri çıkarma işlemi, genellikle ETL işleminde ayıklama adımı olarak adlandırılır. XML, ilişkisel veritabanları, düz dosyalar vb. dahil olmak üzere çeşitli veri çıkarma formatları kullanılır. Bozuk veriler veri ambarına kopyalanırsa, çıkarılan verileri geri almak zor

olacağından, veriler hemen veri ambarına değil, bir hazırlama alanına çıkarılır. Bu nedenle, veriler veri ambarına teslim edilmeden önce, bu aşama veri doğrulama için bir fırsat sağlar. Doğrulama işlemi sırasında keşfedilen hatalı veriler, tercihen hatalı değerleri belirlemek ve düzeltmek için kaynak sisteme geri gönderilir. Verileri fiziksel olarak çıkarmadan ve yüklemeden önce mantıksal bir veri haritası gereklidir. Bu diyagram, arasındaki bağlantıları göstermektedir.

- Veri dönüştürme: Bu süreçte, ayıklanan veriler, kullanıcının veya müşterinin ihtiyaç duyduğu formata dönüştürülür. Veriler orijinal biçiminde olmaması nedeniyle, işlenmesi için bir çeşit temizleme, haritalama ve dönüşümler gerektirmektedir. Toplama ve birkaç özelleştirme adımı burada gerçekleştirilebilir. Herhangi bir değişiklik gerektirmeyen veriler, doğrudan taşıma veya geçiş verileri olarak adlandırılır. Bu seviyede verilere özelleştirilmiş kullanıcı tanımlı eylemler uygulanabilir. Bu aşamada ana dönüşümler, veri ambarına yüklenecek verileri doğrulamak için gerçekleştirilir. Bu süreçte gerçekleştirilen temel dönüşümler şunlardır:
    - Temizlime,
    - Filtreleme,
    - Veri standardizasyonu,
    - Veri akışı doğrulaması,
    - Veri eşiği doğrulama kontrolü,
    - Satır ve sütun yer değiştirmesi,
    - Katılma,
    - Bölme,
    - Sıralama.
- Veri yükleme: Veriler, yükleme prosedürü sırasında nihai veya hedef veri tabanına yazılır. ETL işleminin son adımı olan bu aşamada veri tabanına büyük miktarda veri yüklenecektir. Veri ambarı yöneticilerin süreç devam ettiği esnada süreci yakından takip etmelidir. Veri yükleme sürecinde “İlk yükleme”, “Artırımlı yükleme” ve “Tam yenileme” olmak üzere üç yükleme çeşidi bulunmaktadır.



Şekil 11. ETL Mimarisi ve Süreci (Sreemathy ve diğerleri, 2020, s. 1447)

3.4.8. Referans ve Ana Veri

Referans veriler, bir kuruluştaki verileri tanımlamak, gruplandırmak, sınıflandırmak, organize etmek ve kategorilere ayırmak için veya bir veri tabanındaki verileri kuruluşun dışındaki bilgilerle ilişkilendirmek için kullanılan verilerdir (Strengholt, 2020). En temelde kodlardan ve açıklamalardan oluşan referans veriler karmaşık olabilmekte ve hiyerarşi ve eşlemeleri içerebilmektedir (DAMA International, 2017, 352). Bir konum veya bir para birimi için tanımlanan bir terim referans verinin bir örneğidir.

Ana veri, bir kuruluşun iş süreçleri ve hizmetleri için gerekli olan, birçok sistemde ve bölümde kullanılan verileri ifade etmektedir (Shen, 2019). Bir kuruluştaki ürünlerin kodları, müşterilerin isimleri ve adresleri, tedarikçilerin bilgileri gibi veriler ana veri örnekledir. Herhangi bir kuruluşun verileri Şekil 12'de gösterildiği gibi altı farklı düzeyde veya katmanda görülebilmektedir (Gordon, 2022).

Şekil 12. Verinin Altı Düzeyi (Gordon, 2022)

Üst veriler, verileri tanımlamaktadır. Referans veriler, verileri kategorize etmek veya kuruluş dışındaki bilgilerle ilişkilendirilmek için kullanılmaktadır. İşlem yapısı verileri, bir işlemin dolaysız katılımcılarını (ürün, tedarikçi, müşteri vb.) temsil etmektedir. Kurumsal yapı verileri, kurumsal yapıyı ve mali yapıyı açıklamaktadır. İşlem faaliyeti verileri, kuruluşun gerçekleştirdiği işlemlerle ilgili ayrıntıların kayıt edilmesidir. İşlem denetim verileri ise her bir işlemin kaydını tutan verilerdir. Bir kuruluşun ana verileri, referans verilerin, kurumsal yapı verilerinin ve işlem yapısı verilerinin birleşiminden oluşmaktadır (Gordon, 2022).

Referans ve ana veri yönetimi, verilerin erişilebilir, doğru, güvenli, şeffaf ve güvenilir olduğundan emin olmak için kritik verileri yönetmekle ilgilidir (Strengholt, 2020). Referans ve ana veri yönetiminin amacı ise; bir kurum ve kuruluşun, kurumsal süreçlerde eksiksiz, güncel, tutarlı ve yetkili referans ve ana verilere sahip olmasını temin etmek, verilerin kurumsal işlev ve uygulamalar boyunca paylaşılmasını sağlamak, veri kullanımı ve veri entegrasyonunun yaygın veri modelleri, standartlar ve entegrasyon kalıpları aracılığıyla veri kullanım karmaşıklığının azaltılması ve maliyetinin düşürülmesidir (DAMA International, 2017, ss. 349-350).

Gartner (2023) ana veri yönetimini, kuruluş tarafından resmi olarak paylaşılan ana verilerin doğruluğunun, hesap verilebilirliğinin, tekdüzeliğinin, semantik tutarlığının ve yönetiminin sağlanması için işletme ile bilgi teknolojisinin birlikte çalıştığı teknoloji

destekli bir disiplin olarak tanımlamıştır. Ana veri yönetimi, ana verinin kuruluş çapında nasıl oluşturulacağı, entegre edileceği, sürdürüleceği ve kullanılacağının tanımlanması ve yürütülme faaliyetidir (Smith, 2023).

Gordon (2022)'a göre, ana veri yönetiminin en temel amacı, bir kuruluşun tüm süreçleri için "ana verilerinin" tek bir sürümünü kullanmasını sağlamaktır. Bu sebeple, ana veriler, kuruluş, yer, kişi, ürün, hesap gibi kavramsal varlıkların her bir örneğine ilişkin gerçek ve güvenilir bir sürümün tanımlanması, geliştirilmesini ve bu sürümün geçerliliğinin korunmasını gerektirmektedir (DAMA International, 2017, s. 351). Ana veri yönetiminin hedefi ise net olmayan tanımlamalarla (bir varlığın birden fazla örneğiyle tanımlanması ve birden fazla varlığa atıfta bulunulması) ilişkili risklerin azaltılmasıyla birlikte, doğru ve geçerli değerlerin kullanılmasını temin etmektir (DAMA International, 2017,352).

3.4.9. Üst Veri Yönetimi

Üretilen veya toplanan verilerin belli standartlar ile kayıt altına alınması, bu verilerin bulunabilirliğini, birlikte çalışabilirliğini, paylaşılabilirliğini ve dolayısıyla kullanılabilirliğini etkilemektedir. Yapısal bir veri olan üst veriler diğer veriler hakkındaki bilgileri barındırmakta ve genellikle "veriler hakkında ki veriler" olarak tanımlanmaktadır. Verilerin neyle ilgili olduğu açıklayan üst veriler, veri içeriğinin kısa ve tutarlı bir açıklamasının yapılabilmesi için bir mekanizma sağlamaktadır. Üst veriler, veri setleri, veri tabanı, ürünler veya doküman varlıklarını tanımlamakla birlikte, olayların ne zaman, nerede ve kim tarafından gerçekleştiğini belirten detaylara sahiplerdir (Haselden ve Wolter, 2021).

Üst veriler, verilerin anlaşılır, entegrasyona hazır ve güvenli hale getirilmesi ile veri kalitesinin sağlanması için kullanılabilmektedir. Üst veri yönetimi ise verilerin sınıflandırılması ve açıklanması kapsamında tüm verilerin yönetilmesini içermektedir (Strengholt, 2020). Literatürde üst verilerin çok geniş bir tanımı bulunmasıyla birlikte, üst veriler şu bağlamlarda kullanılmaktadır (Gordon, 2022):

- Veri yönetimi için üst veriler: Klasik görüşe göre üst veriler bir veri tabanında bulunan veri türlerini tanımlamaktadır. Üst veriler; bir SQL veri tabanı yönetim sisteminde bulunan veri tabanı şemasının tablo ve sütun tanımlarını, veri

tabanındaki kısıtlama tanımlarını, veri tabanındaki verilerin kalitesinin korunması ve verilere erişilmesi kapsamındaki kuralları, kavramsal veri modelleri ile bunlardan üretilen veri tanımlarını ve modeldeki ilişkileri, veri tanımlarının kaynağını ve sahipliğinin ayrıntılarını, veri tabanlarına kayıt edilen verilerin tür ve konumların anlaşılmasına yardımcı olan bilgileri ifade etmektedir.

- İçerik yönetimi için üst veriler: Web sayfalarının içeriği ile kütüphane ve arşivlerde bulunan belgelerin içeriğini belirten veri ve bilgilerin tanımlaması kapsamında üst veriler artan oranda kullanılmaktadır. Dublin Core Üst Veri Element Kümesi üst verinin bu şekilde kullanımına yönelik bir örnektir. Çeşitli etki alanlarındaki metin, resim, ses, video ve web sayfaları gibi bilgi kaynaklarını tanımlamak için kullanılan Dublin Core standardının esnek olarak kullanılan 15 elemanı şunlardır (Dublin Core, 2023a):
    - Başlık: Bilgi kaynağının yazarı veya yayıncısı tarafından yapılan adlandırma belirtilmektedir.
    - Üretici: Bilgi kaynağını oluşturmaktan sorumlu olan varlık belirtilmektedir.
    - Konu: Bilgi kaynağı içeriğinin konusu belirtilmektedir.
    - Tanım: Bilgi kaynağının bir açıklaması olarak kullanılır.
    - Yayımcı: Bilgi kaynağına erişilebilmesini mümkün kılan varlıklar (basımevi, servis sağlayıcı, üniversite bölümü vb.) belirtilmektedir.
    - Katkıda bulunan: Bilgi kaynağının içeriğine katkı yapan varlık belirtilmektedir.
    - Tarih: Bilgi kaynağının yaşam döngüsü içerisindeki bir olayın zamanı veya tarih aralığı belirtilmektedir. Bu husus bilgi kaynağının oluşturulma tarihi ya da web sitesine eklenme tarihi olabilmektedir.
    - Tür: Bilgi kaynağının metin, görüntü, ses vb. türü belirtilmektedir.
    - Format (Biçim): Bilgi kaynağının dosya formatı, fiziksel veya sayısal ortamı (text/html gibi) belirtilmektedir.
    - Tanımlayıcı: Bilgi kaynağının benzerlerinden ayırt edilmesini sağlayan (Uluslararası Standart Kitap Numarası (ISBN) vb.) hususları belirtilmektedir.
    - Kaynak: Bilgi kaynağının hangi kaynak veya kaynaklardan faydalanılarak oluşturulduğu belirtilmektedir.
    - Dil: Bilgi kaynağının yazım dili belirtilmektedir.

  - İlişki: Bilgi kaynağı ile ilgili diğer bir kaynağı tanımlamak için kullanılır. Standardın bu elamanı ile bilgi kaynağının başka bir kaynağın bir parçası, çevirisi veya bir kitabın bir bölümü olduğuna ilişkin bilgileri barındırmaktadır.
  - Kapsam: Bilgi kaynağının uzaysal yeri (coğrafik koordinatlar vb.) ya da zamansal (bir tarih veya tarih aralığı) özellikleri belirtilmektedir.
  - Haklar: Bilgi varlığının telif hakkı bilgileri belirtilmektedir.
- Veri değerini açıklamak için üst veriler: Metin, görüntü (durağan/hareketli), ses, vb. multimedya verilerinin içeriğinin tanımlanması için kullanılan üst verilerdir. Bu üst verilerin bir kısmı multimedyanın bir parçası olarak tutulabilmektedir. Fotoğraf gibi durağan görüntüler BMP, JPEG, GIF, ve TIFF gibi birçok farklı biçimde saklanabilmekte ve değiştirilebilmektedir. Söz konusu standart formatlar üst verileri dosyanın içine yerleştirmektedir.

3.4.10. Veri Kalite Yönetimi

Veri kalitesi, verinin doğruluğu, tamlığı, tutarlığı, güncelliği ve güvenilirliği gibi özelliklerini ifade etmektedir. Veri kalitesinin boyutlarını oluşturan söz konusu özelliklerin ölçümleri sonucunda tespit edilen kalite seviyesi, veri hatalarının ve düşük kaliteli verilerin belirlenmesine yardımcı olmaktadır. Kalitesiz verilerin kalitesiz bilgiler üretmesi sebebiyle kuruluşların iş süreçleri ve karar verme yeteneği önemli şekilde etkilenebilmektedir. Gordon'a (2022) göre verilerin kalitesini düşüren hususlar şunlardır:

- Uygun olmayan şemalara sahip veri tabanları: Veri tabanlarının veri tekrarı olmayacak ve muhtemel gereksinimleri karşılayacak şekilde tasarlanması gerekmektedir. Veri tabanlarının, gelecekteki gereksinimleri esnek bir şekilde karşılayabilecek şekilde tasarlanmadığında, veri tabanının yeniden tasarlanmasının maliyetini karşılamak istemeyen kuruluşlar tarafından mevcut veri tabanlarında geliştirilen geçici çözümler veri kalitesini düşürme eğilimindedirler. Bu sebeple, veri tabanlarının tasarlanmasında esneklik ve veri kalitesi hususları göz önünde bulundurulmalıdır.
- Veri girişinde yapılan hatalar: Hatalı veri girişlerinin birçok nedeni olmakla birlikte, bu sebeplerin bazıları kazara bazıları ise kasıtlı olarak yapılmaktadır.

Veri girişlerinde bir tarihin veya ismin yanlış yazılması, yazım yanlışlıkları gibi hatalar veri kalitesini düşüren en yaygın örneklerdir.

- Zamanla azalan veriler: Verilerin değerleri zamanla azalmakta veya güncelliğin kaybetmektedir. Örneğin, insan kaynakları bölümünün iş süreçlerini destekleyen veri tabanlarında çalışanların niteliklerinde meydana gelen gelişim ve değişimler düzenli olarak güncellenmediğinde en uygun nitelikli personelin bulunması edilmesi zaman alacak veya tespit edilemeyecektir.
- Sistemler arasında taşınırken verilerin bozulması: Veriler sistemler arasında taşındığı zaman bozulabilmektedir. Söz konusu bozulma genellikle, değiştirilen besleyici sistemlerin dokümantasyonunun güncel tutulmaması ve bunun sonucunda verilerin dönüştürülmesi ve temizleme işlemlerinin uygun olmayan şekilde yapılmasından kaynaklanmaktadır.
- Kullanıldığında verilerin anlaşılmaması: Üst verilerin eksik veya anlamsız olması veya belgelerin güncel olmaması sebebiyle, veriler kullanıcılar tarafından anlaşılamamaktadır.

Verilerin kalite düzeyinin belirlenmesi için, genellikle veri varlıklarının envanterinin çıkarılmasından sonra veri setlerinin doğruluğunu, geçerliğini ve eşsizliğinin ölçülmesi için temel çalışmalar yapılmaktadır. Söz konusu çalışmaların sonucunda oluşturulan ana derecelendirmeler ile mevcut verilerin karşılaştırılması sonucunda verilerin kalitesine yönelik sorunlar tespit edilmektedir. Veri kalitesinin tespitine yönelik diğer bir yaklaşım ise, işlevsel ve analitik veriler için iş ihtiyaçlarına dayalı bir dizi veri kalitesi kuralının oluşturulmasıdır. Söz konusu kurallar veri kümelerine ilişkin kalite seviyelerini ifade etmekle birlikte, veri kalitesinin özellikleri açısından veri unsurlarının içeriklerini belirlemektedir. Kurum ve kuruluşlar tarafından bahse konu kurallar onaylandıktan sonra veri kalitesi değerlendirmesi yordamıyla veri hataları ve diğer sorunlar tespit edilerek veri kümelerinin kalitesi ölçülmektedir (TechTarget, 2023).

Bir kurum ve kuruluşun etkin ve kalıcı veri kalitesi elde etmesi için bir dizi prosedürü yerine getirmesi, kaliteli verilerin teşvik edilmesi ve bunların sürdürülmesi için kuruluşta bir kültürün oluşturulması ve uygulanması gerekmektedir (Gordon, 2022). Bu kapsamda, verinin karakteristik, durum veya özelliklerini içerisine alan veri kalite boyutları veri ve bilgi kalite ihtiyaçlarının sınıflandırılmasına yardımcı olmaktadır. Bu boyutlar, veri ve bilginin kalitesinin tanımlanması, ölçülmesi ve yönetilmesi için

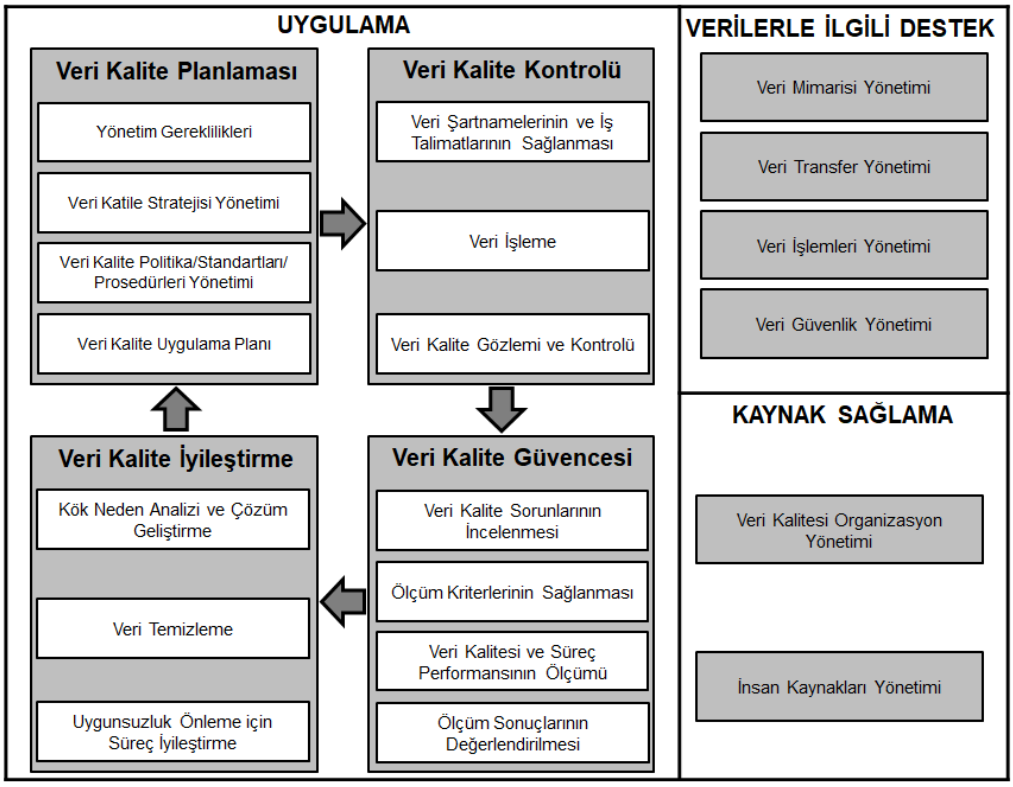
kullanılmaktadır (McGilvray, 2021, s.62). Gordon'a (2022) göre veri kalitesinin boyutları şöyledir:

- Doğruluk: Verilerin gerçek dünyadaki durumu doğru şekilde temsil edip etmediğini değerlendirir. Örneğin, kişilere ait doğum tarihleri, vatandaşlık numaraları gibi verilerin bilgi sistemlerine doğru olarak kayıt edilip edilmediğidir.
- Tamlık: Verilerin gerçek dünyadaki durumu ne ölçüde temsil değerlendirir. Örneğin, ihtiyaç duyulan tüm verilere sahip olunup olmadığını, çalışanlara ait gerekli tüm bilgilerin kayıt edilip edilmediğidir.
- Tutarlılık: İki veya daha fazla veri sorgusunun gerçek dünyadaki bir durum için aynı cevapları vermesi gerekliliğidir. Her bir veri nesnesinin tek bir yerde kayıt edilmesiyle kesin bir tutarlılık sağlanabilir.
- Geçerlilik: Verilerin belirlenen kısıtlama veya doğrulama kurallarına uyup uymamasıdır. Verinin nesnesinin 32 Ocak 2023 gibi geçersiz bir tarihi temsil etmesine neden olabilecek bir kısıtlama veya doğrulama kuralının bulunmaması bu duruma bir örnektir.
- Güncellik: Verilerin güncel olma ve gereksinim duyulduğunda kişi veya sistemler tarafından kullanılabilir olması durumudur. Çalışma şartlarındaki tüm değişikliklerin kayıt altına alınması bu duruma bir örnektir.

İş süreçlerinin uygun maliyetle ve zamanında desteklenmesi için veri ve bilgileri oluşturma, toplama, saklama, sürdürme, iletilme ve sunma yeteneği; veri ve bilgi kalitesini belirleyen karakteristiklerin anlaşılması ile veri ve bilgi kalitesinin ölçülmesine, yönetilmesine ve raporlanmasına yönelik bir kabiliyetin sağlanmasıyla meydana gelmektedir (ISO 8000-61, 2016). Veri kalitesinin iyileştirilmesine yönelik, the International Organization for Standardization (ISO) tarafından geliştirilen "Veri Kalitesi" standart grubunda (ISO 8000-8) veri kalitesine yönelik verilerin "biçim (söz dizimsel)", "anlam (semantik)" ve "yararlılık (pragmatik)" olmak üzere üç bakış açışı tanımlanmıştır (ISO 8000, 2022). Veri kalitesine ilişkin söz konusu bakış açısı Şekil 13'de gösterilmiştir.

Şekil 13. Veri Kalitesine Yönelik Üç Bakış Açısı (Gordon, 2022; ISO 8000-61, 2016)

Veri yönetimi sürecinin temel bir bileşeni olan veri kalitesi yönetimi, verilerin kullanılabilirliğinin temin edilmesi kapsamında verilerin kalitesini yönetmeye yönelik tüm süreçleri içermektedir (Strengholt, 2020). ISO 8000 standardının 61. kısmı olan "Veri Kalitesi Yönetimi: Süreç Referans Modeli (ISO 8000-61, 2016)"nde veri yönetimine ilişkin genel bir yaklaşım belirtilmiştir. Söz konusu yaklaşım "Veri Kalitesinin Planlanması", "Veri Kalitesinin Kontrolü", "Veri Kalitesinin Güvence Altına Alınması" ve "Veri Kalitesinin Geliştirilmesi" döngüsüne dayanmakta olup, bu süreç modeli Şekil 14'te gösterilmiştir.



Şekil 14. ISO 8000-61:2016 Veri Kalitesi Yönetimi: Süreç Referans Modeli (Gordon, 2022)

Modelin sol tarafında döngünün kapsamında olan süreçler, sağ tarafında bulunan iki alanda ise bu döngüye destek sağlayan hususlar belirtilmektedir. Model döngüsünde bulunan süreçler şu hususları ifade etmektedir (Gordon, 2022):

- Veri kalitesinin planlanması: Bu süreç, bir kuruluşta arzu edilen veri kalitesi yönetiminin oluşturulması için genel ihtiyaç, amaç ve planın geliştirilmesi ve bunların kuruluş tarafından kabul edilmesini kapsamaktadır.
- Veri kalitesinin kontrolü: Bu süreç, kuruluşa ait verilerin belirlenen tüm ihtiyaçları karşılaması için, verilerin oluşturulması, güncellenmesi ve kontrol edilmesine ilişkin gerekli olan faaliyetleri kapsamaktadır.
- Veri kalitesinin güvence altına alınması: Bu süreç, var olan kontrol uygulamalarının kuruluşa ait verilerin kalitesi üzerindeki etkisinin tespit edilmesine yönelik gerekli faaliyetleri kapsamaktadır.
- Veri kalitesinin iyileştirilmesi: Bu süreç, veri katilesinin sürdürülebilir iyileştirilmelerinin sağlanmasına ilişkin yapılması gerekli olan faaliyetleri kapsamaktadır. Veri kalitesini düşüren temel nedenlerin yok edilmesi veya azatılması ile veri ve süreç uyumsuzluklarının engellenmesine yönelik çözümlerin uygulanması bu sürecin kilit noktasıdır.

3.4.11. Veri Yönetimi Olgunluk Modelleri

Olgunluk, bir disiplin çerçevesinde bir kuruluşun yeteneklerini değerlendirilmesidir (Belghith ve diğerleri, 2021, s. 299; Gökalp ve Demirörs, 2016). Olgunluk, bir kurum ve kuruluşun belirli süreçlerini gerçekleştirme yeteneğini belirlemek için kullanılabilecek kurumsal gelişim seviyesini yansıtmaktadır. Olgunluk modellerinin kökeni toplam kalite yönetimi alanındadır (Cooke, 2002). Olgunluk modelleri, birçok iş alanında sürekli iyileştirme yaklaşımı sağlamaktadır. Bu kapsamda, sürekli iyileştirmeyi stratejik olarak yönlendirmekle birlikte, bir kuruluşun hali hazırdaki durumunun ve gelecekteki hedef konumunun ayrıntılı bir şekilde anlaşılmasını gerektirmektedir (Brookes ve Clark, 2009).

Olgunluk modelleri, her bir olgunluk düzeyine ilişkin bir genel bakış sağlamaktadır. Bu bağlamda, olgunluk modelleri, sürdürülebilir iyileştirmeyi amaçlayan, yetenek seviyeleri ile yapısal ve aşamalı bir yaklaşımla birlikte kuruluşa bir yol haritayı sunmaktadır (Röglinger, Pöppelbuß ve Becker, 2012). Olgunluk modelleri, kurumsal bir hedefe

ulaşmaya yönelik kurumsal yetenekleri sistematik olarak değerlendirmek ve geliştirmek için kanıtlanmış bir yaklaşımdır. Kurum ve kuruluşlarda veri yönetimi bağlamında, bir olgunluk modeli, mevcut iyileştirme seçenekleri arasında gezinmelerine ve bunların kuruluşun hedefleriyle alaka düzeyini değerlendirmelerine yardımcı olabilmektedir (Defize, 2020).

Veri yönetimi olgunluğu açısından hangi durumda olduklarının farkında olmayan kuruluşlar büyük miktardaki veri akışını yönetmek için gerekli olan uygun yetenekleri belirmek ve uygulamak için mücadele etmektedir (Belghith ve diğerleri, 2021, s. 298). Bu sebeple, veri yönetimlerini devamlı olarak iyileştirmek için, kuruluşlar tarafından mevcut yeteneklerinin değerlendirilmesi gerekmektedir. Olgunluk modelleri, belirli bir iş süreci alanında bir kurum ve kuruluşun mevcut yetenekleri ölçmek için etkili araçlardır. Olgunluk modelleri, bir kurum ve kuruluşun yeteneklerini, güçlü ve zayıf yönlerini değerlendirmek, kurumsal süreçleri karşılaştırmak ve olgunluk ile iş performansı arasındaki bağlantıları bulmak için bir çerçeve çizmektedir (Proença ve Borbinha, 2018).

Veri temelli olarak faaliyet gösteren çoğu kurum ve kuruluşun dijital dönüşümü kapsamında, veri yönetiminin olgunluk seviyesinin değerlendirmesi için doğru araçları kullanmaları önemli bir adımdır. Bu kapsamda, olgunluk modelleri, kurum ve kuruluşlar tarafından gözlemlenen ortamın tanım, yönetilebilirlik, verimlilik ve ölçüm düzeylerini tanımlayan araçlar olarak hizmet etmektedirler (Luftman ve diğerleri, 2015).

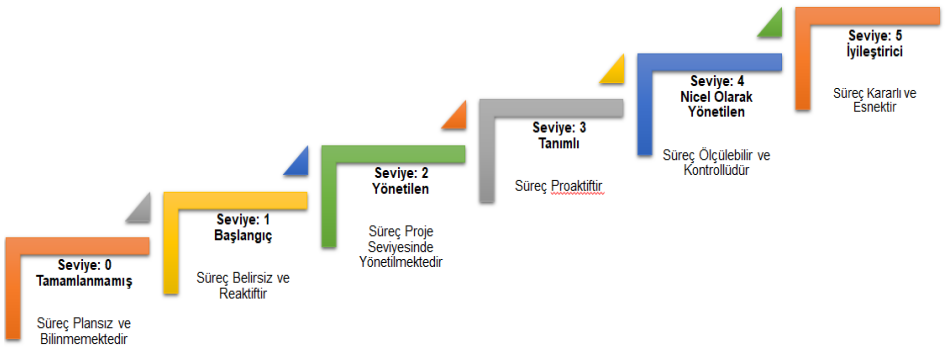
DAMA International tarafından yayınlanan Veri Yönetimi Bilgi Birimi (Data Management Body of Knowledge (DAMA-DMBoK)), Capability Maturity Model Integration (CMMI) tarafından oluşturulan Veri Yönetim Olgunluk Modeli (Data Management Maturity Model (DMM)) ve Enterprise Data Management Council (EDM Council) tarafından geliştirilen Veri Yönetimi Yetenek Değerlendirme Modelinin (Data Management Capability Assessment Model (DCAM)) veri yönetimi boyutları Tablo 5'te gösterilmiştir. CMM-DMM ve DAMA-DMBoK gibi çoğu model, olgunluk düzeyini toplu olarak değerlendirmek için temsili bir katılımcıyla bir uygulama yapılmasını önermektedir. Ancak yöntem, olgunluk tanımı dışında bir değerlendirme kriteri sağlamamaktadır (Defize, 2020, s. 15).

Tablo 5. Veri Yönetimi Modellerinin Boyutları (CMMI, 2023a; DAMA, 2017; EDM Council, 2023)

DMBoK	DMM	DCAM
1. Veri Yönetişimi	1. Veri Stratejisi	1. Veri Stratejisi ve İş Oluru
2. Veri Mimarisi	2. Veri Kalitesi	2. Veri Yönetimi, Programı ve Bütçesi
3. Veri Modelleme ve Tasarımı	3. Platform ve Mimari	3. Kuruluş ve Veri Mimarisi
4. Veri Depolama ve İşlemler	4. Veri Yönetişimi	4. Veri ve Teknoloji Mimarisi
5. Veri Güvenliği	5. Veri İşlemleri	5. Veri Kalite Yönetimi
6. Veri Entegrasyonu ve Birlikte Çalışabilirlik	6. Destekleyici Süreçler	6. Veri Yönetişimi
7. Doküman ve İçerik Yönetimi		7. Veri Kontrol Çevresi
8. Referans ve Ana Veriler		8. Analitik Yönetimi
9. Veri Ambarı ve İş Zekası		
10. Üst Veriler		
11. Veri Kalitesi		

3.4.11.1. Olgunluk Seviyeleri

Defize (2020) tarafından yapılan çalışmada, olgunluk modellerinin çoğunun beş seviyesinin olduğu ve bu seviyelerin CMMI tarafından oluşturulan süreç iyileştirme modeline karşılık geldiği tespit edilmiştir. CMMI olgunluk seviyeleri Şekil 15'de gösterilmiştir. Olgunluk seviyeleri, önceden tanımlanmış uygulama alanları setleri temelinde bir kuruluşun performans ve süreç iyileştirmesine yönelik aşamalı bir yol temsil etmektedir. Her olgunluk seviyesinde, önceden belirlenmiş süreç alanı seti aynı zamanda performans iyileştirmesi için bir yol sağlamaktadır. Her olgunluk seviyesi, yeni işlevsellik veya sıkılık ekleyerek önceki olgunluk seviyelerine dayanmaktadır (CMMI, 2023b).



Şekil 15. CMMI Olgunluk Seviyeleri (CMMI, 2023b)

CMMI olgunluk seviyelerinin başlangıç aşamasında iş tamamlanmakta olup, genellikle işler bütçeyi aşmakta ve bunun sonucu olarak söz konusu işler ertelenmektedir. İkinci seviyede, projeler planlanmakta, gerçekleştirilmekte, ölçülmekte ve kontrol edilmektedir. Üçünce seviyede, kuruluş çapındaki standartlar proje, program ve portföylere rehberlik sağlamaktadır. Dördüncü seviyede, kuruluş, hem iç hem de dış paydaşların ihtiyaçlarını karşılamak için öngörülebilir ve nicel performans geliştirme hedefleriyle yönlendirilen veri odaklı bir yapıya sahiptir. Son seviyede ise, kuruluş sürekli gelişim odaklı olmakla birlikte, fırsatlara ve değişime hızlı bir şekilde cevap verebilmek için esnek bir yapıya sahiptir. Kuruluşun istikrarı, çeviklik ve yenilik için bir platform sağlamaktadır (CMMI, 2023b; Defize, 2020, s. 14).

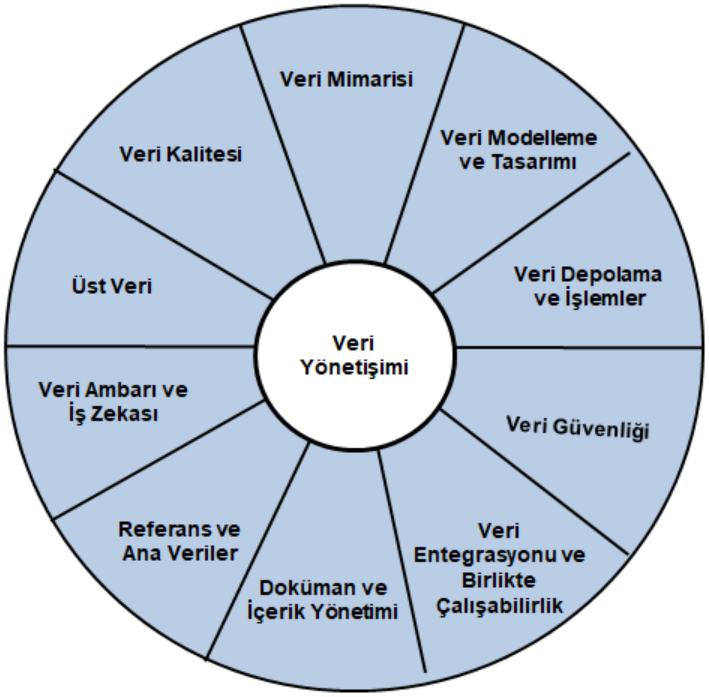
Çalışma kapsamında incelenen Veri Yönetimi Bilgi Birimi (DAMA-DMBoK) ve CMMI Veri Yönetim Olgunluk Modeli (DMM) yukarıda belirtildiği gibi beş seviyeli olmakla birlikte, Veri Yönetimi Yetenek Değerlendirme Modeli (DCAM) birinci olgunluk seviyesinin altına eklenen ve "başlatılmamış" olarak tanımlanan altıncı seviyeye sahip tek modeldir.

3.4.11.2. Veri Yönetimi Bilgi Birikimi (DAMA-DMBoK)

DAMA International tarafından veri yönetimi kapsamında yayınlanan DMBoK'ta (Data Management Body of Knowledge) on bir bilgi alanı tanımlanmıştır. Bu bilgi alanları şu şekildedir (DAMA International, 2017):

- Veri Yönetişimi,
- Veri Mimarisi,
- Veri Modelleme ve Tasarımı,
- Veri Depolama ve İşlemler,
- Veri Güvenliği,
- Veri Entegrasyonu ve Birlikte Çalışabilirlik,
- Doküman ve İçerik Yönetimi,
- Referans ve Ana Veriler,
- Veri Ambarı ve İş Zekası,
- Üst Veriler,
- Veri Kalitesi.

DMBoK'un en son sürümü veri etiği, büyük veri, veri entegrasyonu, birlikte çalışabilirlik ve veri yönetimi olgunluk değerlendirmesi için ayrılmış bölümlerini içermektedir. DAMA International tarafından, veri yönetimin farklı konularının birbirleriyle ilişkisinin gösterilmesi oluşturulan Veri Yönetimi Çerçevesi (DAMA Çarkı) Şekil 16'da sunulmuştur. Veri yönetimi çerçevesinde, her veri yönetim faaliyeti temelinin nasıl oluştuğunu vurgulamak için veri yönetişimi boyutu çarkın merkezinde konumlandırılmıştır (Dataversity, 2023).



.

Şekil 16. DAMA-DMBok Veri Yönetimi Çerçevesi (DAMA International, 2023)

Kurum ve kuruluşların veri yönetimi uygulamalarına ilişkin işletme stratejisi ve iş süreci ihtiyaçları kapsamında, DMBok'ta tanımlanan on iki veri yönetim prensibi şöyledir (de Figueiredo ve diğerleri 2019, s.17):

- Etkili veri yönetimi, liderlik yönetimi gerektirir.
- Veri, eşsiz özelliklidir.
- Verilerin kıymeti iktisadi olarak belirtilmelidir.
- Veri yönetimi, veri kalitesini süreçlerini uygulamaktadır.
- Verilerin yönetilmesi maksadıyla üst veriler gereklidir.
- Verileri yönetmek için planlama gereklidir.

- Veri yönetimi gereksinimleri bilgi teknolojisi kararlarını yönlendirmelidir.
- Veri yönetimi görevler/işlevler arasıdır.
- Veri yönetimi işletme düzeyinde bir perspektif gerektirir.
- Veri yönetimi bir dizi perspektifi dikkate almak zorundadır.
- Farklı veri türlerinin farklı yaşam döngüsü özellikleri vardır.
- Veri yönetimi, verilerle ilişkili risklerin yönetilmesini içermektedir.

3.4.11.3. CMMI Veri Yönetim Olgunluk Modeli (DMM)

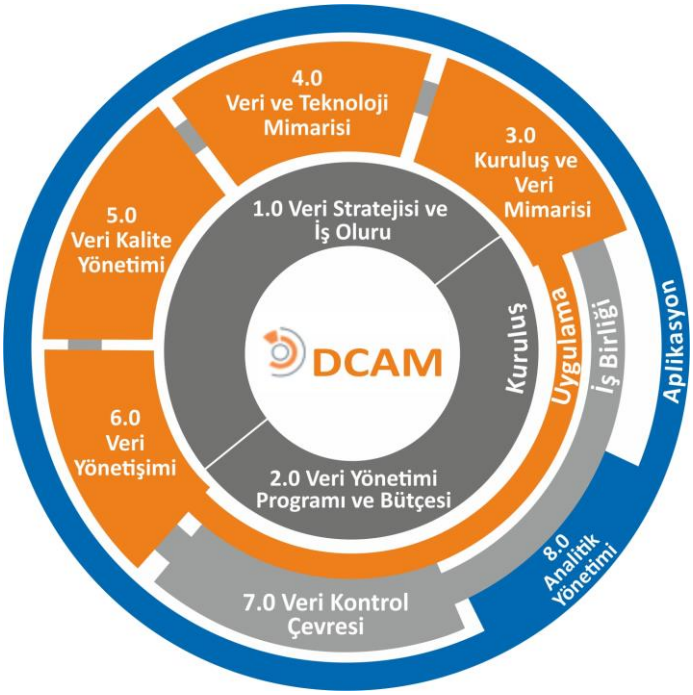
CMMI tarafından, kuruluşların veri yönetimi süreçlerini oluşturmasına, ölçmesine ve iyileştirilmeler yapmasına yardımcı olması kapsamında oluşturulan Veri Yönetim Olgunluk Modelinde (DMM) 6 temel kategoride kapsamlı bir veri yönetimi uygulama çerçevesi tanımlanmıştır (CMMI, 2023). Bu veri yönetimi çerçevesinin 6 temel kategori ve 25 süreç alanı Tablo 6'da gösterilmiştir. DMM, kuruluşların mevcut durumlarını değerlendirmesi ve veri yönetimi yeteneklerini geliştirmesine ilişkin özelleştirilmiş yol haritaları oluşturmak için kullanılmaktadır (Belghith ve diğerleri, 2021, s. 303).

Tablo 6. CMMI DMM Kategorileri ve Süreç Alanları (CMMI, 2023)

DMM Kategorileri	Süreç Kodu	Süreç Alanları
Veri Stratejisi	1.1.	Veri Yönetimi Stratejisi
	1.2.	İletişimler
	1.3.	Veri Yönetimi İşlevi
	1.4.	Olabilme Durumu
	1.5.	Finansman
Veri Yönetişimi	2.1.	Yönetişim Yönetimi
	2.2.	İş Sözlüğü
	2.3.	Üst Veri Yönetimi
Veri Kalitesi	3.1.	Veri Kalitesi Stratejisi
	3.2.	Veri Profili Oluşturma
	3.3.	Veri Kalitesi Değerlendirmesi
	3.4.	Veri Temizleme
Veri İşleme	4.1.	Veri Gereksinimlerinin Tanımı
	4.2.	Veri Yaşam Döngüsü Yönetimi
	4.3	Sağlayıcı Yönetimi
Platform ve Mimari	5.1.	Mimari Yaklaşımı
	5.2.	Mimari Standartları
	5.3.	Veri Yönetim Platformu
	5.4.	Veri Entegrasyonu
	5.5.	Tarihsel Veriler ve Arşivleme
Destekleyici Süreçler	6.1.	Ölçüm ve Analiz
	6.2.	Süreç Yönetimi
	6.3.	Süreç Kalite Güvencesi
	6.4.	Risk Yönetimi
	6.5.	Konfigürasyon Yönetimi

3.4.11.4. Veri Yönetimi Yetenek Değerlendirme Modeli (DCAM)

EDM Council (Enterprise Data Management Council) tarafından geliştirilen Veri Yönetimi Yetenek Değerlendirme Modeli (DCAM), veri yönetimi disiplininin oluşturulması, etkinleştirilmesi ve sürdürülmesi için gerekli olan yetenekleri kapsamaktadır. DCAM, bir kuruluşta veri yönetiminin başarı bir biçimde yönetilmesi için gerekli olan stratejileri, kuruluş yapılarını, teknolojiyi ve iş süreçleri için gerekli uygulamaları belirtmekle birlikte, verilerin dijital dönüşümü, yapay zeka ve makine öğrenimi gibi gelişmiş analitiğin ve veri etiğinin desteklemesini sağlamaktadır. DCAM veri yönetimini, 8 bileşen ve bu bileşenlerin 38 yetenek boyutuyla tanımlamıştır. Bu veri yönetim çerçevesinin bileşenleri Şekil 17'de, yetenek boyutları ise Tablo 7'de gösterilmiştir.



Şekil 17. EDM Council-DCAM Veri Yönetimi Bileşenleri (EDM Council, 2023)

DCAM, kuruluşların veri yönetimi kapsamında, ihtiyaç duydukları vizyonun oluşturulmasına, veri ekosistemini değerlendirmesine, iş gerekçelerinin geliştirilmesine, programların geliştirilmesi ve bütçesinin desteklenmesine ilişkin esnek bir yapı kazanmalarına, en iyi uygulamaların (diijital dönüşüm, yapay zeka ve makine öğrenimi gibi) desteklenmesine, düzenleyici ve uyumluluk gerekliliklerinin gerçekleştirilmesine yardımcı olmaktadır (EDM Council, 2023).

Tablo 7. EDM Council-DCAM Veri Yönetimi Çerçevesi (EDM Council, 2023)

DCAM Bileşenleri	Süreç Kodu	Yetenek Boyutları
Veri Stratejisi ve İş Oluru	1.1.	Veri Yönetimi Stratejisi (DMS) Belirlenmesi ve Paylaşılması
	1.2.	Veri Yönetimi İş Gerekçesinin Tanımlanması
	1.3.	Veri Yönetimi Vizyonunun Tanımlanması
Veri Yönetimi, Programı ve Bütçesi	2.1.	Veri Yönetimi Programının Oluşturulması
	2.2.	Kuruluş Tarafından Veri Yönetimi Finansman Modelinin Oluşturulması, Kabul Edilmesi ve Onaylanması.
	2.3.	Veri Yönetimi Organizasyon Yapısının Oluşturulması ve Uygulanması
	2.4.	Veri Yönetimi Programı Yol Haritalarının Geliştirilmesi, Kaynaştırılması ve Onaylanması
	2.5.	Veri Yönetimi Süreç Mükemmelliği Programının Kurulması
	2.6.	Paydaş Katılımının Oluşturulması ve Onaylanması
	2.7.	İletişim ve Eğitim Programlarının Tasarlanması ve İşletilmesi
	2.8.	Veri Yönetimi Programının Kuruluşun Hedeflerine Göre Ölçülmesi ve Değerlendirilmesi
Kuruluş ve Veri Mimarisi	3.1.	Veri Mimarisi İşlevinin Oluşturulması
	3.2.	İş Mimarisinin Veri Mimarisi ile Entegrasyonun Sağlanması
	3.3.	Verilerin Belirlenmesi
	3.4.	Verilerin Tanımlanması
Veri ve Teknoloji Mimarisi	4.1.	Veri Yönetimi Girişiminin Desteklenmesi İçin Teknoloji Mimarisinin Tanımlanması
	4.2.	Veri Yönetimi Teknolojisi Araçlarının Tanımlanması ve Yönetilmesi
	4.3.	İş Süreci Risk Planlamasının Yapılması
Veri Kalite Yönetimi	5.1.	Veri Kalitesi Yönetiminin Oluşturulması
	5.2.	Veri Profilinin Oluşturulması ve Ölçülmesi
	5.3.	Veri Kalitesi Sorunlarının Giderilmesi
	5.4.	Veri Kalitesinin Gözlemlenmesi ve Sürdürülmesi
Veri Yönetişimi	6.1.	Veri Yönetişimi İşlevinin Oluşturulması
	6.2.	Politika ve Standartların Yazılması ve Onaylanması
	6.3.	Veri Yönetimi Programının Yönetimi
	6.4.	Veri Yapısının Yönetimi
	6.5.	Verilerin Amaca Uygunluğun Yönetimi
	6.6.	Veri Etiğinin Yönetimi
Veri Kontrol Çevresi	7.1.	Veri Kontrol Ortamının Belirtilmesi
	7.2.	Kuruluşlar Arası Kontrol İşlevi İşbirliği
	7.3.	Veri Riskinin Yönetilmesi
Analitik Yönetimi	8.1.	Analitik İşlevinin Oluşturulması
	8.2.	Analitiğin, İş ve Veri Yönetimi Stratejisi ile Uyumlu Olması
	8.3.	Analitiğin, Veri Mimariyle Uyumlu Olması
	8.4.	Analitiğin, Veri Kalitesiyle Uyumlu Olması
	8.5.	Analitik Platformunun Tasarlanması ve Kullanılabilir Olması
	8.6.	Model İşletimin Oluşturulması
	8.7.	Analitik Kültürü ve Eğitim İhtiyaçlarının Yönetimi

4. BÖLÜM

VERİ, BİLGİ VE BELGE YÖNETİMİNE İLİŞKİN STANDARTLAR, REHBERLER, UYGULAMALAR, YASAL VE İDARİ DÜZENLEMELER

4.1. VERİ YÖNETİMİ STANDARTLARI

Uluslararası standartlar, birçok ülkeden uzmanların ortak anlayışlarıyla geliştirilmektedir. Söz konusu standartlar, kuruluşların ürün veya hizmetlerinde uyması gereken kural, yönerge ve süreçleri belirtmektedir. Veri yönetimi kapsamında Uluslararası Standardizasyon Kuruluşu (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) ile işbirliğiyle yayınlanan standartlar aşağıda açıklanmıştır.

4.1.1. ISO 8000 Veri Kalitesi ve Kurumsal Ana Veri Standardı

ISO 8000 veri yönetiminin temel bir yol belirleyicisi olan çok parçalı uluslararası bir standarttır. ISO 8000 standardının amacı, belirli veri türleri için veri kalitesini iyileştirmeye yönelik çerçeveler sağlamakla birlikte, verilerin hangi özelliklerinin veri kalitesiyle ilgili olduğunu tanımlamakta, bu özellikler için geçerli gereksinimleri belirlemekte ve veri kalitesini iyileştirmek için yönergeler sağlamaktadır. Verilerle temsil edilen unsurların kalitesi hariç olmak üzere aşağıda belirtilen hususlar ISO 8000 standardının kapsamındadır (ISO 8000-1, 2022).

- Veri yönetişimi,
- Veri kalitesinin genel yönleri,
- Veri kalitesi yönetimi,
- Veri kalitesi değerlendirmesi,
- Ana verilerin kalitesi.

ISO 8000 standardı, paydaşlar arasındaki ana verilerin paylaşımına ilişkin özellikleri açıklamakta ve gereklilikleri tanımlamaktadır. İş süreçlerini zamanında ve uygun maliyetli bir şekilde desteklemek üzere verilerin oluşturulması, toplanması,

depolanması, bakımı, aktarılması, işlenmesi ve sunulması için hem verilerin kalitesini belirleyen özelliklerinin anlaşılması hem de veri kalitesinin ölçülmesi, yönetilmesi ve raporlanması gerekmektedir. Bu bağlamda, ISO 8000 standardı belirli veri türleri için veri kalitesinin iyileştirilmesine yönelik çerçeveler sağlamaktadır. Söz konusu çerçeveler hem tek başına hem de kalite yönetim sistemleri ile birlikte kullanılabilmektedir (Pande, 2020).

4.1.2. ISO/IEC TR 10032:2003 Bilgi Teknolojileri - Veri Yönetimi Referans Modeli Standardı

Bu teknik rapor, veri yönetimine ilişkin ISO Referans Modelini tanımlamaktadır. Rapor, bilgi sistemlerindeki kalıcı verilerin yönetimine ilişkin mevcut ve gelecekteki standartların geliştirilmesini koordine etmek için bir çerçeve oluşturmaktadır. Bu tür sistemlerde tutulan tüm verilerle ilgili ortak terminoloji ve kavramları tanımlamakta olup, bu kavramlar, veri tabanı yönetim sistemleri ya da veri sözlüğü sistemleri gibi belirli veri yönetimi bileşenleri tarafından sağlanan hizmetleri daha özelde tanımlamak için kullanılmaktadır. Bu bağlamda bu teknik raporda, veri yönetiminin teknik yönlerine odaklanmaktadır (ISO/IEC TR 10032, 2003).

4.1.3. ISO/IEC 11179 Bilgi Teknolojileri - Üst Veri Kayıt Kütükleri (MDR) Standardı

Çok parçalı olan bu standart, veri elemanlarının ve anlamlarının kaydına odaklanmaktadır. Bu standart serisi, verinin anlamını, verinin temsilini ve bunlara ait tanımlarının kaydını ele almaktadır. Bu açıklamalar aracılığıyla, verinin anlamının doğru bir şekilde anlaşılması ve verinin yararlı bir şekilde tasvir edilmesi sağlanmaktadır. Bu standart, veri sözlüklerinin, üst verilerin ve diğer veri tanımlama bileşenlerinin kullanımını standartlaştırmaktadır. Bu sayede, farklı veri kaynaklarının birbiriyle uyumlu bir şekilde çalışabilmesi ve anlaşılabilir olması sağlanmaktadır. Söz konusu standardın amaçları şunlardır (ISO/IEC 11179-1, 2023):

- Verilerin standart olarak tanımlanması,
- Verilerin kurumsal elemanlar arasında ve kurumlar arasında ortak bir anlayışının oluşması,

- Verilerin zaman, mekan ve uygulamalar arasında yeniden kullanımının ve standartlaştırılmasının sağlanması,
- Verilerin kurum içinde ve kurumlar arasında uyumlu ve standart hale getirilmesi,
- Veri tanımları bileşenlerinin yönetilmesi,
- Veri tanımları bileşenlerinin yeniden kullanılması.

4.1.4. ISO/IEC 19583 Bilgi Teknolojileri - Üst Verinin Konseptleri ve Kullanımı Standardı

Bu standart, üst verilerle ilgili bilgilerin kaydedilmesine yönelik yapıyı tanımlamayan ISO/IEC 11179 ve ISO/IEC 19763 standart serilerini destekleyen bir dizi teknik rapordur. Bu teknik raporun diğer kısımları üst veri ya da üst veri kayıtlarının kullanımına ilişkin örnek sunmakta olup, söz konusu kısımlar şunlardır (ISO/IEC 19583-1:2019; ISO/IEC 19583-21:2022; ISO/IEC 19583-22:2018; ISO/IEC 19583-23:2020):

- **ISO/IEC 19583-1:2019 Bilgi Teknolojileri - Üst Verinin Konseptleri ve Kullanımı-Üst Verinin Konseptleri:** Özellikle bilgi teknolojilerindeki veri yönetimi uzmanlığı kapsamındaki üst verilerin kullanımına ilişkin üst veri kavramını açıklamaktadır. Bu teknik rapor, temel üst veri konseptini ve üst verinin, veri ve metamodelleriyle olan ilişkisini açıklamaktadır.
- **ISO/IEC 19583-21:2022 Bilgi Teknolojileri - Üst Verinin Konseptleri ve Kullanımı-SQL'daki Veri Modeli:** Üst verilerle ilgili bilgilerin kaydedilebileceği ve muhafaza edilebileceği bir kayıt defterine ilişkin bir spesifikasyon sağlayan ISO/IEC 11179-3'de belirtilen kayıtların uygulayıcıları ve kullanıcılarının kavramsal modelleri gerçek örneklere dönüştürmek için fazla talimata ihtiyacı vardır. Bu teknik rapor, SQL veri tabanı dili kullanılarak ISO/IEC 11179-3'te açıklanan metamodelin örnek bir SQL örneklemesini sağlamaktadır.
- **ISO/IEC 19583-22:2018 Bilgi Teknolojileri - Üst Verinin Konseptleri ve Kullanımı-ISO/IEC 19763 Kullanarak Geliştirme Süreçlerini Kaydetme ve Eşleme:** Bu teknik rapor, ISO/IEC 11179-3, ISO/IEC 19763-5 ve ISO/IEC 19763-10'da belirtilen yetenekleri kullanarak süreç modelleri arasındaki eşlemenin kaydını gösteren bir kullanım senaryosu içermektedir. Bu bağlamda, kayıtlı süreç modeli eşlemelerinin kullanılabilirliği, süreç modellerinin yeniden kullanımını teşvik etmeye yardımcı olmaktadır.

- **ISO/IEC 19583-23:2020 Bilgi Teknolojileri - Üst Verinin Konseptleri ve Kullanımı- ISO/IEC 11179-3'ün Bir Alt Kümesi İçin Veri Öğesi Değişimi (Data Element Exchange-DEX):** Bu teknik rapor, veri öğesi tanımlarının bir ISO/IEC 11179-3 üst veri kaydı ile iletişimine yönelik mesaj değişim çerçevesini belirtmektedir.

4.1.5. ISO/IEC 19773:2011 Bilgi Teknolojileri - Üst Veri Kayıtları Modülleri Standardı

Bu standart, üst veri kayıtlarında varlık-kişi-grup verileri, posta verileri ve telefon numarası veri kaydına ilişkin küçük modülleri tanımlamaktadır. Bu standardın içeriği bir üst veri kaydı oluşturma planları olmamasına karşın, uluslararası adresleri ya da telefon numaralarını işleme yöntemlerini standartlaştırmakla ilgilenen herkese yardımcı olmaktadır.

4.1.6. ISO/IEC 19763 Bilgi Teknolojileri: Birlikte Çalışabilirlik İçin Üst Model Çerçevesi

Çok parçalı olan bu standart, birlikte çalışabilirliğe yardımcı olmak için modellerin kaydına ve modeller arasındaki eşlemelere odaklanmaktadır. Bu standart, ISO/IEC 11179'da belirtilen ortak olanaklara dayanmaktadır. ISO/IEC 19763 şu bölümlerden oluşmaktadır (ISO/IEC 11179-1, 2015):

1. Bölüm: Çerçeve
3. Bölüm: Ontoloji kaydı için metamodel
5. Bölüm: Süreç modeli kaydı için metamodel
6. Bölüm: Kayıt özeti
7. Bölüm: Hizmet kaydı için metamodel
8. Bölüm: Rol ve hedef kaydı için metamodel
9. Bölüm: Talep üzerine model seçimi (Teknik rapor)
10. Bölüm: Çekirdek model ve temel eşleme
12. Bölüm: Bilgi modeli kaydı için metamodel
13. Bölüm: Form tasarımı kaydı için metamodel
16. Bölüm: Belge modeli kaydı için metamodel

4.1.7. ISO 55001:2014 Varlık Yönetimi: Yönetim Sistemleri-Şartlar

Bu standart, herhangi bir kuruluş kapsamında bir varlık yönetim sistemini kurma, uygulama, sürdürme ve geliştirme gereksinimlerini belirtmektedir. Bu standart, her tür ve büyüklükteki kuruluşa ve her tür varlığa (veri ve bilgi dahil) uygulanabilmektedir. Bu standart, öncelikle şu kişilerce kullanılmak üzere tasarlanmıştır (ISO 55001, 2014):

- Bir varlık yönetim sistemi kurma, uygulama, sürdürme ve geliştirme süreçlerinde yer alanlar,
- Varlık yönetimi faaliyetlerini yürütenler ve hizmet sağlayıcıları,
- Yasal, düzenleyici ve sözleşmeye dayalı gereksinimleri ve kurumların gereksinimlerini karşılama becerisini gözden geçirmek için dahili ve harici taraflar.

4.2. BİLGİ VE BELGE YÖNETİMİ STANDARTLARI

4.2.1. Avustralya Ulusal Belge Yönetim Standardı (AS 4390)

Avusturalya Standartlar Komitesi tarafından oluşturulan Avustralya Ulusal Belge Yönetim Standardı (AS 4390) Şubat 1996'da yayımlanmıştır (Özdemirci, 2003, s.228). Dünya'da belge yönetimi alanında yayımlanan ilk ulusal standart olan AS 4390, ulusal sınırlarının ötesine geçerek uluslararası zeminde ilgi odağı olmuştur (Külcü, 2007, s.247). ISO 15489 standardı AS 4390 standardı esas alınarak geliştirilmiştir (Külcü 2007, s.248; MacKenzie, 1999, s.28). Avusturalya tarafından AS ISO 15489 standardının kabul edilmesiyle birlikte AS 4390 standardı Mart 2002'de geri çekilmiştir (Özdemirci, 2003, s.228).

AS 4390 standardı geliştirilmesine yönelik girişimler, hem fiziki hem de elektronik belgelerin üretimi ve kullanımına yönelik kodlama standartlarının oluşturulması maksadıyla başlatılmıştır. Bu standart, kurumsal belge yönetimine ilişkin uygulamaları bir bütün olarak ele almakta olup, belgelerin tasarımından nihai ayıklanmasına kadar süreçleri detaylı bir şekilde belirtmektedir. Genel olarak standardın amaçları şunlardır (Külcü 2007, s.248; MacKenzie, 1999, s.26):

- Belge hizmetlerinin gerçekleştirildiği kurumsal ortamın çözümlenmesi,

- Belge işlemlerini de kapsayan kurumsal iş sürecinin belirlenmesi,
- Elde edilecek belgelerin tespit edilmesi ve bu belgelerin muhafaza edilme süresinin belirlenmesidir.

4.2.2. ISO 15489-1:2016 Bilgi ve Dokümantasyon - Belge Yönetimi Standardı

Bu standart 2001 yılında belge yönetimi alanında ilk uluslararası standart olarak yayımlanmıştır. Daha sonra teknik olarak revize edilmiş ve 2016 yılında ikinci baskısı yayımlanmış olup, 2021 yılında gözden geçirilerek onaylanmıştır. Bu standart, "Kavramlar ve İlkeler" ve "Klavuzlar (Teknik Rapor)" olarak iki bölümden oluşmaktadır. Tüm belge türlerinin oluşturulması, tutulması ve yönetiminde geçerli olan ISO 15489-1:2016, belge yönetimi süreçlerine ilişkin uygulamaları kodlayan temel standarttır (ISO 30301, 2019).

Bu standart kapsamında belgelerin yönetimi, ISO 30300 serisi Uluslararası Standartlar tarafından tanımlanan Belge Yönetim Sistemi (Management System for Records-MSR) için temel bir unsurdur. Bir MSR belgelerin yönetimini, politika, hedefler ve kayıtlar için direktifler içeren bir çerçeve oluşturarak, kurumsal başarı ve hesap verebilirliğe bağlamaktadır. MRS'nin uygulaması, işletmesi ve iyileştirilmesi kapsamında ISO 15489'un birinci bölümünün, ISO 30300 Uluslararası Standart serisi ile beraber kullanması önerilmektedir (ISO 15489-1, 2016).

4.2.3. TS 13298:2015 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı

E-dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı'na (No: 2005/5) istinaden yürütülen çalışmalar sonucunda ISO 15489 standardı ekseninde geliştirilen Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli 2006 yılında yayınlanmıştır (Kandur, 2006). Sonrasında bu model temelinde geliştirilen TSE 13298 Bilgi ve Dokümantasyon-Elektronik Belge Yönetimi standardı geliştirilmiş ve 2007 tarihinde yayınlanmıştır (Civelek ve Turan, 2010, s. 13, Çakmak ve diğerleri, 2015, s.140). Bu standart son olarak 2015 yılında "TS 13298:2015 Elektronik Belge ve Arşiv Yönetim Sistemi" standardı olarak 23 Ekim 2015 tarihinde yayınmış olup, 18 Şubat 2016 tarihinde standart kapsamında güncellemeler yapılmıştır.

Elektronik belge ve arşiv yönetimi kapsamında kavramları, ilkeleri, yönergeleri ve teknolojileri içeren bu standart, “Sistem Kriterleri”, “Belge Kriterleri”, “Elektronik Arşivleme Sistemi Referans Modeli (ELAS/RM)” ve “Üst Veri Elemanları” olarak dört bölümden oluşmaktadır. Söz konusu bölümler, kendi içlerinde alt kısımlara ayrılmış ve bu kısımların altındaki gereksinimler ayrıntılı olarak açıklanmıştır. Bu standart, kurumlarda üretilen ya da üretilecek elektronik dokümanların belge özelliğinin korunabilmesine yönelik gereksinim duyulan ilkeler ile bu belgelerin arşivlenmesi ve yönetilmesine ilişkin düzenlemeleri kapsamaktadır.

4.2.4. ISO 23081 Bilgi ve Dokümantasyon - Belge Yönetimi Süreçleri – Belgeler için Üst Veri

ISO 23081 standardı, belge yönetimi kapsamında üst verilerinin oluşturulması, kullanılması ve yönetilmesine ilişkin bir çerçeve belirlemekte ve bunların uygulanması için ilkeleri açıklamaktadır. Bu standart “İlkeler”, “Kavramsal ve Uygulama Hususları” ve “Öz Değerlendirme Metotları” olarak üç kısımda geliştirilmiştir. Standardın birinci bölümü, ISO 15489 kapsamında üst verilerin anlaşılması, uygulanması ve kullanılmasına ilişkin kılavuz ilkeleri kapsamaktadır (ISO 23081-1, 2017). İkinci bölümünde, ISO 23081-1:2017’ de belirtilen ilkeler ve uygulamalara ilişkin üst veri unsurlarının tutarlı olarak tanımlanması için bir çerçeve oluşturulmaktadır (ISO 23081-2, 2021). Teknik bir rehber olan son bölüm ise belgelerin kayıt üst verileri hakkında bir öz değerlendirme yapılmasına ilişkin rehberlik sağlamaktadır (ISO/TR 23081-3, 2011).

4.2.5. DCMI (Dublin Core Metadata Initiative) Standardı

Bu standart, Ohio eyaletinin Dublin şehrinde 1995 yılında yapılan çalıştay sonucunda ortaya çıkmıştır (Guha, 2008: 2). DMCI üst verilerin tasarımı ve üst verilere ilişkin iyi uygulamaları destekleyen açık bir kuruluşun (Dublin Core, 2023b) himayesinde geliştirilen bu standart, elektronik bilgi kaynakların tanımlanması ve açıklanması için kullanılan bir üst veri standardıdır. Bu standardın amacı, kaynakların anlaşılabilir, erişilebilir ve aranabilir hale getirilmesini sağlamaktır. Çalışmada önceden belirtildiği gibi, bu standart, farklı etki alanlarındaki bilgi kaynaklarını (metin, resim, ses, video ve web sayfaları vb.) tanımlamak için oluşturulan ve esnek olarak kullanılabilen 15 unsurdan meydana gelmektedir.

4.2.6. ISO 30300:2020 Bilgi ve Dokümantasyon - Belge Yönetim Sistemi - Temel İlkeler ve Sözlükler

Bu standart belge yönetimi alanının temel kavramlarına ilişkin tanımları ve ilgili terimleri kapsamaktadır. Söz konusu tanım ve terimler, SO/TC 46/SC 11 standartlarında güncellenecek yeni tanım ve terimleri sınırlamamaktadır (ISO 30300, 2020).

4.2.7. ISO 30301:2019 Bilgi ve Dokümantasyon - Belgeler için Yönetim Sistemleri - Gereklilikler

Bu standart, bir kurumun misyon, hedef, strateji ve görevlerinin yapılmasına destek sağlamak için bir belge yönetim sisteminin sahip olması gereken gereksinimleri belirlemektedir. Standart ayrıca, bir belge politikası ve hedeflerinin uygulanması geliştirilmesini ele almakla birlikte, bu süreçlerin izlenmesi ve performansının ölçülmesine ilişkin bilgi vermektedir. Bu standart, belge yönetimi faaliyetlerini desteklemek için belge yönetimi sistemini kurmak, uygulamak, sürdürmek ve geliştirmek isteyen tüm kurumlar için geçerlidir (ISO 30301, 2019).

4.2.8. ISO 30302:2022 Bilgi ve Dokümantasyon - Belgeler için Yönetim Sistemleri - Uygulama Rehberleri

Bu standart, ISO 30301:2019 çerçevesinde bir belge yönetimi sisteminin uygulanabilmesine yönelik rehberlik sağlamakta olup, bir belge yönetim sisteminin tasarlanması, uygulanması ve izlenmesi sırasında yapılacak süreçleri açıklamaktadır. Tüm kurumlar tarafından uygulanabilir olan bu standart, belge yönetim sisteminin uygulanması ve faal halde tutulmasından sorumlu olan kişilerce kullanılması amaçlanmaktadır.

4.2.9. ISO 16175 Bilgi ve Dokümantasyon - Belgelerin Yönetilmesine Yönelik Yazılım için Süreçler ve İşlevsel Gereksinimler

ISO 16175 standardı ofis ortamlarında dijital bilgi oluşturulması ve yönetilmesi kapsamında kullanılan yazılım uygulamalarına ilişkin uluslararası kabul görmüş ilkeleri ve işlevsel gereksinimleri sağlamaktadır. Ayrıca, fiziki belgelerin dijitalleştirilmiş versiyonlarının yönetilmesi bunun bir parçasıdır. İki kısımdan oluşan bu standardın

birinci bölümünde dijital kayıtları yöneten uygulamalara ilişkin işlevsel gereksinimler ve ilgili kılavuzlar belirtilmekte, ikinci bölümünde ise, dijitalleştirilmiş belgeler de da dahil olmak üzere belgelerin yönetilmesine yönelik yazılımların seçilmesi, tasarlanması, uygulanması ve sürdürülmesine ilişkin rehberlik sağlamaktadır (ISO 16175-1, 2020; ISO/TS 16175-2, 2020).

4.2.10. DOD 5015.2 Elektronik Belge Yönetimi Yazılım Uygulamaları İçin Standart (the U.S. Department of Defense's Design Criteria Standard for Electronic Records Management Software Application)

Amerika Ulusal Arşivi'nin (National Archives and Records Administration-NARA) katkılarıyla geliştirilen bu standart 1997 yılında yayımlanmıştır (Külcü 2007, s.252). Bu standart, belge ve arşiv yönetimine yönelik NARA ve ABD Savunma Bakanlığı tarafından tanımlanan minimum gereksinimleri açıklamaktadır. Kurumsal amaçlarla geliştirilen bu standart, belge yönetim yazılımlarının sağlaması kapsamında kamu kurumları, özel kuruluşlar ve uluslararası örgütler tarafından etkin olarak kullanılmaktadır (Külcü, 2018, s.181; Spratt, 2004, s.6). Elektronik belge yönetimi yazılımının tasarımında ve bu kapsamda uyması gereken kıstasları belirlemesi sebebiyle önemli bir standart olan DOD 5015.2, yapılan güncellemelerin sonunda günümüzdeki 47 temel kriterli yapısına ulaşmıştır (Külcü, 2018, ss.180-181).

DOD 5015.2 standardının amaçları arasında; belgelerin görünürlüklerinin artırılması maksadıyla üst verinin geliştirilmesi ve kayıt edilmesi, belgelerin web hizmetleri vasıtasıyla erişilebilir olması maksadıyla ara yüzlerin standartlaştırılması, zengin üst verilerin kullanılabilirliğinin sağlanması ve bu üst verilerin kullanılmasıyla belgelerin anlaşılabilir olmasının sağlanması bulunmaktadır (DoD 5015.02-STD, 2007, ss.30-31).

4.2.11. Avustralya Bilgi Yönetimi Standardı

Avustralya Ulusal Arşivleri (National Archives of Avustralia-NAA) tarafından, Avustralya devlet kurumlarına ait kurumsal bilgilerin etkili bir şekilde oluşturulması ve yönetilmesi amacıyla 28 Nisan 2017 tarihinde Bilgi Yönetimi Standardı yayınlanmıştır (Carey, 2017). ISO 15489-1:2016 standardının temel ilke ve kavramlarıyla tutarlı olan bu standart, kurumların faaliyet ve iş süreçlerinde üretilen, sağlanan ve kullanılan dijital veya dijital olmayan formattaki bilgi ve belgeler için geçerlidir (NAA, 2023).

Standart sekiz temel ilkeden oluşmakla birlikte, her ilkenin kendi içinde alt eylemleri bulunmaktadır. Standart, kurumların söz konusu ilkeleri nasıl karşılaması gerektiğini ifade etmemektedir. Kurumların kendilerine özgü kültürleri, yapıları, faaliyet ve hizmet alanları olması sebebiyle, kurumlar tarafından standartta belirtilen sekiz ilke kendi özel koşullarına göre uygulanması gerekmektedir. Standart kapsamında sözü edilen iş bilgisi (business information) kurumlar için anlam ve değer ya da öneme sahip olan tüm bilgi ve belgeleri ifade etmektedir. Standardın temel ilkeler şunlardır (NAA, 2023):

- İş bilgilerinin sistematik olarak yönetilmesi: Yerine getirilen veya getirilecek işlerin ihtiyaçlarını, sonuçlarını ve yükümlülüklerinin desteklenmesi maksadıyla bilgilerin bir varlık olarak yönetilmesi için bilgi yönetişimi planlanmalı ve uygulanmalıdır.
- Gerekli iş bilgilerinin oluşturulması: İş gereksinimlerinin etkili bir şekilde desteklenmesi maksadıyla amaca uygun iş bilgileri oluşturulmalıdır.
- İş bilgilerinin yeterince açıklanması: İş bilgileri, ihtiyaç duyulduğunda bulunabilmesi, uygun şekilde erişilebilmesi ve anlaşılabilmesi için tanımlanmalıdır. Bu bağlamda üst veriler, bir bilgi varlığını tanımlayan bilgilerdir.
- İş bilgileri uygun şekilde saklanması ve korunması: İş bilgileri güvenli şekilde saklanmalı, iş ihtiyaçları ve toplumun erişimi kapsamında gerekli olduğu sürece kullanılabilir durumda tutulmalıdır.
- İş bilgilerinin ne kadar süreyle saklanması gerektiği bilinmesi: Belirlen bir işin ve kişilerin ihtiyaçlarının karşılanması maksadıyla iş bilgilerinin saklama süresi analiz edilmeli ve belgelendirilmelidir.
- İş bilgileri hesap verilebilir şekilde imha edilmesi ya da aktarılması: İş bilgileri gerekli olduğu süre saklanmalı ve bu süre erdiğinde hesap verilebilir şekilde imha edilmeli ya da aktarılmalıdır.
- İş bilgilerinin uygun şekilde yönetilebilecekleri sistemlere kaydedilmesi: Kurumlar için gerekli olan iş bilgileri, bütünlüğünün korunabileceği ve güvenilir şekilde kullanımını sağlayan sistemlerde yönetilmelidir.
- İş bilgilerinin kullanıma ve yeniden kullanıma açık olması: İş bilgileri, erişim yetkisi olan kişilerce zaman içerisinde etkin olarak erişebilecek şekilde oluşturulmalı ve yönetilmelidir.

4.2.12. TSE K 523:2016 Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri

Kişisel ve kurumsal veri, bilgi ve belgeler elektronik ortamın haricinde taşınabilir teknolojinin imkan sağladığı her ortamda yer almaktadır. Paylaşılma riskleri göz önüne alındığında, kişisel ve kurumsal veri, bilgi ve belgelerin bulunduğu varlıkların gizlilik derecelerine göre sınıflandırma gereksinimi ortaya çıkmıştır. Bu bağlamda oluşturulan TSE K 523 "Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri" 2016 yılında yayımlanmıştır. Bu kriter standardının amacı, kurumsal bilgi varlıklarının tespit edilmesi ve bunların belirlenen gizlilik dereceleriyle sınıflandırılarak bilgi gizliğinin tesis edilmesidir. Bu kriter standardında bilgi varlıkları altı başlık altında (fiziksel/elektronik bilgi varlıkları, yazılım bilgi varlıkları, insan, soyut değerler (itibar, imaj vb.), hizmetler ve projeler) toplanmış ve bu bilgi varlıkları "Çok Gizli", "Gizli", "Özel", "Hizmete Özel", "Ticari Gizli", "Ticari Özel", "Kişiye Gizli", "Kişiye Özel" ve "Tasnif Dışı" olmak üzere sekiz gizlilik derecesine göre sınıflandırılmıştır (TSE K 523, 2016).

4.2.13. ISO/IEC 27001:2022 Bilgi Güvenliği, Siber Güvenlik ve Kişisel Gizliliğin Korunması - Bilgi Güvenliği Yönetim Sistemleri – Gereklilikler

Kurumsal bilgi güvenlik sistemleri kapsamında genellikle referans olarak kabul edilen bu standart, BGYS'nin oluşturulması, yürütülmesi, bakımı ve devamlı iyileştirilmesine yönelik gereksinimleri belirtmektedir. Bu standart ayrıca, bir kurum ve kuruluşun bilgi güvenliğine ilişkin risk analizlerinin yapılmasını, sonrasında önleyici ve düzenleyici süreçlerin gerçekleştirmesine yönelik gereksinimleri içermektedir. Bu standart, BGYS'nin kurumsal ihtiyaçları karşılama yeteneğinin değerlendirilmesi maksadıyla kullanılabilmektedir.

ISO ISO/IEC 27001 standardına göre, kuruluşun faaliyetleri ve genel yönetim yapısının BGYS ile entegre edilmesini gerekmekte olup, bilgi sistemleri ve kontroller tasarlanırken bilgi güvenliği göz önünde bulundurulmalıdır. Ayrıca standartta, BGYS'nin uygulanmasının kurumun gereksinimlerine göre ölçeklendirilmesi öngörülmektedir (ISO 27001, 2022). Bu standartta belirtilen gereklilere ilişkin oluşturulan denetimler ISO 27002:2022 standardında detaylı bir şekilde ifade edilmektedir.

TSK 13298:2015 standardında bilgi sistemlerinin güvenliğine yönelik TS ISO/IEC 27001 standardı ve bu standartla ilişkili standartlara uyumlu güvenlik önlemlerinin alınması önerilmekle birlikte, kurum ve kuruluşların BGYS ile ilgili olarak bu standardı kullanabileceği ifade edilmektedir.

KamuNet ağına dahil olmak isteyen kamu kurum ve kuruluşları tarafından, yerine getirilmesi gereken asgari gereksinimler belirlenmiştir. Söz konusu gereksinimler arasında ilgili kamu kurum ve kuruluşların KamuNet ile ilişkilendirilecek birim ve sistemlerini kapsayan bir BGYS'ni kurması ve işletmesi gerektiği ifade edilmektedir. Ayrıca, kamu kurum ve kuruluşlarının, sahip oldukları BGYS'ne yönelik TS ISO/IEC 27001 ya da ISO/IEC 27001 standardına ilişkin belgeleri ilgili kuruluşlardan (akredite edilmiş belgelendirme kuruluşları) temin etmeleri ve güncelliğini sağlaması gerektiği belirtilmektedir (Ulaştırma, Denizcilik…, 2017, mad. 4).

4.2.14. ISO/IEC 27002:2022 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması - Bilgi Güvenliği Kontrolleri

BGYS'nin gerekliliklere yönelik oluşturulan denetimlerin belirlendiği ISO ISO/IEC 27002 standardının üçüncü baskısı 2022 yılında yayımlanmıştır. Tüm kurum ve kuruluşlar tarafından uygulanabilir olan bu standart, ISO/IEC 27001'e yönelik oluşturulan BGYS kapsamında bilgi güvenliği risk değerlendirilmesinin belirlenmesi ve uygulanması için referans kaynaktır. Bu standart ISO/IEC 27001 standardı bağlamının yanı sıra, kurumların bilgi güvenliği yönetimlerine ilişkin kendilerine özgü yönergelerin geliştirilmesi ve uluslararası olarak kabul edilen en iyi uygulamalara yönelik bilgi güvenliği kontrollerinin uygulanması maksadıyla tasarlanmıştır. Bu standart dört ana kontrol başlığında yapılandırılmıştır. Bu kontrol başlıkları kendilerine özgü kontrol maddelerine sahiptir. Her bir kontrol maddesinde, söz konusu kontrole ilişkin uygulama amacı belirtilmekte, kontrollerin nasıl uygulanacağın yönelik rehberlik sağlanmakta ve kontroller kapsamında ilave bilgiler ile diğer standartlara yapılan atıflar yer almaktadır. Söz konusu kontrol başlıkları şu şekildedir (ISO/IEC 27002, 2022):

- Kurumsal Kontroller (37 adet kontrol maddesini içermektedir),
- İnsan Kontrolleri (8 adet kontrol maddesini içermektedir),
- Fiziksel Kontroller (14 adet kontrol maddesini içermektedir),
- Teknolojik Kontroller (34 adet kontrol maddesini içermektedir).

4.2.15. ISO/IEC 27014:2020 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması Bilgi Güvenliği Yönetimi

Bilgi güvenliği yönetimi, bilgi güvenliğinin etkili bir şekilde uygulanmasını sağlamak için kaynakların kullanılması olup, bilgi güvenliğine ilişkin direktiflere uyulacağını ve kurum yönetiminin bilgi güvenliği ile ilgili hususlarda güvenilir raporlar alacağını güvence altına almaktadır. Bu standart kurumlara, kendilerinin bilgi güvenliği ile alakalı süreçleri izleyebileceği, değerlendirebileceği, yönlendirebileceği ve iletebileceği bilgi güvenliği ile ilgili süreçleri bilgi güvenliği yönetimine ilişkin kavram, süreç ve hedefler hakkında rehberlik sağlamaktadır. Herhangi bir alanda faaliyet gösteren ve farklı büyükteki tüm kurum ve kuruluşlar için geçerli olan bu standardın hedef kitlesi; kurum ve kuruluşların yönetim yapısı ve üst yönetim, ISO/IEC 27001'i esas alan BGYS'ni değerlendirmek, yönlendirmek ve izlemekten sorumlu olanlar ile bilgi güvenliği yönetimi kapsamında bulunan fakat ISO/IEC 27001'i esas alan BGYS dışında yürütülen bir bilgi sistemi güvenliği yönetiminden sorumlu olanlardır (ISO/IEC 27014, 2020).

Bu standart, bilgi güvenliği yönetiminin, ISO/IEC 27001'i esas alan BGYS içerisinde nasıl bir yürütüldüğünü ve söz konusu faaliyetlerin, BGYS kapsamı dışında yürütülen diğer yönetim faaliyetleriyle nasıl ilişkili olabileceğini göstermektedir. Bu standart, bir kuruluş içerisinde yapısallaştırılacak bir bilgi güvenliği yönetim sistemindeki ana süreçleri (değerlendirme, yönetim, gözlem ve iletişim) temel hatlarıyla belirtmekle olup, her bir süreçte bilgi güvenliği yönetiminin kurumsal yönetim faaliyetlerine dahil edilmesine yönelik yaklaşımlar sunmaktadır. Ayrıca, bilgi güvenliği yönetimi, bilgi teknolojisi yönetimi ve kurumsal yönetim arasındaki ilişkiler açıklanmaktadır. Bu standart kapsamında belirtilen "Varlık Yönetimi ve Bilgi Güvenliği Yönetimi"ne ilişkin hedefler şu şekildedir (ISO/IEC 27014, 2020) :

- Kuruluş genelinde bütünleşik, kapsamlı bilgi güvenliğinin oluşturulması,
- Risk temelli bir yaklaşım kullanarak kararlar alınması,
- Bilgi güvenliği ediniminin yönünün belirlenmesi,
- İç ve dış gerekliliklere uygunluğun sağlanması,
- Olumlu bir bilgi güvenliği kültürünün teşvik edilmesi,
- Bilgi güvenliği performansının kuruluşun mevcut ve gelecekteki gereksinimlerini karşıladığından emin olunmasıdır.

4.2.16. ISO/IEC 29100:2011 Bilgi Teknolojisi - Güvenlik Teknikleri – Gizlilik Çerçevesi

Bu standart, bilgi ve iletişim teknolojisi sistemlerinde bulunan kişisel bilgilerin (personally identifiable information) korunması kapsamında bir çerçeve sağlamaktadır. Bu bağlamda standart, kurumsal, teknik ve ilkesel unsurları genel bir gizlilik çerçevesine yerleştirmektedir. Söz konusu gizlilik çerçevesi, kuruluşların bilgi ve iletişim teknolojisi ortamlarında kişisel bilgilere ilişkin gizlilik koruma gereksinimlerini şu yollarla tanımlamalarına yardımcı olmaktadır (ISO/IEC 29100, 2011):

- Ortak bir gizlilik terminolojisinin belirlenmesi,
- Kişisel bilgilerin işlenmesindeki aktörlerin ve rollerinin tanımlanması,
- Gizliliğin korunması için gerekliliklerin tanımlanması,
- Bilinen gizlilik ilkelerine atıfta bulunulması.

Bu uluslararası standart, kişisel bilgilerin işlenmesiyle ilgili bir odak noktası ekleyerek mevcut güvenlik standartlarının geliştirilmesini amaçlanmaktadır. Bu standart, kişisel bilgilerin işlemesi kapsamında, gizlilik kontrollerinin gerekli olduğu bilgi ve iletişim teknolojisi sistemlerinin veya hizmetlerinin belirlenmesi, tasarlanması, tedarik edilmesi, geliştirilmesi, test edilmesi, sürdürülmesi, yönetilmesi ve işletilmesinde yer alan gerçek kişiler ve kuruluşlar için geçerlidir (ISO/IEC 29100, 2011).

Bu standardın temelini 11 gizlilik ilkesi oluşturmaktadır. Bu ilkeler; 1. Rıza ve Seçim, 2. Amacın Meşruiyeti ve Belirtilmesi, 3. Toplama Sınırlaması, 4. Veri Minimizasyonu, 5. Kullanım, Saklama ve İfşa Sınırlaması, 6. Doğruluk ve Kalite, 7. Açıklık, Şeffaflık ve Bilgilendirme, 8. Bireysel Katılım ve Erişim, 9. Sorumluluk, 10. Bilgi Güvenliği ve 11. Gizlilik Uyumluluğu'dur. Söz konusu ilkeler, gizlilik politika ve kontrollerinin tasarımı, uygulanması ve geliştirilmesine rehberlik etmekle birlikte, herhangi bir kuruluşta var olan gizlilik yönetimi programlarına ait performansın gözlemlenmesi ve ölçülmesi, denetlenmesi ve kıyaslanmasında bir temel olarak kullanılabilmektedir (ISO/IEC 29100, 2011).

4.2.17. ISO/IEC 29101:2018 Bilgi Teknolojisi - Güvenlik Teknikleri – Gizlilik Mimarisi Çerçevesi

Bu standart, kişisel bilgilerin saklandığı ve işlendiği bilgi ve iletişim teknolojisi sistemlerinde gizliliğin sağlanmasına ilişkin bir mimari çerçeveyi ve ilgili kontrolleri açıklamaktadır. ISO/IEC 29100 tarafından sağlanan gizlilik çerçevesi üzerine kurulmuş olan bu standart kapsamında belirtilen gizlilik mimarisi çerçevesi;

- Kişisel bilgilerin işlendiği bilgi ve iletişim teknolojisi sistemleri için gizlilik kontrollerinin uygulanmasına yönelik tutarlı, üst düzey bir yaklaşım sağlamakta,
- Kişisel bilgilerin işlenmesini, erişimini ve aktarımını kontrol ederek kişisel bilgi ilkelerinin gizliliğini koruyan bilgi ve iletişim teknolojisi sistem mimarilerinin planlanması, tasarlanması ve oluşturulması için rehberlik sağlamakta,
- Gizliliği artıran teknolojilerin gizlilik kontrolleri olarak nasıl kullanılabileceğini göstermektedir (ISO/IEC 29101, 2018).

Bu standart, kişisel bilgi prensipleriyle etkileşimde olmak maksadıyla tasarlanmış olan bilgi ve iletişim teknoloji sistemlerine odaklanmakla birlikte, kişisel bilgileri işleyen bilgi ve iletişim teknoloji sistemlerine ilişkin hususların belirtildiği, bu tür sistemlerin uygulanmasına yönelik bileşenlerin listelendiği ve bu bileşenleri kavramsallaştıran mimari görünümlerin sağlandığı bir gizlilik mimarisi çerçevesi tanımlamaktadır. Bu gizlilik mimarisi çerçevesi teknik bir referans olarak tanımlanmış olup, gizlilik politikalarına yönelik gereklilikleri belirtmemektedir (ISO/IEC 29101, 2018).

4.2.18. Kalıcı Belgelerin Korunmasına Yönelik Standartlar (NFBA)

Kalıcı değere sahip belgelerin koruma altına alınmasına yönelik birçok ulusal standart olmakla birlikte, ABD Ulusal Yangın Koruma Birliği (the National Fire Protection Association (NFPA)) tarafından uluslararası kullanım değerine sahip standartlar yayınlanmaktadır (Külcü, 2007, ss. 260-262). ISO 15489-1:2016 standardı, hırsızlık ve afetler dahil olmak üzere belgelerin bütünlüğü, özgünlüğü ve güvenliğine yönelik bir standart iken, NFA'nın amacı arşiv değerine sahip belgelerin muhtemel bir yangından korunması için gerekli depolama alanları oluşturulması, ekipmanların ve olanakların

belirlenmesine yönelik bilgileri kapsamaktadır. Kalıcı belgelerin yangın korunmasına yönelik NFPA tarafından yayınlanan standartlar şunlardır:

- NFPA 75 (2020) Bilgi Teknolojisi Ekipmanları Koruma Standardı (Standard for Information Technology Equipment Protection): Bu standart, bilgi teknolojisi ekipmanlarının ve bilgi teknolojisi ekipman alanlarının yangın veya ilişkili etkilerinden (duman, oksitlenme, sıcaklık, su vb.) kaynaklanan yangın hasarından korunması için gereklilikleri kapsamaktadır.
- NFPA 232 (2022) Belge Koruma İçin Standart (Standard for the Protection of Records): Bu standart, çeşitli medya formunda bulunan kayıtları yangın tehlikelerinden ve ilgili etkilerinden koruyan, kayıt koruma ekipmanı ve tesisleri ile kayıt işleme teknikleri için gereklilikleri sağlamaktadır.
- NFPA 909 (2021) Kültürel Kaynakların Korunması İçin Düzenleme- Müzeler, Kütüphaneler ve İbadet Yerleri (Code for the Protection of Cultural Resource Properties - Museums, Libraries, and Places of Worship): Bu düzenleme, kültürel kaynakların (müzeler, kütüphaneler, ibadethaneler vb.) içeriklerinin ve koleksiyonlarının hasar görmesine ya da kaybolmasına sebebiyet verebilecek koşullara karşı korunmasına yönelik ilke ve uygulamaları açıklamaktadır.

4.3. PROJELER

4.3.1. Açık Veri Projesi

11. Kalkınma Planında (2019-2023) kamu kurum ve kuruluşlarına ait verilerin, hesap verilebilirlik, şeffaflık, yönetime katılımı artırmak ve yeni hizmetlerin yaratılmasına olanak sağlaması maksadıyla mahremiyet ilkeleri göz önüne alınarak açık veri olarak kullanıma sunulacağı belirtilmiştir. Ayrıca planda, kamu verilerin paylaşılmasına yönelik düzenlemeler yapılacağı, Ulusal Açık Veri Portalı oluşturularak kamu verilerinin bu portal üzerinden paylaşılacağı ve bu bağlamda kamu verilerin anonimleştirilmesine yönelik hususların belirleneceği ifade edilmiştir (Cumhurbaşkanlığı Strateji…, 2019, mad. 815).

Bu plana istinaden, Dijital Dönüşüm Ofisi Başkanlığı koordinatörlüğünde “Açık Veri Projesi” başlatılmıştır. Projenin amacı, kamu verilerinin kişisel veri, ulusal ve ticari sır hususları göz önüne alınarak mahremiyetlerinin sağlanması ile açık devlet verilerin

hesap verilebilir ve şeffaflığa dayalı bir yönetimin anlayışının benimsenmesi ve yenilikçi teknolojilerin geliştirilmesine yardımcı olmaktır. Proje sayfasında, Ulusal Açık Veri Portalı'nın oluşturulmasına yönelik çalışmaların devam ettiği, kamu verilerin açık olarak paylaşılmasına yönelik yasal ve teknik süreçlerin yürütüldüğü ve açık devlet verisine ilişkin veri yönetimi mevzuatı, idari düzenlemeler ile rehber dokümanlarının hazırlanmakta olduğu ifade edilmektedir (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023b).

4.3.2. Ulusal Veri Sözlüğü Projesi

Günümüzde kurumların tamamı iş süreçlerini ve yerine getirdiği hizmetleri sürdürebilmek için bilgi sistemleri vasıtasıyla veri üretilmekte, sağlamakta ve bu verileri başka sistemlerle paylaşmaktadır. Fakat, kurumlar standart olmayan farklı veri tiplerine sahiptirler. Örneğin, bir cinsiyet bilgisi bilgi sistemlerinde Erkek/Kadın, E/K, Bay/Bayan ya da 0/1 olarak farklı değerlerle ifade edilmektedir. Bununla birlikte, kurumlar farklı hizmet sağlayıcıları marifetiyle bilgi sistem yazılımlarını oluşturmaktadır. Dolasıyla kurumsal bilgi sistemlerinde bulunan verilerin ne anlama geleceği ve nasıl saklanacağı gibi konular yazılım geliştiricilerin inisiyatifine bırakılmaktadır. Sonuç olarak, bilgi sistemleri arasında veri paylaşımına yönelik sorunlar ortaya çıkmakta ve bu durum kurumsal hafızanın oluşturulmasını engellemektedir.

Bilgi sistemlerinde bulunan verilerin birbirleriyle çelişmesi, dil birliğinin bulunmaması, veri sahipliğinin belirsizliği ve sistemler arasında veri paylaşımına yönelik entegrasyon zorlukları gibi problemlerin çözümü amacıyla Ulusal Veri Sözlüğü projesi başlatılmıştır (Cumhurbaşkanlığı Dijital Dönüşüm…, 2020b). Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin sorumluluğunda 2019 yılında başlatılan bu proje ile kurumlarda verilerin standartlaştırılarak tekilleştirilmesi, ortak bir dilin oluşturulması ile ulusal veri envanterinin hazırlanması hedeflenmiştir. Proje kapsamında yerine getirilen süreçler şu şekildedir (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023c):

- ISO/IEC 11179 standardı, ulusal standart (TS ISO/IEC 11179) olarak kabul edilmiş, bu standart çerçevesinde Veri Sözlüğü Portalı oluşturularak kullanıma sunulmuş,
- Veri Sözlüğü Oluşturma Metodoloji belirlenmiş,
- Eğitim müfredatı ve eğitim takvimi oluşturulmuş,

- Ulusal Veri Sözlüğü sistemine ilişkin ortaya çıkabilecek problemlerin çözümlerine destek sağlamak maksadıyla Yardım Masası oluşturulmuş,
- Eğitici eğitimleri verilmiştir.

4.3.3. Kamu Sanal Ağı (KamuNet) Projesi

Bakanlar Kurulunun 2012/3842 sayılı kararına istinaden oluşturulan Siber Güvenlik Kurulu tarafından verilen kararlar kapsamında, kamu kurum ve kuruluşların Kamu Sanal Ağı'na (KamuNet) entegre olması ile ilgili Başbakanlık Genelgesi (2016/28) 2016 yılında, KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ ise 2017 yılında yayımlanmıştır.

KamuNet, kamu kurum ve kuruluşları arasında gereksinim duyulan veri iletişiminin, internete erişimi olmayan ve güvenli bir sanal ağ aracılığıyla gerçekleştirilerek siber güvenlik risklerinin azaltılması amacıyla kurulmuş bir ağdır. Ulaştırma ve Altyapı Bakanlığının 2021 Yılı Faaliyet Raporunda, KamuNet'e dahil olan kurum sayısının 140'a ulaştığı ve siber güvenlik risklerinin mümkün olduğunca azaltılması kapsamında KamuNet'de verilen servis sayısının ise 800'ün üzerinde olduğu belirtilmiştir (Ulaştırma ve Altyapı…, 2021). Kamu kurum ve kuruluşlarınca KamuNet ağı vasıtayla yapılan veri trafiği güvenliğinin sağlanması amacıyla ağının uçtan uca şifreli hale getirilmesi çalışmalarına başlanılmıştır (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023a).

KamuNet ağına dahil olmak isteyen kamu kurum ve kuruluşları tarafından, tebliğ'de belirtilen asgari gereksinimleri yerine getirilmesi ve bunların kayıt altına alınması gerekmektedir (Ulaştırma, Denizcilik…2017). Söz konusu gereksinimlerde ağırlıklı olarak, BGYS'nin kurması, belgelendirmesi ve personele eğitim vermesi üzerinde şekillenmektedir.

4.3.4. Ulusal Kamu Entegre Veri Merkezi (UKEVM) Projesi

Dünya genelinde gözlenen veri merkezlerinin birleştirilmesine yönelik eğilim ile birlikte Türkiye'de, Bilim ve Teknoloji Yüksek Kurulu tarafından Ulusal Veri Merkezi çalışmalarının yapılmasına yönelik tavsiye niteliğinde kararlar alınmış ve bu kapsamda Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumlu kuruluş olduğu belirtilmiştir (Bilim ve Teknoloji…, 2013). Elektronik Haberleşme Kanunu'nda (2008) 27 Mart 2015

tarihinde yapılan düzenlemeyle bu görev Ulaştırma, Denizcilik ve Haberleşme Bakanlığının verilmiştir (Elektronik Haberleşme Kanunu, 2008, mad. 5 (ı)).

Halihazırda Ulaştırma ve Altyapı Bakanlığının sorumluluğunda olan UKEVM Projesiyle kamu veri merkezlerinin bütünleştirilmesi ve kamu kurumlarına ait tüm verilerinin tek bir ekosistemde toplanarak söz konusu verilerin yönetilmesi, saklanması, işletilmesi, sunulması ve yüksek düzeyli güvenliğinin sağlanması amaçlanmaktadır. UKEVM ile birlikte;

- Kamu kurumlarının (Veri Merkezi kurmuş olan ya da kurulacak olan) münferit olarak harcama yapması engellenerek iş süreçlerinde, yatırımlarda ve enerjide verimliliğin sağlanacağı,
- Siber güvenlik tehditleri kısa bir zamanda belirlenerek bu tehditlerin çok hızlı bir biçimde önlenebileceği,
- Kurumlar arasındaki iletişimde bilgi güvenliği problemlerinin asgari düzeyde olacağı,
- Bilgi teknolojileri hizmetlerinin daha ekonomik ve verimli olarak sunulacağı,
- Kamu kurumlarının bilgi teknolojilerine yönelik stratejilerinin açık bir şekilde belirlenmesi ve gelişmesine katkı sağlayacağı ifade edilmektedir (Ulaştırma ve Altyapı…, 2023b).

Bakanlığının 2022 Yılı Faaliyet Raporunda; UKEVM fizibilite etüdünün %50 oranda gerçekleştirildiği ve çalışmalarının devam ettiği, bu etüdün tamamlanmasını müteakip tasarım, inşaat, standartlar, kanuni düzenleme vb. düzenlemelerin yerine getireceği ifade edilmektedir (Ulaştırma ve Altyapı Bakanlığı, 2023c).

4.3.5. Elektronik Kamu Bilgi Yönetim Sistemi (KAYSİS) Projesi

Elektronik Kamu Bilgi Yönetim Sistemi (KAYSİS) Projesi, "*kamu kurum ve kuruluşlarının teşkilat yapısının tanımlanmasından, sunulan hizmetlere; hizmetlerde kullanılan belgelerden, kurumların iletişim ve yönetici bilgilerine kadar kamu yönetiminde yer alan unsurların mevzuat dayanaklarıyla birlikte tespit edilerek elektronik ortamda tanımlandığı, geliştirilen Dijital Türkiye (e-Devlet) uygulamalarının birbirine tek merkezden entegre edilmesini sağlayacak bilgi yönetim sistemi*" olarak tanımlanmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023d).

KAYSİS projesinin amacı; devlet organlarının tarihsel gelişiminin elektronik ortamda tutulması, kurum faaliyetlerinin standart hale getirilmesi ve bunların elektronik ortamda tanımlanması, bürokratik süreçlerin belirlenmesi, kamusal faaliyetlere ilişkin mevzuat dayanaklarının ayrıntılı olarak ilişkilendirilerek güncelliğini yitiren mevzuatın tespit edilmesi, Dijital Türkiye çalışmaların planlanması ve resmi yazışmalara ilişkin verilerin, sunulan hizmetlerin, iletişim bilgilerinin ve yürütülen mevzuatın paylaşılmasıdır (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023d).

KAYSİS "Devlet Teşkilatı Merkezi Kayıt Sistemi (DETSİS)", "Hizmet Envanteri Yönetim Sistemi (HEYS)" ve "Kamu Mevzuat Sistemi (KMS)" gibi alt modüllere sahiptir. KAYSİS'in alt uygulamaları vasıtasıyla yerine getirilecek hususlar şunlardır (DETSİS, 2023; HEYS, 2023; KMS, 2023):

- Kamu kurum ve kuruluşlarının teşkilatlarında bulunan birimlerin tanımlanması ve yaşayan organizasyon şemalarının oluşturulması,
- Elektronik olarak verilen hizmetlere ulaşım imkanın sağlanması,
- E-yazışma ve e-imza süreçlerine ilişkin gerekli verilerin sağlanması,
- Kamu kurum ve kuruluşları tarafından yürürlüğe konulan mevzuatın kayıt altına alınması,
- Kamusal hizmetlerin ve bunların paylaşılma süreçlerinin belirlenmesi,
- Kamusal hizmetlerin sunumu kapsamında yapılan resmi yazışmalar ve bu yazışmalara ilişkin onaylama süreçlerinin belirlenmesi ve bunların ilgili hizmetler ile bütünleştirilmesi,
- Kamusal hizmetlerin sunulmasına ilişkin istatistiklerin toplanmasıdır.

4.3.6. Elektronik Yazışma (E-yazışma) Projesi

Bu proje, kamu kurum ve kuruluşlarının resmi yazışma süreçlerinin elektronik ortamda emniyetli olarak yürütülmesi için gerekli standartların belirlenmesi amacıyla başlatılmış olup, halihazırda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda yürütülmektedir. E-yazışma projesi çerçevesinde, söz konusu resmi yazışmalar ile bu yazışmaların e-imzalarını ve üst verilerini taşıyacak olan e-yazışma paketi belirlenmiş ve kurumlar arasındaki belge trafiğinin güvenli şekilde sağlanmasına yönelik şifreleme mekanizması ortaya konulmuştur (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023e).

Elektronik ortamda bulunan bir resmi yazıya ait tüm bileşenlerin (e-imza, dağıtım listesi, ekler, üst veriler vb.) belirlenen kurallara uygun bir biçimde bir dosyada sunulması maksadıyla e-Yazışma Paketi oluşturulmuştur. Bir e-Yazışma Paketi, e-Yazışma Teknik Rehberinde tanımlanan standartları sağladığı zaman geçerli olmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023e). Söz konu teknik rehber e-Yazışma Paketi içerisinde bulunan mekanizmaların prensiplerini ve resmi yazışmaların paylaşımına yönelik teknik standartları tanımlanmaktadır. Rehberde ayrıca, kurumlar arası entegrasyon çalışmalarına yönelik genel bilgiler yer almakta, proje kapsamında geliştirilen e-Yazışma Paket tasarımı ayrıntılı bir şekilde açıklanmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023f; E-yazışma Teknik…, 2023).

E-yazışma Projesi kapsamında, kamu idarelerinin, sahip oldukları EBYS'lerine ithal edebilecekleri yazılım programlama arayüzü (API) geliştirilmiştir. API'nin son sürümü (v2.o) Ağustos 2020'de yayımlanmıştır. Proje bağlamında hazırlanan e-Yazışma Teknik Rehberi ve e-Yazışma API'lerin yanı sıra, e-Yazışma Paketi yardım dokümanları oluşturulmuştur (Cumhurbaşkanlığı Dijital Dönüşüm…, 2023e).

4.3.7. Bütünleşik Arşiv Yönetim Sistemi Projesi

Kurumsal kapasitenin iyileştirilmesi kapsamında, Başbakanlık Strateji Geliştirme Başkanlığı ve Devlet Arşivleri Başkanlığı marifetiyle 2017 yılında "Kamu Arşivlerinin Standardizasyonu ve Entegrasyonu Projesi" hayata geçirilmiştir. Söz konusu entegrasyon projesine yönelik çalışmalar ile Devlet Arşivleri Başkanlığının sorumluluğunda bulunan "Devlet Arşiv Ağı" (DAA) ve "Devlet Arşivi Veri Merkezi" (DAVM) çalışmaları 2019 yılında "Bütünleşik Arşiv Yönetim Sistemi Projesi" çatısı altında yürütülmeye başlanmıştır (Devlet Arşivleri Başkanlığı…, 2018; Rukancı ve diğerleri, 2021, s. 53).

Bütünleşik Arşiv Yönetim Sistemi Projesi; arşiv belgelerinin belirlenmesi, Devlet Arşivleri Başkanlığına gönderilmesi, depolanması ve tasnifinin yapılarak araştırma hizmetine sunulması, belge tanımlamalarının yapılmasına ilişkin mantıksal indeks oluşturulması, DAA ve DAVM'nin hayata geçirilmesi, Devlet Arşivleri Başkanlığı Hakkındaki Cumhurbaşkanlığı Kararnamesinde yükümlü olarak ifade edilen kurum ve kuruluşlar tarafından yerine getirilen arşiv faaliyet ve hizmetlerinin değerlendirilmesi, faaliyet ve birimler arasındaki bağlantı ve süreçlerin belirlenmesini kapsayan birden

fazla bileşenden meydana gelecek bir otomasyon sistemi olarak tanımlanmaktadır (Devlet Arşivleri Başkanlığı, 2023a, s.52).

4.3.8. Devlet Arşiv Ağı ve Devlet Arşivi Veri Merkezi

Devlet Arşivleri Başkanlığı, Cumhurbaşkanlığı Kararnamesiyle 2018 yılında Cumhurbaşkanlığına bağlanmıştır (Devlet Arşivleri Başkanlığı…, 2018). Bu kararname ile Devlet Arşivleri Başkanlığına "Devlet Arşiv Ağı" (DAA) ve "Devlet Arşivi Veri Merkezi" (DAVM) kurma görevi verilmiştir. DAA "*Araştırmaya açılan arşivlere tek merkezden erişim sağlanması amacıyla kurulan bilişim ağı*" ve DAVM ise "*Kamu kurum ve kuruluşları tarafından üretilmiş belgelerin bir sistem içerisinde saklandığı ve kontrollü bir şekilde erişilebildiği merkez*" olarak tanımlanmaktadır (Devlet Arşivleri Başkanlığı, 2018, mad. 4). Devlet Arşivleri Başkanlığının 2020-2024 Dönemi Stratejik Planı'nda DAA ve DAVM çalışmalarına başlanıldığı ve bu sürecin %90'nın 2024 yılında tamamlanacağı belirtilmektedir (Devlet Arşivleri Başkanlığı…, 2019, ss. 5-6).

Veri merkezi ve ağ yapısı, kamu kurum ve kuruluşlarında bulunan veri, bilgi ve belgelerin sistemli olarak yönetilmesinin (depolanması ve gerektiğinde erişimin sağlanması) ana unsurlarındandır. Bu bağlamda, Türkiye'de veri, bilgi ve belgelerin yönetimine (depolama, güvenlik, erişim vb.) ilişkin politikalar geliştirilmiştir. Bu bağlamda, kamu kurumlarına ait verilerin tek merkezde (Ulusal Kamu Entegre Veri Merkezi Projesi) bir araya getirilmesi ve kurulacak emniyetli bir ağ (KamuNet Projesi) üzerinden veri, bilgi ve belge paylaşılmasına yönelik politikalar geliştirilmiştir. Söz konusu veri merkezi ve güvenli ağ yapısı veri, bilgi ve belgelerin saklanması ve paylaşımı kapsamında birbirleriyle ilişkili olarak ve tamamlayıcı özellikte iki temel unsur olarak değerlendirilmektedir (Rukancı ve diğerleri, 2021, s. 14).

Kurumların veri merkezleri ile Devlet Arşivi Veri Merkezinin entegrasyonunun sağlanmasıyla (Devlet Arşivleri Ağı yardımıyla) veri, bilgi ve belge transfer ve paylaşımı gerçekleştirilecek ve araştırmacılara verilen hizmetler ile kurumların (Devlet Arşivleri Başkanlığı Hakkındaki Cumhurbaşkanlığı Kararnamesinde yükümlü olarak ifade edilen kuruluşlar) faaliyetlerini Devlet Arşivleri Ağı vasıtayla yürütmesi sağlanacaktır. Rukancı ve diğerleri (2021, s.15), Devlet Arşivi Veri Merkezi ve Devlet Arşivleri Ağına ilişkin depolama ve güvenlik cihazlarını kapsayan bilişim alt yapısı (donanım ve yazılım) beraber değerlendirildiğinde eksiksiz bir arşiv otomasyon sisteminden söz

edilebileceğini ve söz konusu uygulamanın Ulusal Kamu Entegre Veri Merkezi ve KamuNet güvenli ağ yapısıyla ya da gelecekte uygulamaya sokulabilecek değişik yapılar ile bütünleşebileceğini ifade etmektedirler.

4.4. MEVZUAT

4.4.1. 5070 Sayılı Elektronik İmza Kanunu

E-imzanın yasal ve teknik durumu ile uygulanmasına yönelik esasların belirlendiği Elektronik İmza Kanunu 2004 yılında yürürlüğe girmiştir. Bu kanun, e-imzanın yasal durumu ve kullanımı ile hizmet sağlayıcıların etkinliklerine yönelik işlemleri kapsamaktadır. Bu kanun dört kısımdan oluşmakta olup, birinci kısmında, kanunun kapsamı, amacı ve kanunda yer alan ifadelerin tanımları yapılmaktadır. İkinci kısımda, güvenli e-imzanın tanımı, uygulama alanı ve hukuki sonucu, elektronik sertifikalar, güvenli e-imza oluşturma ve doğrulama araçları ve hizmet sağlayıcıların işlemlerine ve sorumluluklarına ilişkin düzenlemeler yapılmıştır. Üçüncü kısımda, denetim, izin ve ceza hükümleri bulunmaktadır. Dördüncü kısımda ise kanun kapsamında çeşitli hükümlere yer verilmektedir (Elektronik İmza Kanunu, 2004).

4.4.2. 4982 Sayılı Bilgi Edinme Hakkı Kanunu

Bilgi Edinme Hakkı Kanunu'na göre tüm bireyler bilgiye erişim hakkına sahiptir. Kanunda belirtilen istisnalar dışında, başvuru sahibi kamu kurum ve kuruluşlarda bulunan her türlü bilgi veya belgeye erişebilmekte olup, bu bilgi ve belgeler ticari amaçla çoğaltılarak kullanılamamaktadır. Kanunda, bilgi ve belge talebinin karşılanamayacağı koşullar düzenlenmiş olup, paylaşılması mümkün olmayan bilgi ve belgeler (devlet sırrı, gizlilik dereceli, askeri ve istihbarata ilişkin bilgi ve belgeler vb.) açıkça belirtilmiştir (Bilgi Edinme Hakkı…, 2003, mad. 16-25 ve 27).

4.4.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Kişisel Verilerin Korunması Kanunu'nun amacı "*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir*" (Kişisel Verilerin Korunması…, 2016). Kanun'da kişisel ve özel nitelikli

kişisel verilerin tanımı yapılmış, bunların işlenme şartlarına ilişkin tanımlamalar ve düzenlemelere yer verilmiştir. Kanunda kişisel veriler üzerinde gerçekleştirilen her türlü işlem (elde etme, muhafaza etme, değiştirme, yeniden düzenleme, kaydetme, aktarma, açıklama, sınıflandırma, kullanılmasını engelleme vb.) kişisel verilerin işlenmesi olarak tanımlanmakta olup, bunların işlenmesi için kişinin açık rızasının olması gerektiği, fakat kanunda belirtilen istisnalar çerçevesinde kişinin açık rızası aranmadan kişisel verilerin işlenebileceği ifade edilmektedir (Kişisel Verilerin Korunması…, 2016).

4.4.4. 5902 Sayılı Savunma Sanayii Güvenliği Kanunu

Bu kanun, savunma sanayii faaliyetleri kapsamında gerçekleştirilen süreçlerin gizlilik temelinde güvenli bir şekilde yerine getirilmesi için alınması gereken tedbirler ile kanun kapsamında bulunan gerçek ve tüzel kişiler ile fiziki mekanların gerekliliklerini belirlemektedir. Kanun'da "Çok Gizli", "Gizli", "Özel" ve "Hizmete Özel" olmak üzere dört adet gizlilik derecesi belirlenmiş ve bu gizlilik derecelerini taşıyacak bilgi, belge ve malzemelerin neler olduğu belirtilmiştir. Kanun'a göre savunma sanayii faaliyetleri kapsamında gizlilik dereceli varlıklara erişimi olabilecek herkesin "Kişi Güvenlik Belgesi"ne ve bu faaliyetlerin yürütüleceği fiziki mekanların ise "Tesis Güvenlik Belgesi"ne sahip olması gerekmektedir. Ayrıca Kanun'da, faaliyetlerin icra edildiği fiziki mekanların güvenliğine yönelik fiziki önlemlerinin "Özel Güvenlik Hizmetlerine Dair Kanun"da belirtilen hususlara göre yerine getirmesi zorlu tutulmuştur (Savunma Sanayii Güvenliği…, 2004).

4.4.5. 7315 Sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu

Bu kanun, kimler hakkında güvenlik soruşturması ve arşiv araştırmasının yapılacağını, bu araştırmanın gerçekleştirilmesine ve sağlanacak bilgilerin kullanımına yönelik temel ilkelerin neler olduğunu, hangi bilgi ve belgelerin araştırma konusu olacağını, bu bilgilerin nasıl kullanılacağını, elde edilen verilere yönelik emniyet, muhafaza ve yok edilme süreçlerini, soruşturma ve araştırma yapacak hangi mercilerin yetkili olduğunu, oluşturulan/oluşturulacak "Değerlendirme Komisyonu"nun yapısını ve görevlerini belirlemektedir (Güvenlik Soruşturması…, 2021).

Arşiv araştırması, mevcut kayıtlar kullanılarak araştırılmaya konu olan kişinin kolluk kuvvetlerince aranıp aranmadığının, adli sicil durumunun, kamu görevinden çıkarılıp

çıkarılmadığının veya memurluktan çıkarılma kararlı kesinleşmiş cezasının olup olmadığının ve araştırması yapılan kişiye yönelik bir kısıtlamanın olup olmadığının, kişi hakkında adli yargıda bir soruşturma, kovuşturma, devam eden bir yargılama veya mahkeme kararının bulunup bulunmadığının tespit edilmesidir. Kamu görevine ilk defa atanacaklar ile yeniden memuriyet görevine başlayacaklar hakkında arşiv araştırması yapılmaktadır. Güvenlik soruşturması ise, arşiv araştırmasında belirtilen hususlara ek olarak kişinin yerine getireceği görev için gerekli olan özelliklere ilişkin istihbarat ve kolluk kuvvetlerindeki olgusal verilerin, yabancılarla ve yabancı devlet kurumlarıyla ilişiğinin bulunup bulunmadığının, suç işlemek maksadıyla kurulan örgüt veya terör örgütleriyle ilişkili, iltisaklı veya iş birliğinde bulunup bulunmadığının soruşturulmasıdır.
Bir kişinin kamu görevine başlayabilmesi için yeterli güvenilirlikte olup olmadığının tespiti amacıyla yapılan arşiv araştırması ve güvenlik soruşturmasına ilişkin veriler, araştırma ve soruşturma yapmaya yetkili birimler tarafından ilgili Değerlendirme Komisyonuna iletilmektedir. Değerlendirme Komisyonu tarafından, alınan veriler ışığında yapılan değerlendirmeler personeli atamaya yetkili mercilere yazılı olarak sunulmaktadır (Güvenlik Soruşturması…, 2021)..

4.4.6. Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik

Bu yönetmelik, arşiv araştırması ve/veya güvenlik soruşturması yapılmasını isteyen kurum ve kuruluşları, araştırmayı ve soruşturmayı gerçekleştirecek birimleri ve hakkında araştırma ve/veya soruşturma yapılacak kişileri kapsamaktadır. Yönetmelik'te, arşiv araştırması ve güvenlik soruşturmasının yapılmasına yönelik ilke, usul ve esaslar ile izlenecek yöntemlere yönelik açıklayıcı hükümler bulunmaktadır. Yönetmelik'te, kamu kurum ve kuruluşlarındaki hangi bölümlerin gizlilik dereceli birim ve kısımlar olacağı belirtilmiştir. Ayrıca, arşiv araştırması ve güvenlik soruşturmasına konu olan kişi hakkındaki araştırma ve soruşturma sonucuna ait bilgi ve belgelerin en az "gizli" gizlilik derecesinde ilgili kurum dosyasında fiziki ve/veya elektronik ortamda saklanması gerektiği, istihbari hususları içeren bilgi ve belgelerin ise elektronik ortamda muhafaza edilemeyeceği ifade edilmektedir (Araştırması Yapılmasına Dair…, 2022).

4.4.7. Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik

Kamu kurum ve kuruluşlarını kapsayan bu yönetmeliğin amacı, fiziki veya elektronik ortamlarda gerçekleştirilen resmi yazışmaların kurallarını çerçevelemek, yazışma süreçlerini güvenli ve hızlı bir şekilde yürütmek ve uygulama yeknesaklığını sağlamaktır. Yönetmelik'te resmi yazışmalara ilişkin belgenin şekil özellikleri, oluşturulacağı ortamlar, kaç nüsha hazırlanacağı, yazı tipleri ve bu yazılarının büyüklükleri, kısımları, gizlilik derecesi, kişisel olma durumları, süreli olma durumu (miatlı), üst veri elemanları, çoğaltılması, gönderilmesi, alınması, iade edilmesine yönelik işlemler açıklanmaktadır.

Yönetmelik'e göre zorunluluk arz eden veya olağanüstü durumlardaki yazışmalar ile "Özel" gizlilik derecesine ve bunun üst gizlilik derecesine haiz yazışmaların fiziki ortamda, gizlilik derecesi bulunmayan ve "Hizmete Özel" gizlilik derecesine haiz yazışmaların ise elektronik ortamda gerçekleştirileceği belirtilmektedir. Bununla birlikte, 23 Ekim 2010 tarihli ve 27738 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren "Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik"te yetkili kılınan idareler (elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili olan Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı ile bu kurumlara ait kodlu veya kriptolu elektronik haberleşme sistemlerinin kullanıldığı kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler) tarafından gizlilik dereceli belgelerin güvenlik gerekli tedbirlerin alınması koşuluyla elektronik ortamlarda gönderebileceği belirtilmektedir.

4.4.8. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik

Bu yönetmelik 2022 yılında yürürlüğe girmiş ve hizmete özel gizlilik derecesine sahip olması sebebiyle resmi gazetede yayımlanmayan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar"ı (Özdemirci ve Torunlar, 2015, s. 47) geçersiz kılmıştır. Fakat bu esaslara yapılan atıfların yönetmeliğe yapılmış sayılacağı belirtilmektedir (Gizlilik Dereceli Belgelerde…, 2022). Yönetmelik yalnızca gizlilik dereceli belgeleri kapsamakta olup, bilgi notu, doküman, mesaj, veri, toplantı ve bilgi içeren materyalin gizliliği yönetmelik kapsamı dışında tutulmuştur (Gizlilik Dereceli Belgelerde…, 2023).

Yönetmelik'te, gizlilik derecesinin kullanımına, gizlilik dereceli belgelerin hazırlanması, gönderilmesi, teslim edilmesi ve alınması, saklanması ve sayımı, çoğaltılması, gizlilik derecelerinin düşürülmesi, imhası, arşive transfer edilmesine yönelik usul ve esaslar ile genel güvenlik tedbirlerine, personele ilişkin genel hükümlere ve Gizlilik Dereceli Belgeleri Değerlendirme Komisyonlarına ilişkin hususlara yer verilmiştir. Yönetmelik'te, belgelerin gizlilik derecesinin güncelliğini yitireceği zaman ya da olay kapsamında gizlilik derecelerinin düşürülmesi veya kaldırılması ya da belgelerin imha edilmesine yönelik "Süreli Gizlilik" uygulaması tanımlanmış ve bu uygulamaya yönelik açıklamalar yapılmıştır. Yönetmelik'te ayrıca, hangi makam veya kişilerin gizlilik derecesi tayin etmeye yetkili olduğu belirtilmektedir.

Yönetmelik'te "Çok Gizli", "Gizli" ve "Hizmete Özel" olmak üzere üç adet millî gizlilik derecesi belirlenmiş bu gizlilik derecelerinin kullanımına ilişkin açıklamalar yapılmıştır. Yönetmelik öncesinde özel gizlilik derecesiyle ilişkilendirilen belgelere yönelik, kamu kurum ve kuruluşları tarafından 26 Nisan 2023 tarihinde kadar yapılacak değerlendirme sonucunda özel gizlilik dereceli belgelerin gizli gizlilik derecesine yükseltilebileceği ve bu güvenlik seviyesine geçirilmeyen belgelerin ise hizmete özel gizlilik derecesine göre işleme tabi olacağı ifade edilmişltir.

4.4.9. Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik

Yönetmelik'te, resmi istatistikler kapsamında veri gizliliğine ve bu verilerin güvenliğinin sağlanmasına ilişkin usul ve esaslar belirlenmiştir. Yönetmelik çerçevesinde gizli veri tanımı yapılmıştır. Kurumlardaki yetki personel tarafından yapılan çalışmaların gizli veri ifşasına sebep olmayacak şekilde gerçekleştirilmesi, söz konusu verilerin sadece analiz amacıyla kullanılması için gerekli önemlerin alınması ve yetkili olmayan kişilerin gizli verilere erişimlerinin engellenmesi kapsamında gerekli güvenlik sistemlerinin kullanılmasına yönelik hususlar düzenlenmiştir (Resmi İstatistiklerde Veri…, 2006, mad. 7).

4.4.10. Devlet Arşiv Hizmetleri Hakkında Yönetmelik

Yönetmelik'te, belge yönetimi süreçlerin sağlanması ve arşiv hizmetlerin düzenlenmesine yönelik, kamu kurum ve kuruluşlarının faaliyetlerinde üretilen belgelerin hazırlanması, muhafaza edilmesi, güvenliğinin sağlanması ile arşiv

belgelerin belirlenmesi, korunması, bilimsel amaçlarla kullanıma açılması, yok edilmesi, devir edilmesi süreçlerine ilişkin yöntem ve esaslar belirlenmiştir. Bu bağlamda, kamu kurum ve kuruluşları fiziki belgeleri doğal afet, yangın, hayvanlarca verilebilecek zararlar gibi hasar ve kayıplara sebebiyet verecek durumlardan koruyarak belgelerin mevcut durumlarıyla özgünlüğü bozulmadan muhafaza edilmesinden, elektronik belgeleri ise fiziki zararların yanı sıra bilgisayar ve ağ altyapıları kullanılarak verilecek siber saldırı gibi tehdit unsurları ve risklerine karşı gerekli emniyet tedbirlerinin alınmasından, acil durum planlaması yapılması ve bu planın uygulanmasından sorumludurlar (Devlet Arşiv Hizmetleri…, 2019).

4.4.11. Standart Dosya Planı ile İlgili Genelge

Standart dosya planı, kamu kurum ve kuruluşların faaliyetleri ve iş süreçlerinde üretilen ya da teslim alınan belgelerin konu veya kapsam temeline göre dosyalanmasını sağlamak maksadıyla oluşturulan bir sınıflama şemasıdır (Devlet Arşiv Hizmetleri…, 2019). Kurum ve kuruluşların faaliyet ve fonksiyonlarına ilişkin kavramlar Standart Dosya Planında konu başlıkları olarak gösterilmektedir. Söz konusu başlıklar, tablo halinde ana ve alt konu başlıkları olarak oluşturulmuştur. Ana dosya konuları "000-"999" sayı aralığında, alt konu grubu 1-99 sayı aralığında kodlanmıştır. Söz konusu yüzlük ve onluk kodlandırmalar Şekil 18'de gösterilmektedir.

STANDART DOSYA PLANI						
Ana Dosya	**1. Alt Konu**	**2. Alt Konu**	**3. Alt Konu**	**GENEL İŞLER**	**Saklama Süresi**	**Saklama Kodu**
000				***Genel***		
010				***Mevzuat İşleri***		
	01			Kanunlar		
	02			Tüzükler		
	03			Yönetmelikler		
	04			Yönergeler		
	05			Tebliğler		
	06			Genelgeler		
		01		*İç Genelgeler*		
		02		*Dış Genelgeler*		

Şekil 18. Standart Dosya Planı (Devlet Arşivleri Başkanlığı, 2023)

Standart Dosya Planı üç kısım oluşmaktadır. Tüm birimlerde bulunması muhtemel dosyalar için 000-099, ana hizmet birimlerinin faaliyetleri kapsamına giren dosyalar 100-599 ve yardımcı hizmet, danışma ve denetim birimlerinin faaliyetleri kapsamına giren dosyalar için 600-999 sayısal aralığı kullanılmaktadır. Planın birinci ve ikinci kısımları kurumların tavsiyeleri esas alınarak Devlet Arşivleri Başkanlığı tarafından oluşturulmuştur. Her kurumun kendine özgü fonksiyonu bulunmakta birlikte, bunlar 100-599 sayısal aralığında bulunan ana hizmetler bölümünde yer almaktadır. Kurumlar yürüttükleri faaliyetlere ilişkin konu başlıklarını 100-599 sayısal aralığında ortak alanlardan ayrı olarak oluşturmaktadırlar (Devlet Arşivleri Başkanlığı, 2023b).

Standart Saklama Planının tüm konu grupları kendisiyle alakalı konuları kapsamakta olup, bunlar kendileriyle ilgili sırayla birinci, ikinci, üçüncü alt konulara bölümlendirilerek numaralandırılmaktadır. Planda bulunan konu kodu, resmi yazının sayı bölümünde birim kodunun ardından (-) işareti konularak yazılmaktadır (Külcü, 2018 s.359). Bu yazıma ilişkin örnek Şekil 19'da belirtilmektedir.

Sayı:	*56974592*	-	*805.01.02*	-	*1453*
	Birim Kodu (DETSİS)		*Konu Kodu (Dosya No)*		*Belge Kayıt No*

Şekil 19. Resmi Yazışmalarda Sayı Alanı

4.4.12. 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi

Bu genelge'de, kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin güvenlik risklerinin azaltılması, etkisizleştirilmesi ve milli güvenliği tehlikeye sokabilecek kritik veri ve bilgilerin korunması kapsamında uygulanacak tedbirler belirtilmektedir. Genelge'de tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti sağlayan işletmelerde yeni oluşturulacak bilgi sistemlerinde "Bilgi ve İletişim Güvenliği Rehberi"nde bulunan usul ve esaslara uyulmasının zorunlu olduğu ifade edilmektedir. Ayrıca, kurum ve kuruluşlar tarafından rehberin uygulanmasına yönelik denetleme süreçlerinin oluşturulacağı ve yılda en az bir defa uygulamanın denetleneceği ifade edilmektedir (Cumhurbaşkanlığı Bilgi…, 2019).

4.4.13. Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi

Yönerge'de, 5902 sayılı Savunma Sanayii Güvenliği Kanunu (2004) kapsamında faaliyet gösteren gerçek ve tüzel kişiler ile yetkili makamların ve savunma sanayiinde çalışanların yetki ve yükümlülükleri belirtilmiştir. Yönerge'de, antlaşmalar çerçevesinde savunma sanayiinin süreçlerinde yapılan yer alan gerçek ve tüzel kişilerce yerine getirilen faaliyetlerinin güvenliğine yönelik hangi gizlilik derecelerinin kullanılacağı belirlenmiştir. Yönerge'de bilgi, belge ve malzemeye yönelik yetkisiz erişimin engellenmesi kapsamında yerine getirilecek güvenlik tedbirleri, proje uygulamaları, ilgili işletmelerin kuruluş izni işlemleri, "Tesis Güvenlik Belgesi" ve "Kişi Güvenlik Belgesi"nin verilmesi ve iptaline ilişkin esaslar, kontrole tabi malzemelerinin üretimi, ithali ve ihracına yönelik işlemler ve ziyaretlere ilişkin düzenlemeler yapılmıştır (Milli Savunma Bakanlığı…, 2023).

5. BÖLÜM

KAMU KURUMLARINDA GİZLİLİK DERECELİ BELGELERİN YÖNETİMİ

Kamu kurumları tarafından oluşturulan veya sağlanan veri, bilgi ve belgeler iş süreçlerinde kullanılmakta, iletilmekte, muhafaza edilmekte ve bunların güvenliği sağlanmaktadır. Bu veri, bilgi ve belgeler gerçek veya tüzel kişilerin bilgi edinme talepleri talepleri olmaksızın kurum ve kuruluşların internet sayfalarında ya da bu amaçla oluşturulmuş internet tabanlı platformlarda (data.gov., data.gov.uk., veri.gov.tr vb.) paylaşılabilmektedir. Açık devlet hareketi olan bu süreçler temelde kamu kurumlarının bilgilendirme görevi ve bilgi edinme hakkı kapsamında oluşturulan yasal düzenlemelerle desteklenmektedir. Kamu kurumları iş süreçleri ve hizmetlerini yürürlükte bulunan kanun, yönetmelik, yönerge ve ilgili mevzuata göre yerine getirmekle birlikte, kurumsal paydaşların veri, bilgi ve belge taleplerini resmi kanallar ile kabul etmekte ve yine bu kanallar ile paylaşım yapmaktadırlar.

Kurumlarda bulunan veri, bilgi ve belgelere iki ana yolla erişilebilmektedir. Bu yollardan birincisi kamuya açık olan veri, bilgi ve belgelerin talep üzerine paylaşılmasıdır. Reaktif açıklama olarak da bilinen bu paylaşım, vatandaşların veya kuruluşların kendi başlarına sahip olamayacakları veri, bilgi ve belgeleri ilgili kurum ve kuruluşlarına yaptıkları talep sonucunda elde etmesidir (Fox, 2007, s. 665). İkinci yaklaşım ise herhangi bir bilgi talebi olmaksızın kurum ve kuruluşlar tarafından veri, bilgi ve belgelerin yayınlanmasıdır. Proaktif açıklama olarak da bilinen bu paylaşımla, toplum, kendisini ilgilendiren ve etkileyen karar ve kanunlar hakkında bilgilendirilmektedir (Darbishire, 2010, s. 3). Bu bağlamda, kurum ve kuruluşlar tarafından yayın, resmi gazete vb. yollarla yapılan paylaşım sonucunda topluma bilgi verme görevi yerine getirilmekte ve proaktif şeffaflık sağlanmaktadır.

Kamu kurum ve kuruluşlarında, yetkisiz olarak paylaşılması halinde kişisel, kurumsal, ulusal ve uluslararası menfaatlerin zarar görmesine sebep olabilecek veri, bilgi ve belgeler (kişisel ve hassas veriler, fikri mülkiyet kapsamındaki veri ve bilgiler, ekonomik değeri olan veri ve bilgiler, özel korumayı gerektiren gizlilik dereceli veri, bilgi ve

belgeler) bulunmaktadır. Bu bağlamda, ulusal güvenliğin sağlanması ile menfaatlerin korunması maksadıyla veri, bilgi ve belgelere yönelik erişim sınırlamaları yapılmaktadır.

Bilgi ve belge süreçlerinin e-devlet modeli kapsamında elektronik olarak sürdürülmesi, bu bilgi ve belgelerin doğrudan ve geniş ölçekli olarak paylaşılmasını sağlanmaktadır. Elektronik ortamda bulunan belgelere kolay bir şekilde erişilebilmesi gizlilik ve endişelerini artırmaktadır. Bu bağlamda, belgelerin gizliğinin ve güvenliğinin sağlanmasına ilişkin yasal ve teknik zeminde düzenlemeler ve uygulamalar geliştirilmiştir. Özel güvenlik gerektiren belgelerin yönetimine yönelik yapılan düzenlemeler ile geliştirilen uygulamalar kapsamında belgelere yönelik gizlilik sınıflandırılmalarının yapılarak gerekli güvenlik önlemleri alınmakta, gizlilik sınıflandırılması yapılmayan belgelere yönelik ise bilmesi gereken prensibi uygulanarak yetkisiz erişimler engellenmektedir (Diri ve Gülçiçek, 2012, s 499; Gizlilik Dereceli Belgelerde…, 2022, mad. 31).

Belgelerin gizlilik esaslarıyla yönetilmesine ilişkin yasal düzenlemelerin yürürlüğe girmesi ve bunların sürekli olarak revize edilmesiyle birlikte gizlilik dereceli belgelerin sistemli bir şekilde yönetilmesi zorunlu hale gelmiştir. Gizlilik dereceli belge yönetim sistemi, devlet sırrı ve/veya gizli olarak nitelendirilen belgelerin tespit edilmesini, sınıflandırılmasını, belge yönetim süreçlerinin ilgili gizlilik derecesine göre yürütülmesini, erişim düzenlemelerin oluşturulması ile gerekli güvenlik tedbirlerinin alınmasını sağlayan, gizlilik niteliğini kaybeden belgelerin gizlilik dereceli belge yönetimi kapsamından çıkarılmasını sağlayan özel bir belge yönetim sistemidir.

5.1. AMERİKA BİRLEŞİK DEVLETLERİNDE (ABD) GİZLİLİK DERECELİ BİLGİ VE BELGE YÖNETİMİ

Amerika Birleşik Devletleri (ABD), kamu kurumları ve kuruluşlar tarafından üretilen, toplanan ve muhafaza edilen bilgilerin gizlilik dereceleriyle sınıflandırılması ve yönetilmesi hususunda uzun bir geçmişe sahiptir. ABD'de bağımsızlık öncesi dönemde, özel bir yasal yetki olmaksızın uzun süren kongre döneminin ardından, gizli belgeler üretilmiş ve bunlara yönelik erişim kısıtlaması uygulamıştır. ABD Anayasasının yürürlüğe girmesiyle belgelerin gizliliğine yönelik yasal zemin oluşmuştur. ABD Birinci Dünya Savaşına dahil olduğunda, askeri ve diplomatik ilişkiler kapsamında oluşturulan belgelerde büyük artış meydana gelmiş ve gizli belge yönetim sistemi şekillenmeye

başlamıştır. ABD gizli belge yönetim sistemi İkinci Dünya Savaşı döneminde gelişim göstermeye başlamıştır (Lee, 2010, s. 259).

ABD'de gizlilik dereceli belgelerin yönetimine yönelik özel bir yasal mevzuat bulunmamaktadır. ABD, genellikle ABD Başkanlarının yürütme emirleriyle şekillenen gizlilik dereceli belge yönetim sistemine sahip olan bir ülkedir (Kim, 2019, s. 164; Kosar, 2011, s. 3). ABD Başkanlarının yürütme emirleri, yasal mevzuatın aksine, ABD Başkanının imzası ile yürürlüğe girmekte ve bir sonraki Başkan bir emir yayınlayana kadar uygulanabilir olmaktadır (Lee, 2010, s. 262). Söz konusu direktifler tipik olarak; bilgilerin kimler tarafından sınıflandırılabileceği, hangi sınıflandırma seviyelerinin ve sınıflandırma düzeylerinin (Çok Gizli, Gizli, Özel) kullanılabileceği, gizlilik dereceli bilgi ve belgelere kimlerin erişebileceği ve gizliliğinin nasıl ve ne zaman kaldırılacağına yöneliktir (Kosar, 2011, s. 4).

ABD'de gizli bilgi politikasına yönelik ABD Başkanı Barack OBAMA'nın 29 Aralık 2009 tarihli ve 13526 Sayılı Yürütme Emri ile ulusal güvenliğine ilişkin bilgi ve belgelerin sınıflandırılması, korunması ve gizliliğin kaldırılmasına ilişkin tek bir sistem öngörülmüş ve ABD Başkanı William J. Clinton'ın 17 Nisan 1995 tarihi ve 12958 sayılı "Sınıflandırılmış Ulusal Güvenlik Bilgileri (Classified National Security Information)" başlıklı yürütme emri yürürlükten kaldırılmıştır (ABD Başkanı 13526…, 2009). Söz konusu politika; sınıflandırma düzeyleri, sınıflandırılabilecek bilgi türleri, sınıflandırma ve sınıflandırma seviyelerindeki zorluklar, sınıflandırmaya yetkili kişiler, sınıflandırma süresi, sınıflandırmanın kaldırılması, sınıflandırılmış bilginin güvenliğinin sağlanması bileşenlerinden oluşmaktadır (Konsar, 2010).

Çalışmanın bu bölümünde, ABD'nin gizlilik dereceli bilgi ve belge yönetimine yönelik mevcut politikalarının belirlendiği 13526 Sayılı Yürütme Emri odağında söz konusu politikanın bileşenleri ile gizlilik dereceli bilgi ve belgelerin yönetimi kapsamında oluşturulan birimler ve kurullar incelenecektir.

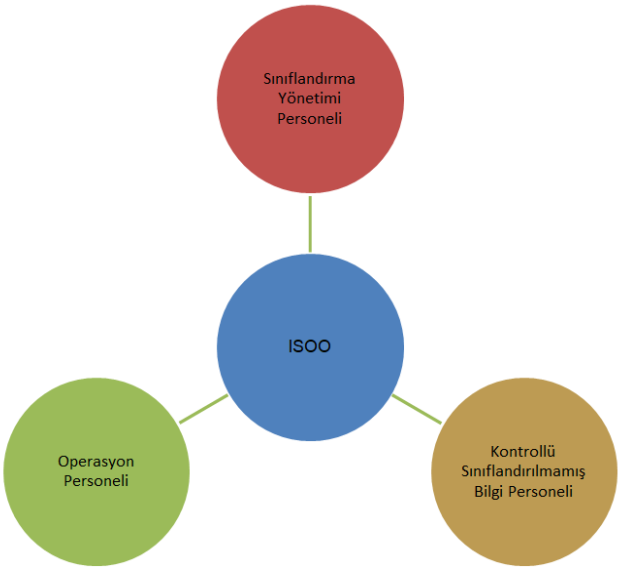
5.1.1. ABD'de Gizlilik Dereceli Bilgi ve Belge Yönetim Organizasyonu

ABD'de yetkili kamu kurum ve kuruluşları, bilgi ve belgeleri gizlilik politikasına uygun olarak sınıflandırmakla, bu bilgileri güvence altına almakla ve personelini bu bilgilerin doğru kullanımı konusunda eğitmekle yükümlüdürler. Söz konusu kurumların gizlilik

politikasına uygunluğu kendilerinin genel müfettişleri tarafından değerlendirilmektedir. Ayrıca, ABD'de gizlilik dereceli bilgi ve belgelerin yönetimi kapsamında dört birim oluşturulmuştur. Gizlilik politikası sorumlulukları verilen bu birimler "Bilgi Güvenliği Gözetim Ofisi (the Information Security Oversight Office (ISOO))", "Kurumlar Arası Güvenlik Sınıflandırması İtiraz Heyeti (the Interagency Security Classification Appeals Panel (ISCAP))", "Ulusal Gizliliği Kaldırma Merkezi (the National Declassification Center (NDC))" ve "Kamu Yararı Gizliliği Kaldırma Kurulu (the Public Interest Declassification Board (PIDB))"dur (Kosar, 2011, s. 7).

5.1.1.1. Bilgi Güvenliği Gözetim Ofisi (Information Security Oversight Office (ISOO))

ISOO, ABD Başkanı Jimmy Carter'ın 1 Aralık 1978 tarihi ve 12065 sayılı "Ulusal Güvenlik Bilgileri (National Security Information)" başlıklı yürütme emrine istinaden kurulmuştur. ISOO, 1972 yılında yayınlanan ABD Başkanı Richard Nixon'ın 11652 sayılı yürütme emri ile oluşturulan Kurumlar Arası Sınıflandırma İnceleme Komitesinin (Interagency Classification Review Committee) yerini almıştır (ISOO, 2023a). ISOO, NARA bünyesinde bulunmakla birlikte, politika ve program rehberliğini Ulusal Güvenlik Konseyi'nden almaktadır (ISOO, 2022). ISOO, güvenlik sınıflandırma sistemi ve Ulusal Endüstriyel Güvenlik Programı'nın politika ve gözetiminden ABD Başkanı'na karşı sorumludur. NARA'nın bünyesinde bulunan ve denetleme yetkisine sahip bağımsız bir kuruluş olan ISOO'nun bileşenleri Şekil 20'de gösterilmiştir.



Şekil 20. ISOO Bileşenleri (ISOO, 2023b).

Sınıflandırma yönetimi personeli, kamu kurum ve kuruluşları ile endüstride üretilen ulusal güvenlikle ilgili bilgi ve belgelerin sınıflandırılması, sınıflandırılmasının sonlandırılması ve korunmasına yönelik güvenlik politikaları geliştirmektedir. Operasyon personeli, ulusal güvenlik çıkarlarının korunmasına yönelik çok önemli bilgi ve belgeleri korumak maksadıyla kamu kurum ve kuruluşları ile endüstri tarafından oluşturulan güvenlik sınıflandırma prosedürlerinin etkinliğini değerlendirmektedir. Kontrollü sınıflandırılmamış bilgi personeli ise hassas bilgilerin uygun şekilde korunmasına yönelik standartlaştırılmış politika ve yönergeleri geliştirmektedir (ISOO, 2023b).

ISOO'nun misyonu, ulusun ve toplumun menfaatlerini geliştirilmesi için bilgi ve belgelerin korunması ile bilgi ve belgeye uygun erişimin sağlanmasını temin ederek ABD Başkanı'nı desteklemektir. Bu bağlamda ISOO, rehberlik, gözetim, raporlama ve politika geliştirme yoluyla sınıflandırılmış (gizlilik dereceli) ve kontrollü sınıflandırılmamış (gizlilik derecesi olmayan) bilgi ve belgelerin yönetimine ilişkin değerlendirmeleri yerine getirmektedir (ISOO, 2022). ISOO'nun görev fonksiyonları şu şekildedir (ISOO, 2023b):

- Sınıflandırılmış Ulusal Güvenlik Bilgileri hakkındaki 13526 sayılı icra emri ve Ulusal Endüstri Güvenlik Programı hakkındaki 12829 sayılı icra emrine yönelik uygulama talimat ve direktiflerinin koordine edilmesini, geliştirilmesini ve yayınlanmasını sağlamak.
- Kamu kurum ve kuruluşları tarafından oluşturulan uygulama yönetmeliklerini gözden geçirmek ve onaylamak.
- Kamu kurum ve kuruluşlarının gizlilik dereceli bilgi ve belge yönetiminin icra emirlerine göre uygunluğuna yönelik denetimler gerçekleştirmek.
- Kamu kurum ve kuruluşlarının güvenlik eğitim ve öğretim programlarını izlemek. Güvenlik eğitimlerine yönelik materyal geliştirmek ve bunları yayımlamak.
- Sınıflandırılmış Ulusal Güvenlik Bilgileri ve Ulusal Endüstri Güvenlik Programı kapsamındaki icra emirlerinin uygulanmasına yönelik kamu kurum ve kuruluşları veya kişiler tarafından gelen şikayet, öneri ve itirazlar hakkında işlem yapmak.

- Her yıl, kamu kurum ve kuruluşların sınıflandırma programı ve faaliyetlerine yönelik maliyet tahminlerine ilişkin istatistiksel verileri toplayarak bunları analiz etmek ve bunları ABD Başkanı'na bildirmek.
- ISOO Direktörü, güvenlik sınıflandırma programıyla alakalı hususlarda Kongre, medya, meslek örgütleri, özel ilgi grupları ve kamuoyuna karşı hükümetin sözcüsü olarak görev yapmak.
- Tespit edilen veya olması muhtemel sorunlar hakkında çalışmalar gerçekleştirmek ve programın iyileştirilmesine yönelik düzeltici yaklaşımlar geliştirmek. Sınıflandırılmış bilgi ve belge yönetimi programının yeknesak bir şekilde uygulanmasını sağlamak ve maliyetleri azaltmak için standartlaştırılmış güvenlik formları geliştirmek ve bunları yayınlamak.
- Ulusal Güvenlik Konseyi aracılığıyla ABD Başkanı'na politika tavsiyesinde bulunmak. Güvenlik sınıflandırma programına yönelik konuları görüşmek maksadıyla toplantılar düzenlemek ve bu toplantılara başkanlık etmek.

5.1.1.2. Kurumlar Arası Güvenlik Sınıflandırması İtiraz Heyeti (Interagency Security Classification Appeals Panel (ISCAP))

ISCAP, ABD Başkanı William J. Clinton'ın 17 Nisan 1995 tarihi ve 12958 sayılı "Sınıflandırılmış Ulusal Güvenlik Bilgileri (Classified National Security Information)" başlıklı yürütme emrine istinaden oluşturulmuştur (ABD Başkanı 12958 …, 1995; ISCAP, 2023). ABD Başkanı Barack OBAMA'nın 29 Aralık 2009 tarihli ve 13526 Sayılı Yürütme Emriyle ISCAP'ın rolüne küçük eklemeler yapılmakla birlikte, ISCAP'ın üyelik ve görevleri büyük ölçüde değişmemiştir (Kosar, 2011, s. 8).

Ulusal güvenlik gerektiren bilgi ve belgelerinin sınıflandırılmasını ve gizliliğin kaldırılmasını gözden geçirmekten sorumlu kurumlar arası bir kurul olan ISCAP, Ulusal İstihbarat Direktörü Ofisi, Dışişleri Bakanlığı, Savunma Bakanlığı, Ulusal Arşivler, Adalet Bakanlığı ve Ulusal Güvenlik Danışmanı tarafından atanan üst düzey temsilcilerden oluşmaktadır. Ayrıca, Merkezi İstihbarat Teşkilatı Direktörü, Merkezi İstihbarat Teşkilatı kaynaklı gizlilik dereceli bilgi ve belgeler kapsamında ISCAP'ın tüm müzakerelerine ve alakalı destek faaliyetlerinde oy hakkı bulunan bir üye olarak katılmak üzere geçici bir temsilci atayabilmektedir. ISCAP Başkanı ABD Başkanı tarafından kurul üyeleri arasından belirlemektedir. ISOO Direktörü ISCAP'ın İcra

Sekreteri olarak görev yapmakla olup, ISOO personeli ISCAP için program ve idari destek sağlamaktadır (ISCAP, 2023).

ISCAP, kamuoyuna ve sınıflandırma sistemin kullanıcılarına sınıflandırma kararlarının daha fazla incelenmesi için bir platform sunmaktadır. ISCAP'ın 13526 sayılı yürütme emrine (mad. 5.3) istinaden getirmesi gereken işlevler şunlardır (ABD Başkanı 13526 …, 2009; ISCAP, 2023; ISCAP Tüzüğü, Kuralları…, 2012):

- 13526 Sayılı Yürütme Emrinin 1.8'inci bölümü kapsamında sınıflandırma itirazında bulunan yetkili kişilerin itirazları hakkında karar vermek.
- Otomatik sınıflandırmaya ilişkin muafiyetlerin onaylanması, reddedilmesi veya değiştirilmesi ile belirlenmiş olan bir dosya serisinin 25 yıl süresince otomatik sınıflandırmadan muaf tutulmasına yönelik kamu kurum ve kuruluşların talepleri hakkında karar vermek.
- 13526 Sayılı Yürütme Emrinin 3.5'inci bölümü kapsamında zorunlu gizlilik kaldırma incelemesi için talepte bulunan kurum, kuruluş ve kişilerin itirazları hakkında karar vermek.
- 13526 Sayılı Yürütme Emrinin 1.8'inci ve 3.5'inci bölümleri kapsamındaki itirazlara yönelik kesinleşmiş heyet kararlarını üst düzey kurum yetkililerine ve kamuoyuna uygun şekilde açıklamak.

5.1.1.3. Ulusal Sınıflandırmayı Kaldırma Merkezi (the National Declassification Center (NDC))

NDC, ABD Başkanı Barack OBAMA'nın 29 Aralık 2009 tarihli ve 13526 Sayılı Yürütme Emrine istinaden NARA'nın bünyesinde kurulmuştur. NDC'nin kurulma amaçları; gizlilik kaldırma süreçlerini düzene sokmak, kalite güvence önlemlerini kolaylaştırılmak ve kalıcı tarihi değere sahip olduğu tespit edilen belgelere ait gizliliğinin kaldırılmasına ilişkin standartlaştırılmış eğitim uygulamaktır (NDC, 2023). NDC, kurumlar tarafından NARA'ya teslim edilen ancak henüz gizliliği kaldırılmak üzere tam olarak incelenmemiş olan önemli miktardaki sınıflandırılmış belge birikiminin azılmasına yönelik bir araç olarak tasarlanmıştır (Konsar, 2010, s. 15). 13526 Sayılı Yürütme Emri kapsamında NDC tarafından koordine edilecek hususlar şunlardır (ABD Başkanı 13526 Sayılı Yürütme Emri, 2009, mad. 3.7. (b); NDC, 2023):

- Kurum ve kuruluşlarda bulunan belgeler ve transfer edilen Başkanlık belgelerine yönelik kurumlar arası sevk işlemlerinin zamanında ve uygun bir biçimde yürütülmesini,
- 13526 Sayılı Yürütme Emrinin 3.3 (otomatik sınıflandırma kaldırma faaliyetleri) ve 3.4 (sistematik sınıflandırma kaldırma incelemesi) bölümlerinde belirtilen hususlar kapsamında kurumlar arası sınıflandırma kaldırma faaliyetlerin yürütülmesini,
- Ayrıntılı sınıflandırma kaldırma rehberliğinin kurumlar arasında alışverişini,
- İşlevsel, açık ve standart sınıflandırma kaldırma iş süreçleri, eğitim ve kalite güvence tedbirlerinin geliştirilmesini,
- Elektronik veri, bilgi ve belgeler, özel medya ve güncel teknolojilerin neden olduğu sınıflandırma kaldırma problemlerine çözümlerin geliştirilmesi,
- Kurumların veri tabanlarının birbirine bağlanması, bu veri tabanlarının etkin kullanımı ve NDC'nin yetkisi altındaki sınıflandırma kaldırma faaliyetlerini desteklemek için yeni teknolojilerin kullanılmasını sağlamaktır.

5.1.1.4. Kamu Yararı Gizliliği Kaldırma Kurulu (the Public Interest Declassification Board (PIDB))

PIDB, 27 Aralık 2000 tarihinde ABD Kongresi tarafından kurulmuş bir danışma kuruludur (Kosar, 2011, s. 8). PIDB, önemli ABD ulusal güvenlik kararları ve faaliyetlerine ilişkin kapsamlı, doğru ve güvenilir bir belgesel kaydına yönelik kamu erişiminin en geniş şekilde olabilmesini teşvik etmekle yetkilidir. ISOO Direktörü, PIDB'nin Yönetici Sekreteri olarak görev yapmaktadır (PIDB, 2023).

PIDB, ABD Başkanı ile diğer kamu kurum ve kuruluşların yetkililerine, sınıflandırılması kaldırılmış belgelerin ve arşiv değeri olan materyallerin belirlenmesi, toplanması, sınıflandırılmanın kaldırılması için gözden geçirilmesi ve yayınlanması konusunda tavsiyelerde bulunmaktadır. Bununla birlikte PIDB, ABD Başkanı'nın ulusal güvenlik ile ilgili bilgi ve belgelere yönelik sınıflandırılma ve sınıflandırılmanın kaldırılmasına yönelik yürütme emirleri yayınlamasından kaynaklanan politikalar hakkında ABD Başkan'ı ile diğer kamu kurum ve kuruluşların yetkililerine tavsiyelerde bulunmaktadır (PIDB, 2023).

PIDB'nin bir belgeye ait sınıflandırılmanın tamamen veya kısmi olarak kaldırılması yönündeki tavsiyesi, belgeyi ilk olarak sınıflandıran makamın görüşleri dikkate alınarak ve sınıflandırılmanın kaldırılmasının kamu yararına olduğuna kanaat getirildiğinde verilmektedir. Sınıflandırılmanın tamamen veya kısmı olarak kaldırılmasına yönelik tavsiye kararı PIDB'nin mevcut üyelerinin oy çoğunluğuyla verilmektedir (PIDB Yönetmeliği, 2020, mad. 8).

5.1.2. Sınıflandırma Düzeyleri

Bilgi ve belgelerin sınıflandırılmasına yönelik gizlilik düzeylerinin belirlenmesi gizlilik dereceli bilgi ve belge yönetim sisteminin temelini oluşturmaktadır. Gizlilik düzeyleri, sınıflandırma standartlarına göre belirlenmektedir. Bu bağlamda, 13526 sayılı ABD Başkanı Yürütme Emrinde çok gizli, gizli ve özel olmak üzere üçlü sınıflandırma düzeyi belirlenmiş olup, bunlar şu şekildedir (ABD Başkanı 13526 Sayılı Yürütme Emri, 2009, mad. 1.2 (a)):

- Çok Gizli: Yetkisiz olarak açıklanması halinde, ulusal güvenliğe son derece önemli (sınıflandırmayı yapmaya yetkili kişi ve kurumlarca tespit edilebilen veya tanımlanabilen) bir zarar verebilecek olan bilgi ve belgelere yönelik kullanılmaktadır.
- Gizli: Yetkisiz olarak açıklanması halinde, ulusal güvenliğe önemli (sınıflandırmayı yapmaya yetkili kişi ve kurumlarca tespit edilebilen veya tanımlanabilen) bir zarar verebilecek olan bilgi ve belgelere yönelik kullanılmaktadır.
- Özel: Yetkisiz olarak açıklanması halinde, ulusal güvenliğe (sınıflandırmayı yapmaya yetkili kişi ve kurumlarca tespit edilebilen veya tanımlanabilen) bir zarar verebilecek olan bilgi ve belgelere yönelik kullanılmaktadır.

5.1.3. Sınıflandırılabilecek Bilgi Türleri

ABD'de bilgi ve belgelerin sınıflandırılmasına ilişkin konular açık bir şekilde sıralanmış ve bu konuları kapsamayan bilgi ve belgelerin sınıflandırmayacağı belirtilmiştir. Sınıflandırmaya tabi olacak konular şunlardır (ABD Başkanı 13526 Sayılı Yürütme Emri, 2009, mad. 1.4):

- Askeri planlar veya askeri operasyonlar,
- Askeri silah sistemleri,
- Yabancı devlet yönetimi bilgiler,
- Gizli eylemlerde dahil olmak üzere istihbarat faaliyetleri, istihbarat kaynakları veya yöntemleri,
- ABD'nin dış ilişkileri veya dış faaliyetleri,
- Ulusal güvenliğe ilişkin bilimsel, teknolojik veya ekonomik konular,
- Nükleer malzemelerin veya tesislerin korunması kapsamında ABD'nin programları,
- Ulusal güvenliğe ilişkin sistemlerin, tesislerin, altyapıların, projelerin, planların ya da koruma hizmetlerinin zayıflıkları veya yetenekleri,
- Kitle imha silahlarının üretilmesi, geliştirilmesi veya kullanılması.

ABD'de sınıflandırmanın yasaklanması ve sınırlandırılmasına yönelik olarak 13526 Sayılı Yürütme Emri'nde (mad. 1.7);

- Rekabeti sınırlandırmak,
- Yasa ihlallerini, verimsizliği veya idari hataları gizlemek,
- Bir kişi, kurum veya kuruluşu sıkıntıya düşürebilecek olguları önlemek,
- Milli savunma bakımından güvende olan bilgilerin paylaşılmasını engellemek veya ertelemek,

maksadıyla hiçbir bilgi ve belgenin sınıflandırılamayacağı, sınıflandırılmış olsa bile bu işleme son verileceği veya gizliliğin kaldırılamamasına yönelik teşebbüslerde bulunulmayacağı ifade edilmektedir. Bununla birlikte, açık bir şekilde milli güvenlikle ilgili olmayan temel bilimsel araştırma bilgilerinin sınıflandırılması da yasaklanmaktadır (13526 Sayılı Yürütme Emri, 2009, mad. 1.7).

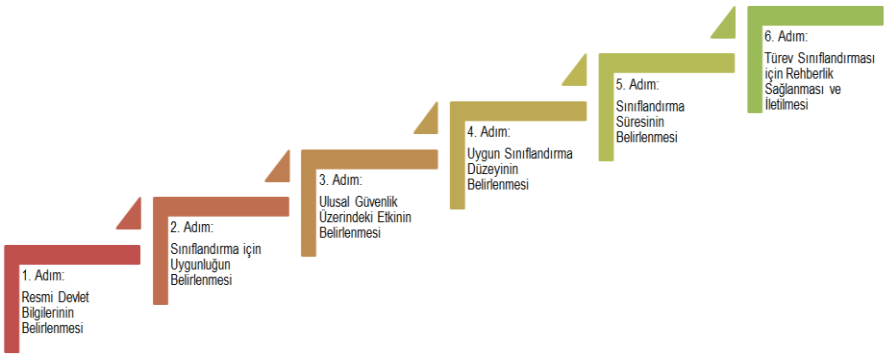
5.1.4. Sınıflandırmaya Yetkili Kişiler

ABD gizlilik dereceli bilgi ve belge yönetimi kapsamında ilk sınıflandırma (original classification) ve türev (derivative classification) sınıflandırmaya yönelik uygulamalar geliştirilmiştir. İlk sınıflandırma, ulusal güvenlik açısından bilginin korunması gerektiği tespit edilen bilgi ve belgenin yetkili kişi tarafından ilk defa sınıflandırılmasıdır. Türev sınıflandırma ise, hali hazırda sınıflandırılmış olanların birleştirilmesi, yeniden

yorumlanması, yeniden ifade edilmesi veya yeni bir biçimde üretilmesi anlamına gelmektedir (ABD Başkanı 13526…, 2009, mad. 6.1).

ABD Başkanı, ABD Başkan Yardımcısı, ABD Başkanı tarafından atanan kurum başkanları ve görevlileri bilgileri ilk defa sınıflandırmakla yetkilidir (ABD Başkanı 13526…, 2009, mad. 1.3). İlk sınıflandırma yetkisine sahip kişiler yetkisini diğer kurum yetkililerine devredebilmekte olup, böyle bir yetki devrinin ISOO Direktörüne bildirilmesi gerekmektedir (Konsar, 2010, s. 12). 13526 Sayılı Yürütme Emrine istinaden yayımlanan kılavuzda ilk sınıflandırma vermeye yetkili kurum makamları ve bunların gizlilik derecesi verme yetkileri (Çok gizli ve gizli) açık bir şekilde yayınlanmıştır (Whitehouse, 2009).

ABD Savunma Bakanlığı tarafından bilgilerin ilk defa sınıflandırılmasına yönelik altı adımlı bir sınıflandırma süreç referansı yayınlanmıştır (ABD Savunma Bakanlığı, 2019). Bir sınıflandırma düzeyi (çok gizli, gizli ve özel) ile yetkili olan kişiler, sahip oldukları sınıflandırma düzeyi ve bir alt düzey kapsamında bilgi ve belgeleri ilgili gizlilik derecesiyle ilişkilendirmeye yetkilidir. Örneğin, çok gizli gizlilik derecesi sınıflandırma düzeyine sahip bir kişi, bir bilgi ve belgeye gizli veya özel gizlilik derecesi tayin edebilmektedir. Ayrıca, kişilerin sadece sorumluluk alanlarıyla ilgili bilgi ve belgelere yönelik ilk sınıflandırma yapması gerektiği ifade edilmektedir. İlk sınıflandırmaya yönelik oluşturulan referans modelinde ifade edilen süreç adımları Şekil 21'de gösterilmiştir.



Şekil 21. ABD Savunma Bakanlığı İlk Sınıflandırma Süreç Adımları

ABD Savunma Bakanlığı tarafından yayımlanan ilk sınıflandırma süreç referansının 1'inci adımında, bilginin resmi bir bilgi olup olmadığına karar verilmektedir. Söz konusu

bilgi resmi bir bilgi değilse bir sonraki adıma geçilmemektedir. 2'nci adımda, bilginin sınıflandırmaya esas olan konular (askeri plan, istihbarat faaliyetleri vb.) kapsamında olup olmadığı ve sınıflandırılmasına ilişkin herhangi bir yasaklamanın (rekabetin engellenmesi vb.) bulunup bulunmadığı tespit edilmektedir. 3'üncü adımda, yetkisiz olarak açıklanması halinde ulusal güvenliği zarar verme potansiyeli olmayan bilgiler sınıflandırılmamaktadır. Eğer ulusal güvenliğe zarar verme potansiyeli olan ve 2'nci adımda belirtildiği gibi sınıflandırma için uygun olduğunda, bilgi ve belgeler ilgili gizlilik derecesiyle sınıflandırılmaktadır. 4'üncü adımda, bilginin hassasiyetlik ve potansiyel zararın ne olacağı belirlenerek sınıflandırmaya ilişkin etki değerlendirilmesi yapılmaktadır. Belirlenen etki düzeyine göre bilgi ve belgeler çok gizli, gizli ve özel gizlilik derecesiyle sınıflandırılmaktadır. 5'inci adımda, sınıflandırma seviyesinin düşürülmesi ve sınıflandırmanın kaldırılmasının ne zaman yapılacağı belirtilmektedir. Son olarak 6'ncı adımda ise, sınıflandırılma kararı güvenlik sınıflandırma kılavuzları veya işaretlenmiş kaynak belgeler ile bildirilmektedir. Söz konusu kararlar, türev sınıflandırılmaları kapsamında, bilgi ve belgenin yetkisiz olarak açıklanmamasını sağlamak için belgeyi elde eden kişiler tarafından kullanılmaktadır (ABD Savunma Bakanlığı, 2019).

Kosar (2010, s. 12) sınıflandırma yetkisine sahip kişilere sınıflandırma ve sınıflandırmasının kaldırılması veya düzeyinin düşürülmesi hususunda eğitim verilmesi gerektiğini ifade etmekle birlikte, söz konusu eğitimin ilk sınıflandırma yetkisine sahip kişilere her yıl ve türev sınıflandırıcılara ise iki yılda bir verilmesini tavsiye etmektedir.

5.1.5. Sınıflandırma Süresi

Sınıflandırma süresinin belirlenmesi, gizlilik sınıflandırması için zaman aşımını ifade etmekte olup, belirli zamanın sonuna gelindiğine veya bir olayın meydana gelmesi/son bulması durumunda sınıflandırılan bilgi ve belgenin paylaşılmasında gereksiz gecikmeleri önlemek amacıyla tasarlanmış bir sistemdir.

ABD'de bilgi ve belgeler sınıflandırıldığında kamuya açıklanma tarihinin belirlenmesi gerekmektedir. Bilgi ve belgelerin ilk sınıflandırılması sırasında yetkili kişi veya makamlar bilginin ulusal güvenlik hassasiyet süresine bağlı olarak sınıflandırmanın kaldırılması kapsamında bir olayın gerçekleşme veya son bulma olgularını ya da bir

tarih belirlemektedir. Belirlenen tarihe ulaşıldığında ya da olay gerçekleştiğinde/son bulduğunda, bilgi ve belgenin gizliliği otomatik olarak kaldırılmaktadır.

ABD'de sınıflandırma süresi "*gizli bir insan kaynağının kimliğini veya kitle imha silahlarının kilit tasarım konseptlerini açıkça veya kanıtlanabilir şekilde ortaya çıkarabilecek*" bilgi ve belgeler hariç, sınıflandırma süresini 10 yıl ile sınırlandırmaktadır. Söz konusu bilgi ve belgeler 25 yıl süreyle sınıflandırılmakla birlikte, 13526 Sayılı ABD Başkanı Yürütme Emrinde (mad. 3.3) belirtilen politikalara uygun olarak ilave 50 yıl kadar sınıflandırılmış olarak kalabilmektedir (ABD Başkanı 13526…, 2009, mad. 1.5)

ABD Başkanı 13526 Sayılı Yürütme Emrine (mad. 1.5 (d)) göre hiçbir bilgi ve belge süresiz olarak sınıflandırılamamaktadır. Bu bağlamda, 13526 sayılı yürütme emrinden önceki emirler kapsamında süresiz olarak sınıflandırılan bilgi ve belgeler ile eksik sınıflandırma kaldırma talimatları veya sınıflandırma kaldırma talimatından yoksun olarak sınıflandırılmış bilgi ve belgelerin gizliliği söz konusu yürütme emrinde belirtilen hususlara (mad. 3) uygun olarak kaldırılmaktadır.

5.1.6. Sınıflandırılmanın Kaldırılması

Sınıflandırılmanın kaldırılması, bilgi ve belgenin gizliliğine ilişkin yapılan sınıflandırılmanın son bularak söz konusu bilgi ve belgelerin sınıflandırılmamış hale getirilmesini ifade etmektedir. Sınıflandırmanın kaldırılma sorumluluğu genellikle bilgi ve belgeyi ilk olarak sınıflandıran kurum ve kuruluşlara veya kişilere aittir. Söz konusu kurum ve kuruluşlar veya kişiler, bilgi ve belgenin sınıflandırılmasının kaldırılıp kaldırılmayacağını, mevcut gizlilik bilgi politikasındaki bir istisna ile sınıflandırmanın kaldırılmasından muaf tutulup tutulmayacağını veya bilgi ve belgeyi saklamak isteyebilecek başka bir kuruma yönlendirilip yönlendirilmeyeceğini incelemektedir. Bu bağlamda, bilgi ve belgelerin gizliliği tamamen kaldırılabilir veya kaldırılmayabilir ya da gizlilik derecesi bir alt düzeyle ilişkilendirilebilmektedir (Konsar, 2010, s. 13).

ABD'de ulusal güvenlik kapsamında sınıflandırılmış bilgi ve belgelerin gizliliğin ortadan kaldırılmasına yönelik beş yol bulunmaktadır. Söz konusu yollar şunlardır (Konsar, 2010, s. 13)

- Bilgi ve belgenin gizliliğine yönelik yapılan sınıflandırma nedenlerinin ortadan kalması sebebiyle, ilk sınıflandırmayı yapan kurum veya kişilerin sınıflandırmayı kaldırmasıdır.
- Bir kurumun, başka bir kurum tarafından yapılan sınıflandırmaya yönelik yaptığı itiraza istinaden sınıflandırılmasının kaldırılmasıdır (daha önce ifade edildiği gibi, ISCAP söz konusu itirazları karara bağlamaktadır).
- Sınıflandırmanın otomatik olarak kaldırılması, sistematik sınıflandırma kaldırma incelemesi ve zorunlu sınıflandırma kaldırılması incelemesidir.
- Kongre tarafından, belirli bilgi ve belgelerinin gizliliğinin kaldırılmasını gerektiren bir yasaya istinaden sınıflandırılmanın kaldırılmasıdır.
- Bilgi Edinme Özgürlüğü Kanunu'na istinaden yapılan bilgi talepleri, bilgi ve belgelere yönelik yapılan gizlilik sınıflandırmasının kaldırılmasına neden olmasıdır.

5.1.6.1. Sınıflandırmanın Otomatik Olarak Kaldırılması

Sınıflandırılmanın otomatik olarak kaldırılması, ilk sınıflandırma makamınca belirlenen belirli bir tarihe gelinmesi veya bir olayın meydana gelmesi/son bulması ya da 13526 Sayılı Yürütme Emrinde ifade edilen sınıflandırma süresi için azami bir zaman dilimin sona ermesi neticesinde bilgi ve belgenin gizliliğine yönelik sınıflandırılmanın kendiliğinden ortadan kalkması durumudur (ABD Başkanı 13526…, 2009, 6.1 (e)).

Sınıflandırılmanın otomatik olarak kaldırılması kapsamında, sınıflandırılan bilgi ve belgelerin gizliliğinin kaldırılması gerekmektedir. Ancak, bu durum söz konusu bilgi ve belgelerin hemen kamuya açık hale geleceği anlamına gelmemektedir. Bununla birlikte, bir kurum ve kuruluşun üst yetkisi veya başkanı bazı durumlarda sınıflandırmanın otomatik olarak kaldırılma işleminden muaf tutulabilmektedir. Söz konu durumlar şunlardır (ABD Başkanı 13526 Sayılı Yürütme Emri, 2009, 3.3 (b)):

- Gizli bir insan kaynağına veya istihbarat yönetimine zarar verilmesi,
- Kitle imha silahlarının üretilmesine, kullanılmasına veya geliştirilmesine yardımcı olacak bilgilerin ifşa edilmesi,
- ABD kriptolojik sistemlerine veya faaliyetlerine zarar verecek bilgilerin ifşa edilmesi,

- Bir ABD silah sistemi içinde en son teknolojinin uygulanmasına zarar verecek bilgilerin ifşa edilmesi,
- Yürürlükte olan resmi olarak adlandırılmış veya numaralandırılmış ABD askeri savaş planlarının, operasyonel veya taktik unsurlarının ifşa edilmesi,
- ABD ile yabancı bir ülke arasındaki ilişkilere önemli derecede zarar verecek bilgilerin ifşa edilmesi,
- ABD Başkanı, Başkan Yardımcısı ve ulusal güvenlik yararına koruma hizmetlerine izin verilen diğer kişilerin korunması kapsamında ilgili yetkililerinin mevcut kabiliyetlerine zarar verecek bilgilerin ifşa edilmesi,
- Ulusal güvenlik acil durum hazırlık planlarına önemli zarar verecek veya ulusal güvenlikle ilgili sistemlerin, tesislerin veya altyapıların mevcut güvenlik açıklarını ortaya çıkaracak bilgilerin ifşa edilmesi,
- Bilgi ve belgelerin gizliliğinin 25 yıl sonra otomatik veya tek taraflı olarak kaldırılmasına izin vermeyen bir yasanın, anlaşmanın veya uluslararası anlaşmanın ihlal edilmesidir.

5.1.6.2. Sınıflandırılmanın Sistematik Olarak Kaldırılması

Sınıflandırılmış bilgi ve belgelerinin otomatik sınıflandırma kaldırma sürecinden muaf tutulmasını isteyen bir kurum, ayrıntılı olarak hazırladığı talebini ISOO Direktörüne sunması gerekmektedir. ISCAP bahse konu talep hakkında karar verici merciidir. ISCAP tarafından talep onaylanırsa, söz konusu bilgiler sistematik olarak sınıflandırmanın kaldırılması incelemesine tabi olacaktır. Bu süreç sonunda ISCAP tarafından talep onaylanırsa, bilgi ve belgeler 50 yıla kadar daha sınıflandırılmış olarak gizli kalacak ve bu sürenin sonunda, talep eden kurum başka bir muafiyet talep etmedikçe otomatik olarak gizliliği kaldırılacaktır (Konsar, 2010, s. 14).

ISCAP, talep eden kurumuna bilgi ve belgelerin otomatik olarak sınıflandırma kaldırılmasından muaf tutulmaması veya tavsiye edilenden daha erken bir tarihte gizliliğinin kaldırılması yönünde talimat verebilir. Bu durumda, ilgili kurumun üst yöneticisi veya başkanı böyle bir karara Güvenlik Danışmanı aracılığıyla ABD Başkan'ına itiraz edebilir. Söz konusu itiraz sonuçlanıncaya kadar söz konusu bilgi ve belgelerin gizlilik dereceleri mevcut durumunu korumaktadır (ABD Başkanı 13526…, 2009, 3.3 (j)).

5.1.6.3. Zorunlu Sınıflandırma Kaldırma İncelemesi

Zorunlu gizlilik kaldırma incelemesi, 13526 Sayılı Yürütme Emrinin 3.5'inci bölümü kapsamındaki gereklilikleri karşılayan bir gizlilik kaldırma talebine yanıt olarak, sınıflandırılmış bilgi ve belgelerin gizliliklerinin kaldırılması için yapılan incelemedir. Zorunlu sınıflandırma kaldırma incelemesi, yaşı veya kökeni/ırkı ne olursa olsun herhangi bir kişi veya kuruluşun, belirli istisnalar dışında, herhangi bir kamu kurumu ve kuruluşundan sınıflandırılmış bilgi ve belgenin gizliliğinin kaldırılması için bu bilgilerin gözden geçirilmesini talep edebileceği bir yoldur (ISOO, 2023c). Söz konusu istisnalar, ABD Başkanı veya Başkan Yardımcısı ve onlarla birlikte çalışan bazı kişiler tarafından oluşturulan bilgiler ve yayın öncesi inceleme için sunulması gereken belgeler (örneğin istihbarat ajanlarının anıları) gibi belirli bilgi ve belge türlerini kapsamaktadır (ABD Başkanı 13526…, 2009, mad. 3.5).

Zorunlu gizlilik kaldırma incelemesine ilişkin bir talep, bilgiyi içeren belgeyi veya materyali, kurumun makul bir çaba ile bulmasını sağlayacak yeterli özgünlükte tanımlanmalıdır. Bu talebe yönelik, ilk sınıflandırmayı yapan kurum veya kişi tarafından, bir gizlilik derecesiyle sınıflandırılmış bilgi ve belgenin ilgili gizlilik düzeyinde (çok gizli, gizli ve özel) belirtilen standartları karşılayıp karşılamadığı değerlendirilmektedir. Bu değerlendirme sonucunda, sınıflandırma standartlarını sağlamayan bilgi ve belgelerin sınıflandırması ilgili kurum tarafından kaldırılmaktadır (ABD Başkanı 13526…, 2009, mad. 3.5).

5.1.7. Sınıflandırılmış Bilginin Güvenliğinin Sağlanması

Sınıflandırılmış bilgi ve belgeleri üreten ve kullanan kurumlar, söz konu bilgi ve belgeleri korumakla yükümlüdürler. Bu bağlamda, 13526 Sayılı Yürütme Emri'nde kamu çalışanları ve diğer kişilerin sınıflandırılmış bilgi ve belgelere erişimine ilişkin temel standartlar belirlenmiştir. Bir kişinin sınıflandırılmış bilgilere erişebilmesi için sağlaması gereken koşullar şunlardır (ABD Başkanı 13526…, 2009, mad. 4):

- Sınıflandırılmış bilgi ve belgeye erişim için uygunluğun bir kurum başkanı veya kurum başkanının görevlendirdiği kişi tarafından olumlu bir şekilde belirlenmesi,
- Kişinin onaylanmış bir gizlilik sözleşmesi imzalaması,

- Kişinin yürüttüğü görev ve faaliyetler kapsamında sınıflandırılmış bilgi ve belgeye ihtiyacı olmasıdır.

Yukarıda belirtilen gereklilikleri sağlayan kişilerin, sınıflandırılmış bilgi ve belgelerin uygun şekilde korunması ve sınıflandırılmış bilgi ve belgelerin yetkisiz olarak ifşa edilmesine sebebiyet veren kişilere verilebilecek cezai, hukuki ve idari yaptırımlar hakkında eğitim alması gerekmektedir.

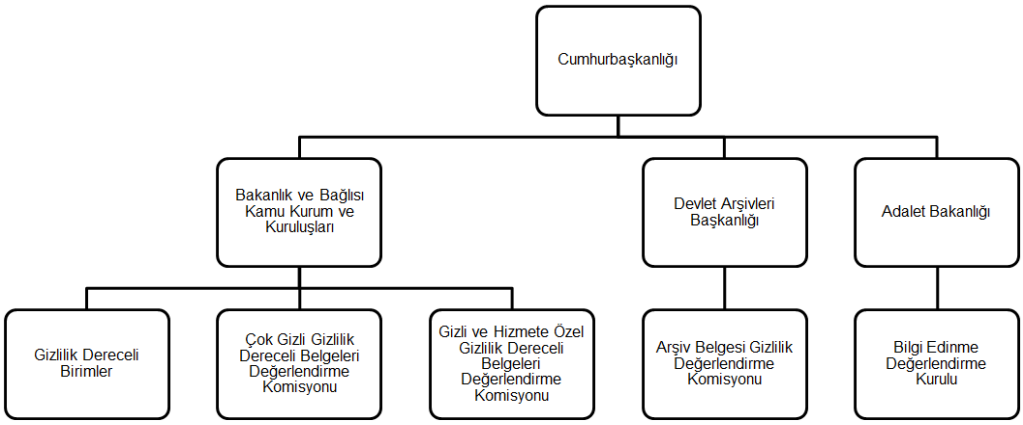
5.2. TÜRKİYE'DE GİZLİLİK DERECELİ BELGELERİN YÖNETİMİ

Kamu kurum ve kuruluşlarına ait bilgi ve belgeler e-devlet modeli kapsamında elektronik ortamlarda varlık bulmaktadırlar. Bilgi ve belgelerin elektronik ortamlarda bulunması doğrudan ve geniş ölçekli olarak paylaşılmasının getirdiği kolaylık ve yararlar ile birlikte, ulusal güvenliğin ve kişilerin mahremiyetinin korunması konusunda endişe kaynağı olmaktadır. Bu sebeple, kişisel, hassas ve önemli bilgileri içeren belgelerin normal belgelerden farklı işleme tabi tutulması gerekmektedir (Odabaş, 2008, s.126). Bu kapsamda, Türkiye'de birçok yasal ve idari düzenleme yapılmış, standartlar kabul edilmiş ve yapılar oluşturulmuştur. Yapılan düzenleme ve geliştirilen uygulamalarda, belgelerin gizliğine yönelik alınacak özel güvenlik önlemleri kapsamında gizlilik sınıflandırılması yapılmaktadır (Diri ve Gülçiçek, 2012, s 499). Gizlilik sınıflandırılması yapılmayan fakat özel güvenlik gerektiren belgelere yönelik bilmesi gereken prensibi uygulanmakta olup, bu belgelerin paylaşımı ise Bilgi Edinme Hakkı Kanunu (2003) kapsamında yapılacak talebin incelenmesi sonucunda yapılmaktadır (Gizlilik Dereceli Belgelerde…, 2022, mad. 31).

Gizlilik dereceli belgelerin yönetimi, yasal mevzuatın gereği olarak taşıdıkları gizlilik derecesine göre fiziksel ya da elektronik olarak ve farklı güvenlik esaslarına göre yönetilmektedir. Hizmete özel gizlilik dereceli belgelerin yönetimi olağanüstü durumlar haricinde sadece elektronik ortamda (EBYS), gizli gizlilik dereceli belgelerin yönetimi gerekli güvenlik önlemleri alınan fiziki ortamlarda ve çok gizli gizlilik dereceli belgelerin yönetimi ise bu amaçla özel olarak oluşturulmuş Çok Gizli Belge Bürosu koordinatörlüğünde yapılmaktadır (Elektronik İmza Kanunu, 2004; Gizlilik Dereceli Belgelerde…, 2022; Resmi Yazışmalarda… Yönetmelik, 2020). Bu sebeple kurum ve kuruluşlarda, gizlilik dereceli belgelerin yönetimi için farklı düzeylerde yapıların oluşturulması gerekmektedir.

5.2.1. Türkiye'de Gizlilik Dereceli Belge Yönetimi İle İlişkili Yapılar

Türkiye'de gizli/sır niteliğinde olan belgelerin yönetimi kapsamında, gizlilik derecesinin belirlenmesi ve belgelerin yaşam döngüsü boyunca ilgili gizlilik derecesine göre gerekli işlemlerin yapılması ve önlemlerin alınması belgeyi üreten veya belgeye sahip olan kurum ve kuruluşlar tarafından yerine getirilmektedir. Gizlilik dereceli belgelerin yönetimi ile bu belgelerin gizlilik derecesinin değerlendirilmesi, gizlilik derecesinin düşürülmesi/kaldırılması ile imha edilmesi veya bilgi talebi itirazları kapsamında oluşturulan yapılar Şekil 22'de gösterilmiştir. Çalışmanın devamında söz konusu yapılar incelecektir.



Şekil 22. Gizlilik Dereceli Belgelerin Yönetimiyle İlişkili Olan Yapılar

5.2.1. Kamu Kurum ve Kuruluşlarında Gizlilik Dereceli Birim ve Kısımlar

Kamu kurum ve kuruluşlarında çok gizli ve gizli gizlilik dereceli bilgi ve belgeleri üreten ve koruyan birim ve kısımlar ile teftiş ve denetim birimleri, bilgi işlem birimleri, özel kalem müdürlükleri ve personel birimleri gizlilik dereceli birimlerdir. Kamu kurum ve kuruluşlarınca gizlilik dereceli birim ve kısım olarak belirlenenler Cumhurbaşkanlığına bildirilmektedir. Söz konusu bildirime müteakip, bahse konu birim ve kısımların Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik kapsamında (6'ncı madde, 1'inci fıkra) olup olmadığı değerlendirildikten sonra, gizlilik dereceli birim ve kısım olması uygun görülenlere ait bilgiler Cumhurbaşkanlığınca İçişleri Bakanlığı, Milli İstihbarat Teşkilatı Başkanlığı ve Emniyet Genel Müdürlüğüne gönderilmektedir (Güvenlik Soruşturması…, 2022, mad. 6).

5.2.1.2. Gizlilik Dereceli Belgeleri Değerlendirme Komisyonları

Çok gizli gizlilik dereceli belgelere ilişkin gizlilik derecesinin değerlendirilmesi ile bu gizliliğin düşürülmesi, kaldırılması veya belgenin imha edilmesi kararı belge sahibi idare (belgeyi üreten ve gizlilik derecesi belirleyen) tarafından oluşturulan "Çok Gizli Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu" tarafından verilmektedir. Komisyon, belgeyi üreten kurumun en üst yöneticisi veya bu yöneticinin yetki vermiş olduğu yöneticinin başkanlığında en az üç kişiden oluşmaktadır. Komisyon, sonu çift rakam olan senelerin Ocak ayında toplanmakta ve önceki yıllarda üretilen belgelerin durumunu değerlendirmektedir. Ayrıca, belgeyi hazırlayan birim ya da belgeye sahip olan kurumların teklifi üzerine, komisyon olağanüstü toplanarak belgenin gizlilik derecesinin değerlendirilmesi ve imhasına ilişkin karar almaktadır. Komisyon kararları oy çokluğuyla alınmaktadır. Komisyon tarafından verilen gizlilik derecesinin düşürülmesi, kaldırılması veya belgenin imha edilmesi kararına istinaden gerekli işlemler Çok Gizli Belge Bürosu tarafından yerine getirilmektedir (Gizlilik Dereceli Belgelerde…, 2022, mad. 7).

Gizli veya hizmete özel gizlilik dereceli belgelere ilişkin gizlilik derecesinin değerlendirilmesi ile bu gizliliğin devam etmesi veya gizliliğin kaldırılması kararı belge sahibi idare (belgeyi üreten ve gizlilik derecesi belirleyen) tarafından oluşturulan "Gizli ve Hizmete Özel Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu" tarafından verilmektedir. Komisyon, belgeyi üreten birimin yöneticisi veya bu yöneticinin yetki vermiş olduğu yöneticinin başkanlığında, birim yöneticisinin oluruyla belgeyi hazırlayan alt birimden bir yönetici ve bir personel ile birlikte toplam üç kişiden oluşmaktadır. Komisyonun ne zaman ve ne sıklıkla toplanacağı belge sahibi idare tarafından belirlenmektedir. Ayrıca, belgelerin kurum arşivine devredilmesi durumunda, gizlilik derecesinin değerlendirilmesi maksadıyla ilgili komisyon olağanüstü olarak toplanabilmektedir. Komisyon kararları oy çokluğuyla alınmaktadır. Komisyon tarafından verilen kararlara yönelik işlemler belge sahibi birim tarafından yerine getirilmektedir (Gizlilik Dereceli... Yönetmelik, 2022, mad. 7).

5.2.1.3. Arşiv Belgesi Gizlilik Değerlendirme Komisyonu

Devlet Arşiv Başkanlığında bulunan gizlilik dereceli arşiv belgelerinin araştırmaya açılması kapsamında, belgelerin gizlilik niteliğinin değerlendirilmesi ve uygun görülmesi

halinde bu belgelerin gizliliklerinin kaldırılma süreçleri Devlet Arşivleri Başkanlığı tarafından oluşturulan “Arşiv Belgesi Gizlilik Değerlendirme Komisyonu” tarafından yapılmaktadır. Komisyon, Devlet Arşivleri Başkanı tarafından belirlenecek başkan ve üyeler ile ilgili kurum ve kuruluşun temsilcisi (üye) olmak üzere asgari beş kişiden oluşmaktadır. Kararlar oy çoğunluğuyla alınmakta olup, Devlet Arşivleri Başkanının onayı sonrası kesinleşmektedir. Komisyon kararları, Devlet Arşivleri Başkanı oluru ve bunlara ilişkin yazışmalar süresiz olarak saklanmaktadır (Arşivlerden Yararlanma Usul…, 2021).

5.2.1.4. Bilgi Edinme Değerlendirme Kurulu

Bu kurul, 4982 sayılı Bilgi Edinme Hakkı Kanunu’nun (2003) 14’üncü maddesinin gereği olarak oluşturulmuştur. Kurul, Cumhurbaşkanı tarafından atanan dokuz üyeden meydana gelmektedir. Kurulun oluşturulma amacı, Bilgi Edinme Hakkı Kanunu’nda belirtilen istisnalar sebep gösterilerek talebi kabul edilmeyen kişilerin yapacakları itirazlara yönelik (yargı yoluna başvurmadan ikinci bir seçenek olarak) ilgili kurumun kararlarını değerlendirmekte ve ilgili kurumu bağlayıcı kararlar verebilmektedir. Söz konusu kararlar itirazın kabulü, reddi, kısmen kabulü ve kısmen reddi yönünde olabilmektedir (Bilgi Edinme Değerlendirme…, 2023b).

Kişiler bilgi edinme itirazları kapsamında yargı yoluna başvurmadan önce bu kurula itiraz başvurusu yapabilmektedirler. Bu başvuru, bilgi edinme talebinin reddedilmesi kararı tebliğinden itibaren 15 gün içerisinde yapabilmektedir. Kurulun, yapılan itirazları 30 gün içerisinde karara bağlaması gerekmektedir. Bununla birlikte, kurula yapılan bilgi edinme itiraz talepleri, kişilerin idari yargıya başvurma süresini durdurmaktadır (Bilgi Edinme Hakkı…, 2003, mad. 13-14). Kurul, bilgi edinme başvurusuna olumsuz yanıt veren kurumdan ilgili tüm bilgi ve belgeleri isteyebilmekte olup, ilgili kurum bu talebi on beş gün içerisinde yerine getirmekle yükümlüdür. Kurul, itiraz konusuyla ilgili olarak, bilgi edinme talebini yapan kişi ile bilgi edinme talebini reddeden kurum ve kuruluşların yazılı ya da sözlü görüşlerine başvurabilmektedir (Bilgi Edinme Değerlendirme.., 2023a).

5.2.2. Veri, Bilgi ve Belge Yönetiminde Gizlilik

Aras (2011, s. 546), Türkiye Cumhuriyeti Anayasası’nda belirtilen hükümlerin hiçbirinin devlete ya da bireylere verilen hak ve özgürlüklerin ortadan kaldırılmasını ya da

sınırlandırılmasını amaçlayacak şekilde yorumlanamayacağını ifade etmekle birlikte, söz konusu hak ve özgürlüklerin sadece Anayasa'nın on üçüncü maddesi esas alınarak ve ilgili maddelerinde hükme bağlanan sebeplere istinaden, kanunla sınırlanabileceğini ifade etmektedir. Anayasa'da (mad.13 ve mad.14) hak ve özgürlüklerin sınırlandırılma ölçütleri belirtilmekte olup, bilgiye erişim hakkı, bilgiye erişimin sınırları ve bilgiye erişimde yerine getirilecek esaslar ile sorumluluklar Bilgi Edinme Hakkı Kanunu (2003) ile düzenlenmiştir.

Kamu kurum ve kuruluşlarının iş süreçleri, hizmetleri ve iletişiminde varlık bulan veri, bilgi ve belgelerin bir gizlilik derecesiyle ilişkilendirilmesi bilgi edinme hakkı, toplumun yönetime katılması ve şeffaflık ilkesinin kısıtlayıcısı olabilmektedir. Bununla birlikte, herhangi bir gizlilik derecesi taşımamasına rağmen bilgi edinme talebinin yasal olarak olumsuz karşılanmasına olanak sağlayan bazı hususlar bulunmaktadır. Bilgi Edinme Hakkı Kanunu (2003) kapsamında kurumlardan talep edilemeyecek, edilse dahi bilgi edinme talebinin karşılanması mümkün olmayan bilgi ve belgeler Tablo 8' de sunulmaktadır.

Tablo 8. Bilgi Edinme Hakkı Kanunu (2003) Kapsamında Bilgi Edinme Talebi Karşılanmayacak Bilgi ve Belgeler

Kanun Maddesi	**Bilgi Edinme Talebi Karşılanmayacak Bilgi ve Belgeler**
16. madde	Açıklanması hâlinde Devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek ve niteliği itibarıyla Devlet sırrı olan gizlilik dereceli bilgi veya belgeler.
17. madde	Açıklanması ya da zamanından önce açıklanması halinde, ülkenin ekonomik çıkarlarına zarar verecek, haksız rekabet ve kazanca sebep olacak bilgi veya belgeler.
18. madde	Sivil ve askerî istihbarat birimlerinin görev ve faaliyetlerine ilişkin bilgi veya belgeler.
19. madde	Kurum ve kuruluşların yetkili birimlerince yürütülen idari soruşturmalarla ilgili, açıklanması veya zamanından önce açıklanması halinde; kişilerin özel hayatına açıkça haksız müdahale sonucunu doğuracak, kişilerin veya soruşturmayı yürüten görevlilerin hayatını ya da güvenliğini tehlikeye sokacak, soruşturmanın güvenliğini tehlikeye düşürecek, gizli kalması gereken bilgi kaynağının açığa çıkmasına neden olacak veya soruşturma ile ilgili benzeri bilgi ve bilgi kaynaklarının temin edilmesini güçleştirecek bilgi veya belgeler.

20. madde	Adil soruşturma ve kovuşturmalarla ilgili, açıklanması veya zamanından önce açıklanması hâlinde; suç islenmesine yol açacak, suçların önlenmesi ve 119 soruşturulması ya da suçluların kanunî yollarla yakalanıp kovuşturulmasını tehlikeye düşürecek, yargılama görevinin gereğince yerine getirilmesini engelleyecek, hakkında dava açılmış bir kişinin adil yargılanma hakkını ihlâl edecek nitelikteki bilgi veya belgeler.
21. madde	Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler (Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir).
22. madde	Haberleşmenin gizliliği esasını ihlal edecek bilgi veya belgeler.
23. madde	Kanunlarda ticari sır olarak nitelenen bilgi veya belgeler ile kurum ve kuruluşlar tarafından gerçek veya tüzel kişilerden gizli kalması kaydıyla sağlanan ticari ve mali bilgiler.
24. madde	Fikir ve sanat eserlerine ilişkin olarak yapılacak bilgi edinme başvuruları hakkında ilgili kanun hükümleri uygulanır.
25. madde	Kurum ve kuruluşların, kamuoyunu ilgilendirmeyen ve sadece kendi personeli ile kurum içi uygulamalarına ilişkin düzenlemeler hakkındaki bilgi veya belgeler" (Ancak, söz konusu düzenlemeden etkilenen kurum çalışanlarının bilgi edinme hakları saklıdır).
27. Madde	Tavsiye ve mütalaa talepleri.

Bilgi Edinme Hakkı Kanunu'nda (2003, mad. 28) ayrıca, gizliliği kaldırılan bilgi ve belgelerin yukarıda belirtilen istisnalar kapsamına girmemesi koşuluyla bilgi edinme taleplerinde açık hale getirileceği hükmü bağlanmıştır.

Türkiye Cumhuriyeti Anayasası ile yasal ve idari düzenlemelerde devlet sırrı ile veri, bilgi ve belge gizliliğine ilişkin hükümler yer almaktadır. Bu hükümlerde, hangi olguların devlet sırrı olacağı, devlet sırlarının belirlenme usulleri, hangi makam ve mercilerin bilgi ve belgeleri devlet sırrı olarak belirleyeceğine ilişkin yeterli açıklamalar bulunmamaktadır. Bu eksikliğin giderilmesi maksadıyla "Devlet Sırrı Kanunu Tasarısı" hazırlanmış ve 2011 yılında TBMM'ye sunulmuştur. Henüz yasalaşmamış olan Devlet Sırrı Kanunu Tasarısı'nda bilgi ve belgelerin gizliliğin sağlanması ve korunmasına yönelik "devlet sırrı" ve "devlet sırrı niteliği taşımayan diğer gizli bilgi ve belgeler" şeklinde iki ayrı kavrama yer verilmiştir. Kanun tasarısında, hangi olguların devlet sırrı olarak kabul edileceği, hangi bilgi ve belgelerin gizlilik derecesiyle ilişkilendirileceği,

hangi makam ve mercilerin devlet sırrını belirlemeye yetkili olacağı yer almaktadır. Kanun tasarısında devlet sırrı olarak nitelendirilen bilgi ve belgelere ilişkin gizliliğin süreli veya süresiz olarak verilebileceği, süreli olarak belirlenen gizliliğin yetmiş beş yılı geçemeyeceği ve Devlet Sırrı Kurulu'nca aksi bir karar verilmediği müddetçe süresiz olarak belirlenen devlet sırrı niteliğindeki bilgi ve belgelerin bu gizlilik niteliklerini elli yıl sonra kaybedecekleri ifade edilmektedir. Kanun tasarısı ile oluşturulması planlanan Devlet Sırrı Kurulu'nca, on yıldan fazla süreli olarak devlet sırrı olarak kıymetlendirilen bilgi ve belgelerin beş yılda bir, süresiz olarak devlet sırrı olarak kıymetlendirilenlerin ise on yılda bir gözden geçirilerek devlet sırrı niteliklerinin değerlendirileceği hükme bağlanmak istenmiştir. Kanun tasarısında ayrıca, devlet sırrı niteliğinde olmayan gizlilik dereceli bilgi ve belgelerin gizlilik sürelerinin ise devlet sırrı sürelerinin (süresiz olarak en fazla elli yıl, süreli olarak en fazla yetmişbeş yıl) yarısını geçemeyeceği ifade edilmektedir (Devlet Sırrı Kanunu Tasarısı, 2008).

5271 sayılı Ceza Muhakemesi Kanunu'nda (2004, mad. 47, 125) hangi bilgilerin devlet sırrı sayılacağı ifade edilmekte birlikte, devlet sırrı olan bilgilerin mahkemelerce erişimine ilişkin düzenlemeler yapılmıştır. 5237 Sayılı Türk Ceza Kanunu'nda (2004, mad. 326-339) devlet sırları ve gizli bilgi/belge ihlallerine yönelik suç vasıfları belirtilmiş ve ilgili cezalar düzenlenmiştir.

Kamusal veri, bilgi ve belgelerin yetkisiz kişilerle paylaşılmaması durumu olan gizlilik, sır niteliğinde olanların koruma yöntemi olup, söz konusu kavramlar iç içe geçmiş ve çoğunlukla birbirlerinin yerine kullanılabilir duruma gelmiştir (Aras, 2011, s. 548). Yasal mevzuatta veri, bilgi ve belgelerin korunması ve yetkili kişiler haricinde erişilmesinin kısıtlanmasına yönelik çok çeşitli konu ve alanlarda (Kolluk kuvveti, haberleşme özgürlüğü, sivil savunma mevzuatı vb.) "sır" ve "gizlilik" kavramları kullanılmakta olup, yasal düzenlemelerde ifade edilen sır ve gizlilik kavramları arasında net bir farklılık bulunmamaktadır (Gemalmaz ve Gemalmaz, 2004).

Kamu kurum ve kuruluşları tarafından yerine getirilen görev ve hizmetlerde, devletin ve kişilerin menfaatlerinin korunması için, gizlilik sınıflandırılması yapılarak veri, bilgi ve belgelere yönelik yetkisiz erişimler engellenmektedir (Diri ve Gülçiçek, 2012, s.499). Sır ve gizlilik, bilgilerin sınıflandırılmasını ve gizlilik derecesinin belirlenmesini gerektiren bir sınıflandırma ve kategorize etme işlemidir (Özdemir ve Torunlar, 2015, s. 50). Bu işlem bilginin neden gizli olduğunun, ne kadar gizli olduğunun, nerede bulunduğunun, nasıl

saklandığının, ne kadar süreyle gizli kalacağının ve kimlere yönelik gizli olduğunun belirlenmesi amacıyla yapılmaktadır.

Veri, bilgi ve belgelerin ilgili gizlilik derecelerine göre sınıflandırılması ve bu gizlilik derecesine sahip gerçek veya tüzel kişilerle paylaşılması süreci bir gizlilik politikası uygulamasıdır (Eken, 1994, s. 26). Bu gizlilik politikası kurum ve kuruluşların iç ve dış çevrelerine karşı uygulanmaktadır (Karaman ve Atak, 1996, s. 111). Söz konusu gizlilik politikasının temelini oluşturulan gizlilik sınıflandırılması ise yasal zeminden vücut bulmaktadır.

5.2.3. Belge Yönetiminde Gizlilik Düzeyleri

Belgelerin gizlilik derecelerine göre sınıflandırılması, uygun iş ve güvenlik süreçlerinin belirlenmesinde en önemli bileşendir. Gizlilik derecesinin doğru kullanımı, belge yönetimi süreçlerinin verimli bir şekilde yönetilmesine, hesap verilebilir ve şeffaf bir yönetim anlayışının etkin bir şekilde sürdürülebilmesine ve bilgi edinme taleplerinin doğru bir şekilde karşılanmasını sağlamaktadır. Gizlilik derecesinin yanlış kullanımı (belgenin gereğinden fazla ya da düşük gizlilik derecesiyle sınıflandırılması) ise, iş süreçlerinin yoğunluğunun ve maliyetinin artmasına, yerine getirilen faaliyetlerin gecikmesine, güvenlik ve hak ihlallerinin yaşanmasına sebep olabilmektedir.

Kurumsal faaliyetlerinin önemli bir parçasını oluşturan belge süreçlerinin belirli güvenlik düzeylerinde yeknesak olarak gerçekleştirilmesi maksadıyla 26 Nisan 2022 tarihinde Resmi Gazetede yayınlanan “Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik” ile “Çok Gizli” “Gizli” ve “Hizmete Özel” olmak üzere üç adet millî gizlilik derecesi belirlenmiş olup, bu yönetmelik öncesinde kullanılmakta olan “Özel” gizlilik derecesi yürürlükten kaldırılmıştır. Özel gizlilik dereceli olan belgelere yönelik ilgili idareler tarafından 26 Nisan 2023 tarihinde kadar yapılacak değerlendirme sonucunda, bu gizlilik derecesine sahip belgeler gizli olarak tanımlanabilmekle birlikte, bu şekilde tanımlanmayan belgeler ise hizmete özel gizlilik derecesinde değerlendirilecektir (Gizlilik Dereceli Belgelerde…,2022).

Savunma Sanayii Güvenliği Kanunu’nda (2004), antlaşmalar çerçevesinde savunma sanayii süreçlerinde yapılan yer alan gerçek ve tüzel kişilerin bilgi, belge, proje, malzeme ve hizmetlerin ve bunlarla ilgili yerlerin güvenliğinin ve korunmasının

sağlanmasına yönelik “Çok Gizli”, “Gizli”, “Özel” ve “Hizmete Özel” olmak üzere dört adet gizlilik derecesinin kullanılacağı ifade edilmiştir. Ayrıca, Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesinde, NATO ile ilişkili uygulamalar ve yazışmalarda kullanılacak gizlilik dereceleri ve bunların Türkçe karşılıkları belirlenmiştir. Bu gizlilik dereceleri ve Türkçe karşılıkları şu şekildedir (Milli Savunma Bakanlığı…, 2023):

- Cosmic Top Secret (Kozmik Çok Gizli),
- NATO Secret (NATO Gizli),
- NATO Confidential (NATO Özel),
- NATO Restricted (NATO Hizmete Özel).

TS 13298 Standardında (2015, mad. 9.2.3), EBYS’nin, bünyesinde bulunan elamanlara yönelik erişim haklarının “Çok Gizli”, “Gizli”, “Özel”, “Hizmete Özel” ve “Tasnif Dışı” olmak üzere beş kademeli olarak tanımlayabilmesi gerektiği ifade edilmektedir. Bu gizlilik derecelerinin bilgi, belge, evrak, mesaj ve dokümanlarla ilişkili olduğu ifade belirtilmektedir. Bu standartta; müsaadesiz olarak açıklanması halinde ulusal güvenlik, devlete ve müttefiklere büyük zarar verebilecek olan varlıklarda kullanılan gizlilik derecesinin çok gizli olduğu, müsaadesiz olarak açıklanması halinde ulusal güvenlik, milli prestij ve menfaatleri önemli ve ciddi olarak zedeleyecek olan varlıklarda kullanılan gizlilik derecesinin gizli olduğu, müsaadesiz olarak açıklanması halinde milli menfaatleri olumsuz olarak etkilenmesine sebebiyet verebilecek olan varlıklarda kullanılan gizlilik derecesinin özel olduğu, devlet hizmetlerinin yürütülmesine ilişkin özel bilgilere haiz olan varlıklarda kullanılan gizlilik derecesinin hizmete özel olduğu, gizlilik derecesine sahip olmayan varlıkların tasnif dışı olduğu ifade edilmektedir.

5.2.4. Veri Yönetiminde Gizlilik Düzeyleri

Kamu kurum ve kuruluşlarına ait bazı verileri gruplarının ulusal sır içermesi, bilgilere erişim endişesinin ve açık veri uygulamasındaki kısıtlamalarının önemli bir parçasını oluşturmaktadır (Eroğlu, 2017, s. 115). Bu sebeple, verilerinin ilgili gizlilik derecelerine göre sınıflandırılması ve yetkisiz erişimin engellenmesi kişilerin, kurum ve kuruluşların, devletin ve uluslararası menfaatlerinin korunması açısından oldukça önemlidir. 06 Temmuz 2019 tarihinde yayınlanan 2019/2 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi’nin bir gereği olarak yayınlanan ve Bilgi ve İletişim

Güvenliği Rehberi'nde bilgi/veriler farklı güvenlik seviyelerine göre "Gizlilik Dereceli Bilgi/Veri" ve "Kritik Bilgi/Veri" olarak kategorize edilmiştir (Bilgi ve İletişim…, 2020, s. 7).

- Gizlilik dereceli bilgi/veri: Yetkisiz olarak paylaşılması milli güvenliğe ve ülke menfaatlerine zarar verebilecek veriler "Çok Gizli", "Gizli", "Özel" ve "Hizmete Özel" olarak farklı güvenlik seviyelerinde sınıflandırılmıştır.
- Kritik bilgi/veri: Güvenlik ihlali olmasıyla yasal olarak yaptırımlara sebep olabilecek ve yetkilendirilmemiş kamu personeli veya kişilerce içeriğin görülmesiyle kuruma çok ağır parasal veya manevi zarar verebilecek olan bilgi/veriler, rehberde belirtilen anket sonucuna göre kritiklik derecesi 3 olarak hesaplanan bilgi varlıklarının işlemiş olduğu veriler ve özel nitelikli kişisel veriler (hassas kişisel veriler) kritik bilgi/veri olarak sınıflandırılmıştır.

Verilerin gerekli güvenlik düzeylerine uygun olarak sınıflandırılmasının yapılması kapsamında, Koç Üniversitesi (2022) tarafından oluşturulan veri sınıflandırma prosedüründe veriler beş hassasiyet grubuna ayrılmış olup, prosedür kapsamında belirlenen gizlilik dereceleri ve bu gizlilik derecelerinin açıklamaları ile örnek olgular Şekil 23'de gösterilmiştir.

Gizlilik Derecesi	Açıklama	Örnek
Çok Gizli	Sınırlı kişiler tarafından bilinmesi gereken, başka kişi/kişiler/kuruluşlar ile paylaşılması, kaybolması durumunda Üniversite'nin mevcudiyetini ve faaliyetini ciddi olarak olumsuz etkileyecek ulusal ya da uluslararası risklere ya da anlaşmazlıklara neden olacak, yasal soruşturma ya da incelemeye neden olacak verilerdir.	Ulusal güvenlik ya da savunma sanayi projeleri için kullanılacak her türlü proje ve amacı olan buluş ile ilgili bilgiler (yazılımlar, çizimler, proje belgeleri vb.), yatırım planları, yatırım stratejileri ve hedefleri ile ilgili bilgiler, sektörde büyük değişikliklere neden olacak, rekabet koşullarını değiştirecek buluş ya da metodolojiler ile ilgili bilgiler vb.
Gizli	Yetkisiz kişi/kişiler/kuruluşlar ile paylaşılması ya da kaybolması durumunda Üniversite'nin operasyonlarını, imajını veya gelirlerini ciddi olarak etkileyecek ve aksatacak veriler bu kapsama girer.	Şifreler, iş planları, maaş bilgileri, sözleşmeler, teklifler, maliyet raporları, şartnameler, hassas tasarım çalışmaları, hasta bilgileri, satış bilgileri, servis bilgileri, lansmanı yapılmamış yeni hizmetler, iş ortaklığı anlaşma içerikleri, stratejik planlar, personele ait özlük bilgileri, uygulanan güvenlik kontrolleri, kredi kartı bilgileri vb. Ayrıca KVKK özel nitelikli hassas kişisel veriler bu kategoriye girer.
Hizmete Özel	Sadece Üniversite içinde veya ihtiyaç durumunda hizmet alınan ve Gizlilik Sözleşmesi imzalanan kurumlarla paylaşılan ve Üniversite veya belirtilen kurumların dışına çıkması onaylanmayan, izinsiz paylaşımı ya da kaybı Üniversite organizasyonu için imaj kaybı gibi sonuçlar doğurabilecek, uygunsuzluklar yaratabilecek ancak ciddi maddi zararlara ya da hasarlara neden olmayacak verilerdir.	Hizmet alınacak firmalarla paylaşılabilecek operasyonel bilgiler, projelerle ilgili dokümanlar, proje gereği Gizlilik Sözleşmesi imzalanmış firmalarla paylaşılan iş özelindeki bilgiler vb.
Kurum İçi	Sadece Üniversite içinde paylaşılan ve Üniversite dışına çıkması onaylanmayan, izinsiz paylaşımı ya da kaybı Üniversite organizasyonu için imaj kaybı gibi sonuçlar doğurabilecek, uygunsuzluklar yaratabilecek ancak ciddi maddi zararlara ya da hasarlara neden olmayacak verilerdir.	Toplantı zamanları, genel üniversite bilgilendirmeleri, duyurular, telefon listeleri, çalışan listeleri, eğitim bilgileri, formlar, yazışma örnekleri, prosedürler, operasyonel bilgiler, proje planları, ad, soyad ve IP adresleri içeren dokümanlar vb. Ayrıca KVKK kişisel verileri bu kategoriye girer.
Genel	Geneli ilgilendiren en düşük güvenlik seviyesindeki veriler olup paylaşılması ya da kaybolması durumunda risk oluşmayan, herkese açık verilerdir. "KURUM İÇİ", "GİZLİ", "HİZMETE ÖZEL" ve "ÇOK GİZLİ" olarak gizlilik sınıflandırması belirlenmemiş olan veriler "GENEL" olarak sınıflandırılır.	Basın açıklamaları, genel duyurular, kurumsal web sayfaları, hizmet katalogları, tanıtım broşürleri vb.

Şekil 23. Veri Sınıflandırma Prosedürü (Koç Üniversitesi, 2022)

Kamu kurum ve kuruluşları faaliyet alanlarıyla ilgi iş süreçleri ve hizmetlerinde devlet tarafından konulan kurallara uymak zorundadır. Eroğlu (2017) tarafından yapılan çalışmada, kamu kurumlarında veri sınıflamaların, yasal ve idari düzenlemeler kapsamında oluşturulan EBYS sistemlerindeki dosyalama, format ve gizlilik hususları kapsamında yapıldığı tespit edilmiştir. Kamu verilerinin gizlilik ve güvenliğinin sağlanması için yürürlükte bulunan yasal düzenlemelere göre gizlilik sınıflandırma prosedürlerin oluşturulması, kurum içi ve dışı paydaşlarla veri alışverişinde bu prosedürlere uyulması oldukça önemlidir.

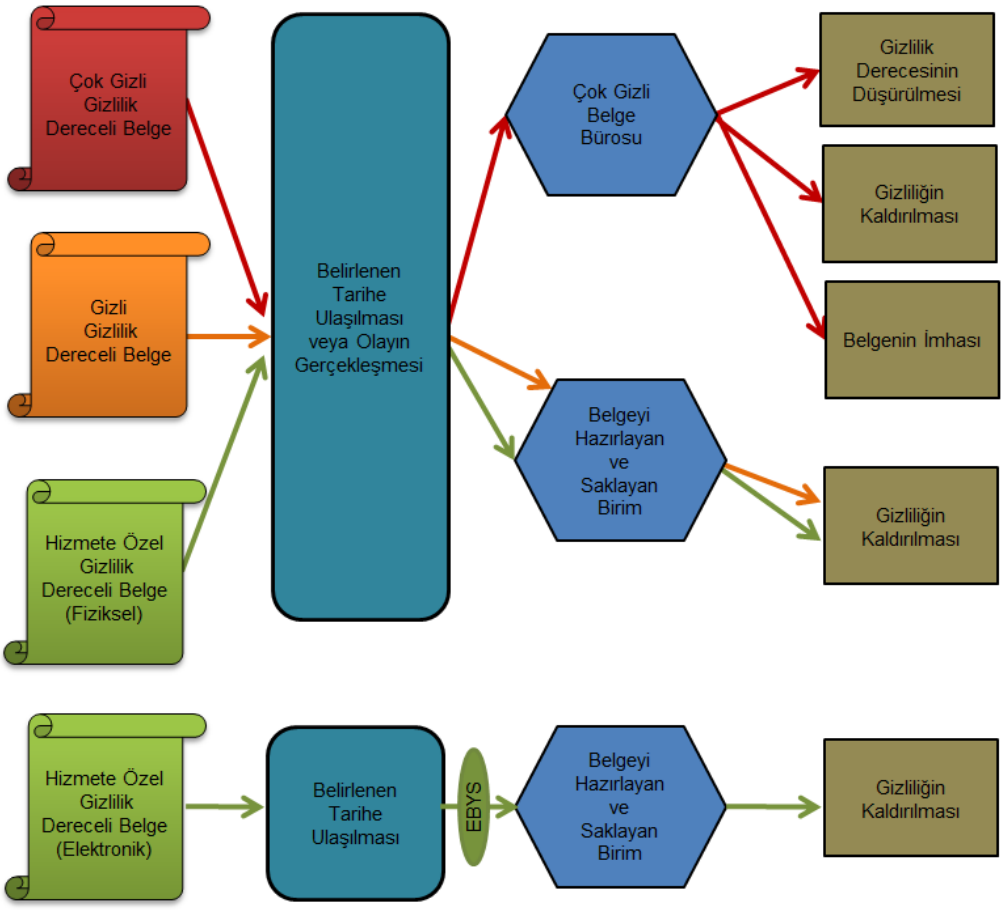
5.2.5. Gizlilik Derecesi Belirlemeye Yetkili Makam ve Kişiler

Kamu kurum ve kuruluşlarında, çok gizli gizlilik derecesine sahip belgeye idarenin üst yöneticisi, gizli gizlilik derecesine sahip belgeye birim yöneticisi (alt birim yöneticisine devredebilir), hizmete özel gizlilik derecesine sahip belgeye birim veya alt birim yöneticisi gizlilik derecesi verme yetkilidir (Gizlilik Dereceli Belgelerde…, 2022). Belge yönetiminde gizlilik derecesinin belirlenmesine ilişkin yetkili şeması Şekil 24'de gösterilmiştir.

Şekil 24. Belgelerde Gizlilik Derecesi Belirlemeye Yetkili Makam ve Kişiler (Gizlilik Dereceli Belgelerde…, 2022)

5.2.6. Süreli Gizlilik

Süreli gizlilik, belgelerin gizlilik derecesinin güncelliğini yitireceği zaman veya olay kapsamında gizlilik derecelerinin düşürülmesi veya belgelerin imha edilmesine yönelik bir uygulamadır (Gizlilik Dereceli Belgelerde…, 2022). Belgenin gizlilik derecesinin belirlenmesi esnasında verilecek olan süreli gizliğe ilişkin bilgiler belgenin üzerinde, elektronik belgenin ise üst verisinde belirtilebilmektedir. Belirlenen tarihe gelindiğinde ya da olay vuku bulduğunda veya sona erdiğinde, bir komisyon kararı veya yazışmaya gerek duyulmadan, belge üzerinde veya üst verisinde bulunan talimata göre işlem yapılmaktadır. Belgelerde süreli gizlilik süreci Şekil 25'de gösterilmiştir.



Şekil 25. Belgelerde Süreli Gizlilik Süreci

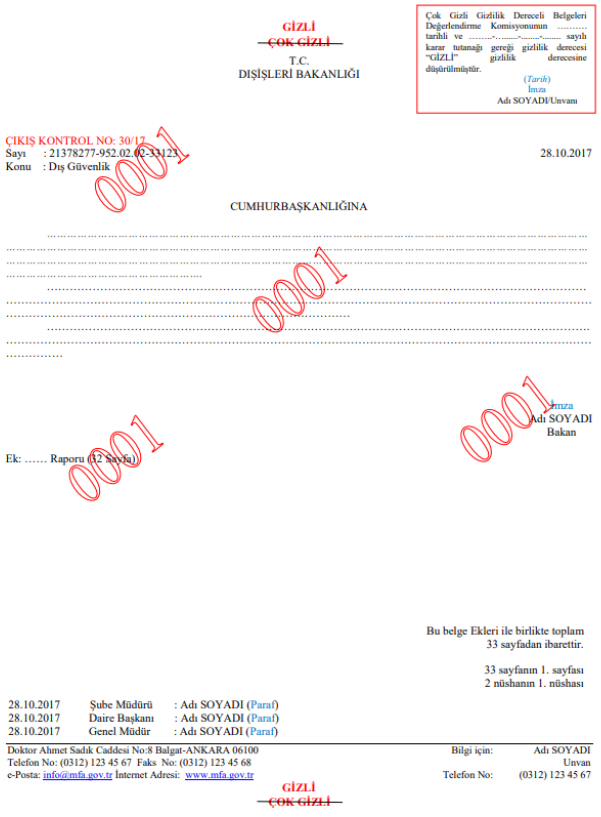
Süreli gizlilik süreci sona eren çok gizli gizlilik dereceli belgelere yönelik işlemler ilgili büro tarafından, diğer gizlilik dereceli belgelere yönelik işlemler ise belgeyi üreten veya elinde bulunduran birimlerce yapılmaktadır. Gizlilik dereceli belgeyi üreten kurum

tarafından oluşturulan komisyonlar süreli gizlilik zamanına ulaşılmadan veya olay gerçekleşmeden/sonlanmadan gizliğe ilişkin değerlendirme yapabilmektedir.

5.2.7. Gizlilik Derecesinin Düşürülmesi ve Kaldırılması ile Belgenin İmhası

Çok gizli gizlilik dereceli belgeye yönelik gizlilik derecesinin düşürülmesi, gizliliğin kaldırılması veya belgenin imhasına ilişkin karar belgeyi üreten kurumca oluşturulan değerlendirme komisyonu tarafından verilmektedir. Çok gizli gizlilik dereceli belgeye gizli gizlilik derecesine düşürülebilmekte olup, hizmete özel gizlilik derecesine düşürülememektedir.

Gizlilik derecesi düşürülen veya kaldırılan çok gizli gizlilik dereceli belgenin tüm sayfalarındaki gizlilik derecesi çizilir ve altına gizli gizlilik derecesi yazılır veya kaşelenir, ilk sayfasına Komisyon tarafından verilen karara ilişkin bilgiler yazılır ve bu hususlar belgeye ait defter ve form kayıtlarının ilgili bölümlerine yazılır. Gizlilik güncellenmesi ve komisyon kararına ilişkin bilgiler Şekil 26'da gösterildiği gibi çok gizli gizlilik dereceli belgelere ithal edilir.


GİZLİ
~~ÇOK GİZLİ~~

T.C.
DIŞİŞLERİ BAKANLIĞI

Çok Gizli Gizlilik Dereceli Belgeleri Değerlendirme Komisyonunun ..... tarihli ve .....-.....-.....-..... sayılı karar tutanağı gereği gizlilik derecesi "GİZLİ" gizlilik derecesine düşürülmüştür.
(Tarih)
İmza
Adı SOYADI/Unvanı

ÇIKIŞ KONTROL NO: 30/17
Sayı : 21378277-952.02.02-33123
Konu : Dış Güvenlik

28.10.2017

CUMHURBAŞKANLIĞINA

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

İmza
Adı SOYADI
Bakan

Ek: ..... Raporu (32 sayfa)

Bu belge Ekleri ile birlikte toplam
33 sayfadan ibarettir.

33 sayfanın 1. sayfası
2 nüshanın 1. nüshası

28.10.2017 Şube Müdürü : Adı SOYADI (Paraf)
28.10.2017 Daire Başkanı : Adı SOYADI (Paraf)
28.10.2017 Genel Müdür : Adı SOYADI (Paraf)

Doktor Ahmet Sadık Caddesi No:8 Balgat-ANKARA 06100
Telefon No: (0312) 123 45 67 Faks No: (0312) 123 45 68
e-Posta: info@mfa.gov.tr İnternet Adresi: www.mfa.gov.tr

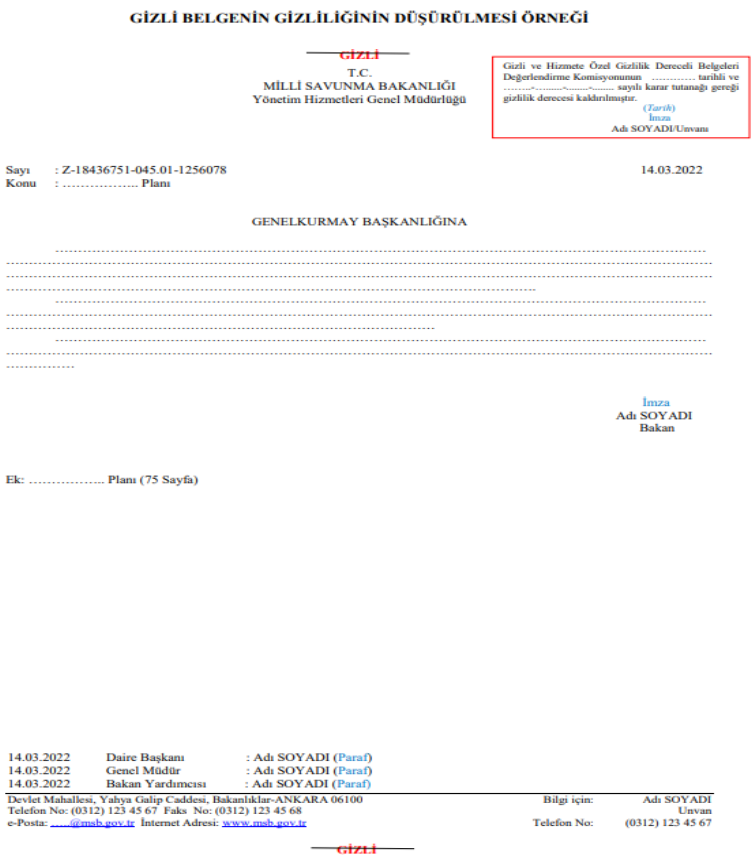
Bilgi için: Adı SOYADI
Unvan
Telefon No: (0312) 123 45 67

GİZLİ
~~ÇOK GİZLİ~~

Şekil 26. Gizlilik Derecesinin Düşürülmesi veya Kaldırılmasına İlişkin Çok Gizli Gizlilik Dereceli Belgeye İthal Edilen Bilgiler (Gizlilik Dereceli Belgelerde…, 2022).

Belgenin imhasına karar verildiğinde, Çok Gizli Belge Bürosu tarafından imha kararı verilen belgeye sahip olan ilgili idarelerden söz konusu belgeleri imha etmeleri ve imha tutanaklarının gönderilmesi istenir. Söz konusu imhanın gerçekleştirildiğine ilişkin tutanak büroya geldiğinde, büro tarafından idarenin sahip olduğu dosya nüshası "Çok Gizli Belge İmha Tutanağı" tanzim edilerek imha edilir. Çok gizli gizlilik dereceli belgenin imha işlemi, kağıdı, basılı ve elektronik materyali okunmaz ve kurtarılamaz hale getiren bir cihaz vasıtasıyla gerçekleştirilir.

Gizli ve hizmete özel gizlilik dereceli belgelerin gizlilik derecesinin kaldırılmasına ilişkin karar belgeyi üreten kurumca oluşturulan değerlendirme komisyonu tarafından verilmektedir. Gizlilik derecesi kaldırılan belgelerin gönderildiği kurumlara ya da birimlere bu durum bildirilmektedir. Gizli gizlilik dereceli belgenin gizlilik derecesinin kaldırılması ve komisyon kararına ilişkin bilgiler Şekil 27'de gösterildiği gibi belgeye ithal edilir. Gizlilik derecesi kaldırılan belge EBYS'ye dahil edilmekle birlikte, belgenin fiziki nüshası saklanmalıdır.



GİZLİ BELGENİN GİZLİLİĞİNİN DÜŞÜRÜLMESİ ÖRNEĞİ

GİZLİ

T.C.
MİLLİ SAVUNMA BAKANLIĞI
Yönetim Hizmetleri Genel Müdürlüğü

Gizli ve Hizmete Özel Gizlilik Dereceli Belgeleri Değerlendirme Komisyonunun ..... tarihli ve ..... sayılı karar tutanağı gereği gizlilik derecesi kaldırılmıştır.
(Tarih)
İmza
Adı SOYADI/Unvanı

Sayı : Z-18436751-045.01-1256078
Konu : ..... Planı

14.03.2022

GENELKURMAY BAŞKANLIĞINA

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

İmza
Adı SOYADI
Bakan

Ek: ..... Planı (75 Sayfa)

14.03.2022 Daire Başkanı : Adı SOYADI (Paraf)
14.03.2022 Genel Müdür : Adı SOYADI (Paraf)
14.03.2022 Bakan Yardımcısı : Adı SOYADI (Paraf)

Devlet Mahallesi, Yahya Galip Caddesi, Bakanlıklar-ANKARA 06100
Telefon No: (0312) 123 45 67 Faks No: (0312) 123 45 68
e-Posta: ....@msb.gov.tr İnternet Adresi: www.msb.gov.tr

Bilgi için: Adı SOYADI
Unvan
Telefon No: (0312) 123 45 67

GİZLİ

Şekil 27. Gizlilik Derecesinin Kaldırılmasına İlişkin Gizli Gizlilik Dereceli Belgeye İthal Edilen Bilgiler (Gizlilik Dereceli Belgelerde…, 2022).

Hizmete özel gizlilik dereceli belgenin gizlilik derecesinin kaldırılması kapsamında EBYS'deki üst veri alanında güncelleme yapılması ve güncellenen belge e-mühür vasıtayla mühürlenerek zaman damgasıyla damgalanması gerekmektedir. Söz konusu işlemler EBYS'nin günlük kayıtlarında yer almalıdır. Gizlilik derecesinin kaldırılmasına ilişkin komisyon kararı belgeyle ilişkilendirilerek EBYS'de muhafaza edilmektedir.

Gizlilik dereceli belgelerin arşive devredilmesi kapsamında, gizlilik dereceli belgeye sahip olan dosya ya da klasör etiketinin üzerine en yüksek dereceye gizlilik derecesine sahip belgenin bilgileri yazılmakta olup, bu dosya/klasörler arşivde tasnif ve yerleştirmesi diğer dosya/klasörlerle birlikte tasnife tabi tutulmaktadır. Kurum arşivinden Devlet Arşivleri Başkanlığına sevk edilen ve burada arşivlenen belgeler, arşive aktarıldıkları sırada sahip oldukları gizlilik derecesini korumaktadır. Bu gizliliğin kaldırılmasına yönelik karar ilgili kurum, kuruluş ve idarenin görüşü alındıktan sonra Devlet Arşivleri Başkanlığınca verilebilmektedir (Devlet Arşiv Hizmetleri…, 2019, mad.7).

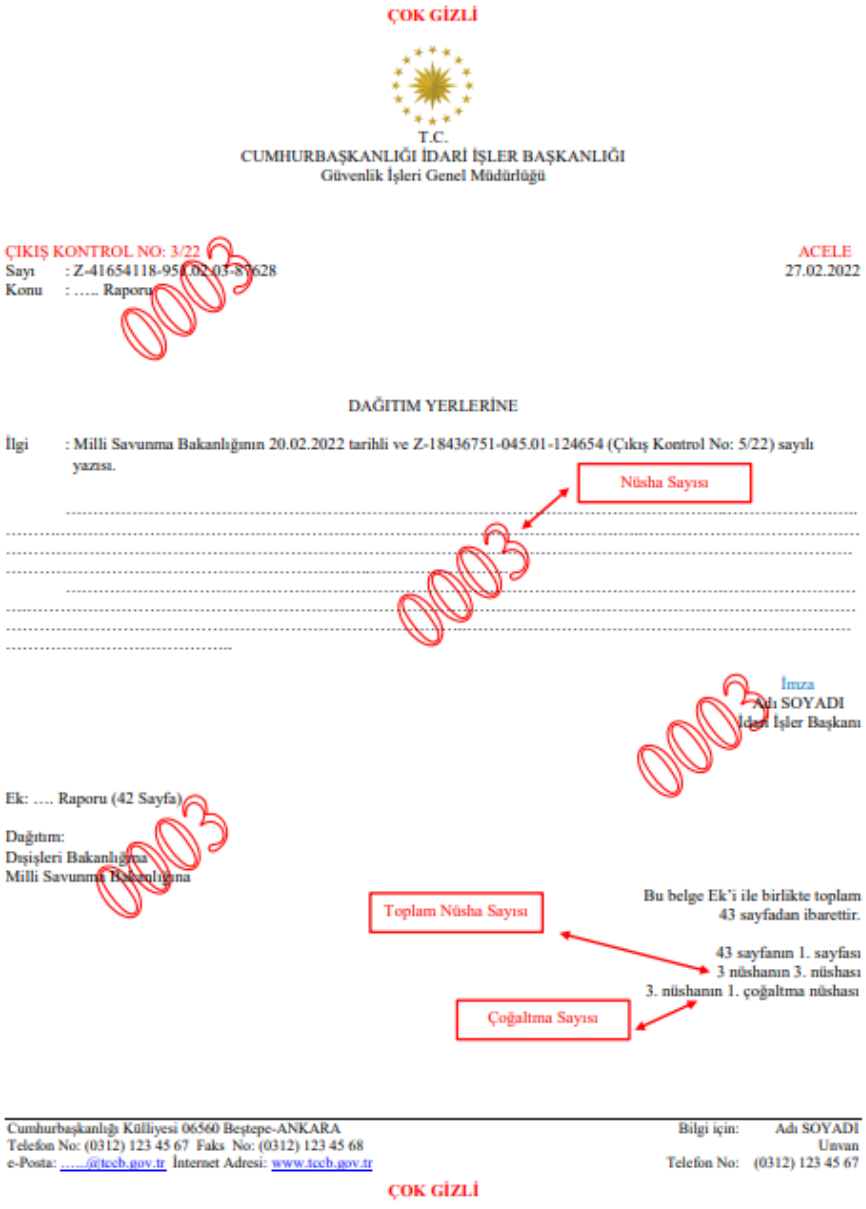
Devlet Arşivleri Başkanlığına devredilen gizlilik dereceli arşiv belgelerinin gizliliğinin değerlendirilmesi ve bu gizliliğin kaldırılma işlemleri Devlet Arşivleri Başkanlığı tarafından oluşturulan "Arşiv Belgesi Gizlilik Değerlendirme Komisyonu" tarafından yürütülmektedir. Gizlilik dereceli arşiv belgesinin incelenmesi ve ilgili gizlilik derecesinin kaldırılması yönündeki komisyon kararı Devlet Arşivleri Başkanının onayıyla kesinleşmektedir. Gizliliği kaldırılan arşiv belgeleri diğer belgeler ile araştırma hizmetine sunulmaktadır (Arşivlerden Yararlanma Usul…, 2021, mad. 10).

5.2.8. Gizlilik Dereceli Belgelerin Yönetimi

5.2.8.1. Çok Gizli Gizlilik Dereceli Belgelerin Hazırlanması

Çok gizli gizlilik dereceli belgeler, bu gizlilik derecesine sahip işlem personeli tarafından, gerekli güvenlik önlemleri alınmış cihazlarla (bilgisayar, yazıcı vb.), belgelerin yönetimi için oluşturulmuş "Çok Gizli Belge Büroları"nda büro personelinin gözetiminde hazırlanmalıdır. Belge, Çok Gizli Belge Bürosu haricinde oluşturulmuş başka bir odada hazırlanıyorsa büro personelin refakat etmesi zorunlu değildir.

Çok gizli gizlilik dereceli belgeler muhatap sayısı (dağıtım nüshası) ve dosya nüshası kadar hazırlanır. Belgede ve bu belgenin tüm eklerinde çıkış kontrol numarası, nüsha sayısı ve toplam nüsha sayısının belirtilmelidir. Nüsha sayısı belgenin dosya nüshası ile başlamakta ve ardışık olarak dağıtım listesinde belirtilen muhatap kadar oluşturulmaktadır. Belgenin tüm ekleriyle birlikte kaç sayfadan oluştuğu, kaçıncı nüsha olduğu, çıkış kontrol numarasının ne olduğu belgenin üst yazısında ve tüm eklerinde belirtilmekte olup, bunların kullanımı Şekil 28'de gösterilmektedir.



Şekil 28. Çok Gizli Belge Örneği (Gizlilik Dereceli Belgelerde..., 2022)

Çok gizli gizlilik dereceli belgelerin hazırlanması kapsamında oluşan müsveddedeler Çok Gizli Belge Bürosunun denetiminde imha edilir. Belgenin üretiminde kullanılan taslaklar ve bilgiler bilgisayarın belleğinden silinmelidir. Çok gizli belgeyi hazırlayan işlem personeli takibinde yürütülen imza süreçleri tamamlanmasının ardından, belge tüm nüsha ve ekleriyle birlikte Çok Gizli Belge Bürosuna teslim edilmektedir.

5.2.8.2. Çok Gizli Gizlilik Dereceli Belgelerin Gönderilmesi

Çok Gizli Büro personeli, teslim alınan belgelere yönelik kayıt işlemleri yaparak belgenin dosya nüshası için örneği Şekil 29'da gösterilen Çok Gizli Belge Takip Kontrol Formu oluşturulur ve belgenin muhatap idarelere gönderilecek nüshaları için ikişer nüsha senet hazırlamaktadır.

ÇOK GİZLİ BELGE TAKİP KONTROL FORMU ÖRNEĞİ

Hazırlayan İdare/Birim: İçişleri Bakanlığı (Emniyet Genel Müdürlüğü)			**Dili:** Türkçe	**Belge Tarihi:** 18.03.2022
Belge Sayısı: Z-11837526-951.01.01-23453211			**Ek/Ekler**: 15 Sayfa	**Sayfa Sayısı:** 16
Toplam Nüsha Sayısı: 2			**Çıkış Kontrol Numarası:** 11/22	**Giriş Kontrol Numarası:** 25/21
Nüsha Sayısı: 0002			**Belge Senedi Numarası:** 45/22	**Saklandığı Alan:** C-8
Geldiği Tarih: 18.03.2022			**Belge Konusu:** …….. Tedbirleri	
BELGEYE İLİŞKİN İŞLEMLER				
Tarih-Saat	**İşlem Türü**	**Gerekçe/Açıklama**	**Teslim Eden/ İmza**	**Teslim Alan/ İmza**
18.03.2022 13.30	İncelemek Üzere Belgeye Erişim	**…….** tarihli ve ……sayılı olur gereğince üzerinde çalışmak üzere 15 gün süreyle belge teslim edilmiştir.	Adı SOYADI Çok Gizli Belge Büro Personeli İmza	Adı SOYADI Şube Müdürü 123 45 67 İmza
01.04.2022 15.30	İade İşlemi	**…….** tarihli ve ……sayılı olur gereğince teslim edilen belge eksiksiz iade edilmiş ve teslim alınmıştır.	Adı SOYADI Şube Müdürü 123 45 67 İmza	Adı SOYADI Çok Gizli Belge Büro Personeli İmza
05.04.2022 14.30	Çoğaltma İşlemi	…… tarihli ve …. sayılı olur ile belgenin Hukuk ve Mevzuat Genel Müdürlüğüne iletilmek üzere 1 nüsha çoğaltılması talep edilmiştir. Çoğaltma nüshası erişim yetkisi bulunan Adı SOYADI'na teslim edilmiştir.	Adı SOYADI Çok Gizli Belge Büro Yetkilisi İmza	Adı SOYADI Uzman İmza

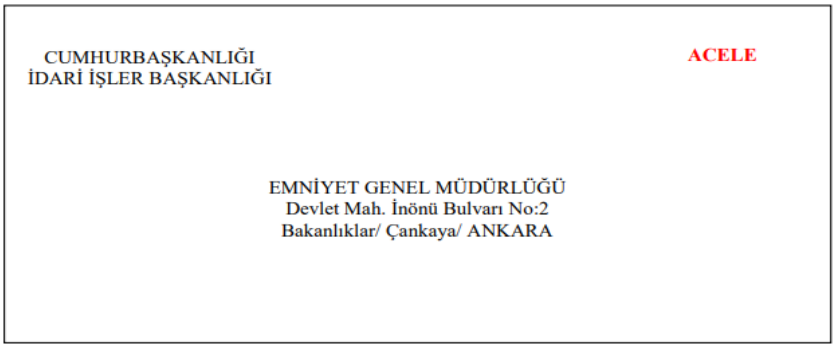
NOT: Çizelgenin bitiminde, Çok Gizli Belge Takip Kontrol Formu'nun arka yüzünden devam edilir.

Şekil 29. Çok Gizli Belge Takip Kontrol Formu Örneği (Gizlilik Dereceli Belgelerde…, 2022).

Belgeler iç içe çift zarf ile gönderilir. Zarf hazırlama usulü Şekil 30'da gösterilmiştir. Çok gizli gizlilik dereceli belge birinci zarfa konulur ve zarfın birleşim yerleri, zarfın yetkisiz kişiler tarafından açıldığının tespit edilmesini sağlayacak şekilde önemler alınarak kapatılır. Bu önlemler; zarfın birleşim yerlerinin el yazısıyla imzalanması ve kurum mührü ile mühürlenmesi sonrasında bu kısımların bant ile kapatılması yordamıyla yapılabilir. Sonrasında, birinci zarf ve hazırlanan iki nüsha Çok Gizli Belge Senedi ikinci zarfın içine konularak bu zarfın açıldığının tespiti amacıyla birinci zarfta belirtilen önlemler alınmaktadır.

İç Zarf Örneği

Dış Zarf Örneği



Şekil 30. Çok Gizli Gizlilik Dereceli Belge Zarf Örnekleri (Gizlilik Dereceli Belgelerde…, 2022).

“Kişiye Özel” bir gizlilik derecesi olmayıp, belgenin sadece ilgilisi tarafından görülebileceğini ifade etmektedir. Kişiye özel ibareli belge, belgeyi hazırlayan personelce birinci zarf kapalı olacak şekilde hazırlanan ikinci zarf ile birlikte Çok Gizli Belge Büro personeline teslim edilir. Bu belgelerin kayıt ve senet işlemleri birinci zarfta yer alan bilgilere göre yapılmaktadır.

Çok gizli gizlilik dereceli belgeler yurt içi veya yurt dışına posta ile gönderilememektedir. Bu belgeler kurumlarca tarafından yetkilendirilmiş kurye tarafından, muhatap idarenin Çok Gizli Belge Büro personeline elden teslim edilir. Kurye, belgelerin taşınmasının güvenliğinden sorumlu olup, belgeler ele geçirilemeyecek dayanıklılıkta mühürlü torbalarda veya şifreli ve kilitli çantalarda taşınması gerekmektedir.

5.2.8.3. Çok Gizli Gizlilik Dereceli Belgelerin Teslim Alınması ve Havale Edilmesi

Diğer kurumlardan kurye kanalıyla gelen çok gizli gizlilik dereceli belgeye ait Çok Gizli Belge Senedi'nin, çıkış kontrol numarasının, belgenin ve eklerinin sayfa sayısının kontrolü büro personeli tarafından yapılır. Bu kontrollerde eksik ve hatalı bir durum tespit edilmemiş ise Çok Gizli Belge Senedi'nin her iki nüshası imzalanır ve bu senedin biri büro personelinde kalır, diğeri ise kuryeye teslim edilir. Yapılan kontrollerde herhangi bir eksik ve hatalı durum tespit edildiğinde, bu durum hakkında tutanak düzenlenir ve belge söz konusu senetler imzalanmadan kuryeye teslim edilmektedir.

Büro personeli tarafından yapılan kontroller sonucunda teslim alınan belgelere yönelik kayıt işlemleri yapılır ve belgenin kurum içerisindeki hareketini kayıt altına almak için Çok Gizli Belge Takip Kontrol Formu hazırlanır. Kuruma gelen kişiye özel ibareli belgelerin kayıt işlemleri iç zarfı açılmadan Çok Gizli Belge Senedi'nde ve zarf üzerinde bulunan bilgilere gerçekleştirilir ve ilgili kişiye zimmetle teslim edilir.

Çok gizli gizlilik dereceli belgelerin havale işlemleri Çok Gizli Belge Bürosunca yapılır. Havale işlemlerinde kullanılan kontrol formu zimmet yerine geçmektedir. Çok gizli gizlilik dereceli belgelere sadece mesai saatleri içerisinde erişilmektedir. Belgeler, üzerinde yapılan işlemler tamamlanmasa bile mesai bitiminde güvenliğinin sağlanması maksadıyla Çok Gizli Belge Bürosuna teslim edilmesi gerekmektedir.

5.2.8.4. Çok Gizli Gizlilik Dereceli Belgelerin Muhafazası

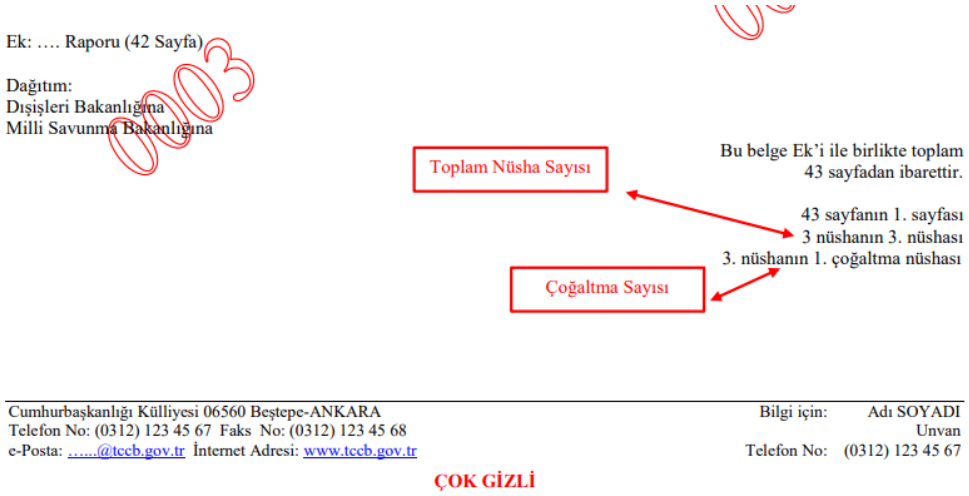
Gerekli kayıt ve havale işlemleri yapılan çok gizli gizlilik dereceli belgeler Çok Gizli Belge Bürosunda muhafaza edilir. İhtiyaç duyulduğunda, çok gizli gizlilik derecesine sahip ilgili personele teslim edilir. Belgenin incelenmesi Çok Gizli Belge Bürosunda veya büroca uygun görülen alanlarda yapılır. Kural olarak belgeler mesai bitiminde büroya teslim edilmesi gerekmekte olup, uzun süreli bir inceleme yapılması gerektiğinde 15 günden fazla olmamak kaydıyla üst yöneticinin veya talepte bulunan birim yöneticisinin onayının alınması gerekmektedir. Belge uzun süre olarak büro dışında bulunduğunda kilitli dolapta veya çelik kasada uygun güvenlik önlemleri alınarak saklanmalıdır. Belgeye erişime ait bilgiler kontrol formuna kayıt edilmektedir.

Büro personelinin görevlendirme, atama, emeklilik vb. gibi sebeplerle görevi sona erdiğinde, yeni personel ile yapılacak devir işlemleri “Çok Gizli Belge Devir-Teslim Tutanağı” düzenlenerek yapılmaktadır.

5.2.8.5. Çok Gizli Gizlilik Dereceli Belgelerin Çoğaltılması, Tercüme Edilmesi ve Alıntılanması

Çok gizli gizlilik dereceli belgeye yönelik çoğaltma, tercüme veya alıntılama işlemleri için belgeyi üreten kurumun üst yöneticisi veya birim yöneticisinden onay alınması gerekmektedir. Başka bir kuruma ait belgenin çoğaltılması, tercüme edilmesi veya alıntı yapılması ilgili kurumun izni ile yapılmaktadır.

Çok gizli gizlilik dereceli belgenin çoğaltma işlemi belgeyi muhafaza eden büro personeli tarafından, kablolu veya kablosuz ağ bağlantısı bulunmayan fotokopi cihazıyla yapılmaktadır. Çoğaltma işlemi tamamlandıktan sonra, çoğaltılan belgeye Şekil 31’de gösterildiği gibi çoğaltma sayısına ilişkin bilgiler yazılmalıdır. Belgenin türcüme veya alıntılı yapılma işlemi ise çok gizli gizlilik derecesiyle yetkilendirilmiş ilgili işlem personeli tarafından yapılmaktadır. Çoğaltma, türcüme ve alıntı işlemi kontrol formuna kayıt edilmektedir.



Şekil 31. Çoğaltılan Çok Gizli Gizlilik Dereceli Belgeye Çoğaltma Sayısının Verilmesi (Gizlilik Dereceli Belgelerde…, 2022).

5.2.8.6. Çok Gizli Gizlilik Dereceli Belgelerin Kontrolü

Belgelerin güvenliğine yönelik, belgenin hazırlanmasından imhasına kadar olan süreçte alınacak önlemlerin yanı sıra, Çok Gizli Belge Bürosu tarafından her yılın Ocak ayında belgelerin hareket kontrolünün ve belgenin gönderildiği muhatap idarelerde sayımının yapılması gerekmektedir. Sayım süreci şu şekilde yapılmaktadır (Gizlilik Dereceli Belgelerde…, 2022):

- Belgelerin dosya nüshaları ve muhatap idareye gönderilen nüshalarının sayımı için "Çok Gizli Belge Sayım Listesi" oluşturulur. Söz konusu listesi muhatap idare veya idarelere gönderilir. Muhatap idarelerin büroları tarafından sayım listesi üzerinden gerekli sayımlar yapılır, sayım sonuçları 15 gün içerisinde çok gizli gizlilik dereceli belgeyi çıkaran idareye gönderilir.
- Belgelerin sayımı ile beraber, idare tarafından hazırlanan ve başka bir idare ait belgelerin hareket kayıtları kontrol edilerek, süresi içerisinde teslim edilmeyen belgelerin büroya iade edilmesi istenir.
- İdare içinde ve muhatap idarede yapılan sayım tamamlandığında, Çok Gizli Belge Bürosu tarafından belgelerin güvenliğine yönelik bir ihlal tespit edildiğinde yönetmeliğin 21'inci maddesi gereği Araştırma Komisyonu kurulması için süreç başlatılır.
- Belgelerin sayım ve kontrol tamamlandığında bir rapor hazırlanır. Bu rapor üst yöneticiye, üst yöneticinin uygun görmesi halinde ise yetkilendirdiği yöneticiye arz edilir.

5.2.9. Gizli Gizlilik Dereceli Belgelerin Hazırlanması, Gönderilmesi, Teslim Alınması, Muhafaza Edilmesi, Çoğaltılması ve Tercüme Edilmesi

Gizli gizlilik dereceli belgeler, birim yöneticisinin oluruyla görevlendirilmiş personel tarafından, fiziki ortamlarda ve gerekli güvenlik önlemleri alınmış cihazlarla (bilgisayar, yazıcı vb.) hazırlanmaktadır.

Gizli gizlilik dereceli belgeler örneği Şekil 32'de gösterildiği gibi içi içe çift zarf yapılarak, belge yönetiminden sorumlu birim tarafından PTT kanalıyla gönderilmesi gerekmektedir. Zarfın birleşim yerleri, zarfın yetkisiz kişiler tarafından açıldığının tespit edilmesini sağlayacak şekilde önemler alınarak kapatılmaktadır.

İç Zarf

GİZLİ

CUMHURBAŞKANLIĞI İDARİ İŞLER BAŞKANLIĞI	
Tarih	
Sayı	

ACELE
KİŞİYE ÖZEL
Adı SOYADI

EMNİYET GENEL MÜDÜRLÜĞÜ
Devlet Mah. İnönü Bulvarı No:2
Bakanlıklar/ Çankaya/ ANKARA

GİZLİ

Dış Zarf

CUMHURBAŞKANLIĞI İDARİ
İŞLER BAŞKANLIĞI

ACELE

EMNİYET GENEL MÜDÜRLÜĞÜ
Devlet Mah. İnönü Bulvarı No:2
Bakanlıklar/ Çankaya/ ANKARA

Şekil 32. Gizli Gizlilik Dereceli Belge Zarf Örnekleri (Gizlilik Dereceli Belgelerde…,2022).

Teslim alınan belge iç zarfı açılmadan, zarfın üzerinde belirtilen bilgilerle kurumsal belge yönetim sistemine veya EBYS'ye kayıt edilir sonrasında ilgili yöneticiye teslim edilir. İlgili yönetici tarafından belgenin havale işlemleri yapılır. Belgelerin hava işlemleri Şekil 33'de gösterilen "Gizli Belge Zimmet Formu" ile yapılmaktadır.

GİZLİ BELGE ZİMMET FORMU ÖRNEĞİ

İDARE ADI:

SIRA NO.	GÖNDEREN İDARE/BİRİM	BELGE TARİHİ	BELGE SAYISI	ALICI	TESLİM TARİHİ	TESLİM ALAN ADI SOYADI İMZA

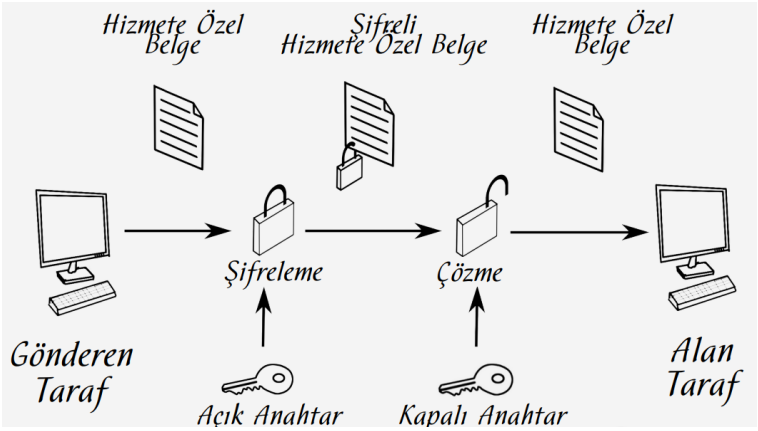
Şekil 33. Gizli Belge Zimmet Formu Örneği (Gizlilik Dereceli Belgelerde..., 2022).

Belgelerin yetkisiz kişilerin erişmesine imkan vermeyecek şekilde kilitli dolaplarda veya güvenli odalarda muhafaza edilmesi ve söz konusu odalarda yapılacak çalışmalarda belirtilen güvenlik önlemlerinin alınması gerekmektedir. Gizli gizlilik dereceli belgelerin tercüme ve çoğaltma işlemleri birim yöneticisinin onayından sonra yapılmaktadır.

Belgenin çoğaltılması kablolu veya kablosuz ağ bağlantısı bulunmayan fotokopi cihazıyla yapılmalıdır.

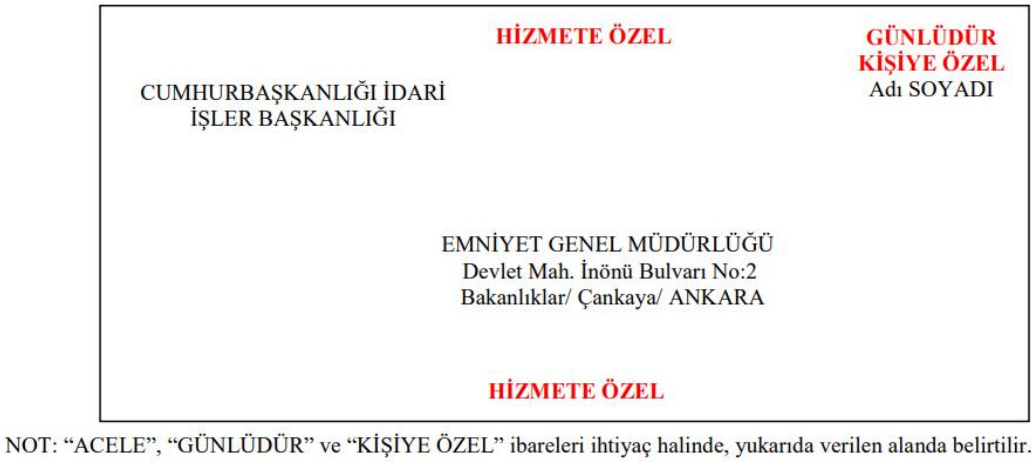
5.2.10. Hizmete Özel Gizlilik Dereceli Belgelerin Hazırlanması, Gönderilmesi, Teslim Alınması, Muhafaza Edilmesi ve Çoğaltılması

Hizmete özel gizlilik dereceli belgeler olağanüstü durumlar haricinde elektronik ortamda hazırlanır. Güvenli e-imza ile imzalanarak oluşturulan belge, e-Yazışma Teknik Rehberine göre kurumsal şifreleme sertifikası ile şifrelenerek ilgili idareye gönderilmektedir. Söz konusu şifreleme sürecinin doğru bir şekilde yapılabilmesi için belgenin gönderileceği muhatabın DETSİS'de bulunan ve yazışma yapılabilen birim olması gerekmektedir. KEP adresi sahibinin alıcı idare haricindeki başka bir idare olması durumunda, şifrenin açılamaması sebebiyle belge görüntülenemeyecektir. Örneğin, Ankara İl Emniyet Müdürlüğüne gönderilmesi gereken bir belgenin muhatabı İçişleri Bakanlığı seçildiğinde, Ankara İl Emniyet Müdürlüğüne iletilen belgenin şifresi sadece İçişleri Bakanlığı tarafından açılabilecek olması sebebiyle Ankara İl Emniyet Müdürlüğü belgeyi açamayacaktır. Hizmete özel gizlilik dereceli belgelenin elektronik ortamda gönderilmesi ve alınması Şekil 34'de gösterilmiştir.



Şekil 34. Hizmete Özel Gizlilik Dereceli Belgenin Elektronik Ortamda Gönderilme ve Alınması (Gizlilik Dereceli Belgelerde…, 2023).

Olağanüstü durumlarda fiziki ortamda hazırlanan, elektronik ortamla hazırlanan fakat muhataba elektronik olarak gönderilemeyen veya kişiye özel ibareli belgeler Şekil 35'de örneği gösterilen tek zarf usulü PTT kanalıyla gönderilmektedir. Zarfın birleşim yerleri, zarfın yetkisiz kişiler tarafından açıldığının tespit edilmesini sağlayacak şekilde önemler alınarak kapatılması gerekmektedir.



Şekil 35. Hizmete Özel Gizlilik Dereceli Belge Zarf Örneği (Gizlilik Dereceli Belgelerde… , 2022).

Hizmete özel gizlilik dereceli belgeler esas olarak elektronik ortamda (EBYS) teslim alınmasının yanı sıra, olağanüstü durumlarda (el yazısıyla imzalanmış) ve elektronik iletimin mümkün olmadığı durumlarda (güvenli e-imzalı) fiziki ortamlarda da teslim alınmaktadır. EBYS ile gelen belgeler, kurumsal şifreleme sertifikasıyla açılarak ilgili birimlere havale edilmektedir. Olağanüstü durumlar sebebiyle fiziki ortamlarda hazırlanmış, el yazısıyla imzalanmış ve fiziki olarak gelen belge, dijitalleştirilerek EBYS'ye kaydedilmekte ve sonrasında ilgili birimlere havale edilmektedir. EBYS'de hazırlanan ve güvenli e-imzalı olan fakat elektronik iletimin mümkün olmadığı durumlarda fiziki olarak teslim alınan belgenin güvenli e-imzalı nüshasına e-Devlet'ten ulaşılmakta, EBYS'ye ithal edilmekte, şifreleme sertifikasıyla açılmakta, EBYS'ye kayıt edildikten sonra ilgili birimlere havalesi yapılmaktadır.

Olağanüstü durumlarda fiziki ortamda hazırlanan hizmete özel gizlilik dereceli belgelere yönelik gizli gizlilik dereceli belgelerde uygulanan muhafaza ve güvenlik önlemleri uygulanması gerekmektedir. Elektronik ortamda bulunan hizmete özel gizlilik dereceli belgeler, EBYS'de şifreli ya da kriptolu olarak muhafaza edilmesi gerekmektedir. Ayrıca, hizmete özel gizlilik dereceli belgelerin işlendiği ve muhafaza edildiği alanlarda (veri merkezleri, veri tabanları, sunucular, sistem odaları) hakkında yayma güvenliği (TEMPEST) önlemleri alınması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2023).

EBYS'lerin veri depolama ve uygulamalarına ilişkin kullanılan sunucuların yurt içinde bulunan alanlarda olması, EBYS'deki belgelere ilişkin tüm verilerin düzenli olarak

yedeklenmesi ve kesintisiz olarak hizmet verilebilmesi için gerekli önlemlerin alınması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2023, s. 44).

5.2.11. Gizli ve Hizmete Özel Gizlilik Dereceli Belgelerin Kurum Arşivine Devredilmesi

Belgeler mevcut gizlilik dereceleriyle ya da gizlilik dereceleri kaldırılarak kurum arşivine devredilebilmektedir (Gizlilik Dereceli Belgelerde…, 2023, s. 49). Belgelerin Değerlendirme Komisyonu tarafından inceleme yapılmadan arşive devredilmesi bilgi edinme hakkının kullanımını ve sürecini olumsuz etkilemekte birlikte, kamuoyunca bilinen süreçlere ilişkin belgelerin arşivlerde gizlilik derecesine sahip olarak bulunmasına, arşivlerde alınacak güvenlik önlemlerinin artmasına, gereğinden fazla insan gücüne ve maliyete neden olabilmektedir. Bu sebeple, söz konusu belgelerin, Değerlendirme Komisyonu tarafından incelenmesi ve gizlilik derecesinin kaldırılmasına karar verilenler için gerekli işlemler yapıldıktan sonra kurum arşivine devredilmesi yerinde olacaktır.

Gizli ve hizmete özel gizlilik dereceli belgeler, sahip oldukları gizlilik derecesine göre alınacak önemlerle birlikte kurum arşivinin yetkili personeline teslim edilmektedir. Kurum arşivine devri yapılan belgeler için gerekli güvenlik tedbirleri alınmakta ve yetkisiz personelin arşivde muhafaza edilen belgelere erişiminin engellenmesi sağlanmaktadır.

6. BÖLÜM

BULGULAR VE DEĞERLENDİRME

Araştırmanın bu bölümünde, kuramsal bölümlerde ele alınan veri, bilgi ve belgelerin gizlilik nedenleri, gizlilik dereceleri, gizlilik süresi ile gizlilik sınıflandırması yapılabilecek belge türleri, gizlilik dereceli belgelerin yönetimi ve güvenliği kapsamında Tablo 9'da yer alan araştırma belgelerinden elde edilen bulgulara ve değerlendirmelere yer verilmiştir.

Tablo 9. Araştırma Kapsamında İncelenen Belgeler

Belge Türü	Belge Adı	Belge Kodu
Kanunlar	651 Sayılı Devlet Memurları Kanunu (1965)	Kanun-1
	4982 Sayılı Bilgi Edinme Hakkı Kanunu (2003)	Kanun-2
	5271 Sayılı Ceza Muhakemesi Kanunu (2004)	Kanun-3
	5070 Sayılı Elektronik İmza Kanunu (2004)	Kanun-4
	5809 Sayılı Elektronik Haberleşme Kanunu (2008)	Kanun-5
	6698 Sayılı Kişisel Verilerin Korunması Kanunu (2016)	Kanun-6
	7315 Sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu (2021)	Kanun-7
Kararname	Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi (2018)	Kararname-1
Genelgeler	Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (2019)	Genelge-1
	E-Yazışma Projesi Hakkındaki Başbakanlık Genelgesi (Genelge No: 2017/21)	Genelge-2
Yönetmelikler	Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik (2021)	Yönetmelik-1
	Devlet Arşiv Hizmetleri Hakkında Yönetmelik (2019)	Yönetmelik-2
	Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022)	Yönetmelik-3
	Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik (2022)	Yönetmelik-4
	Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2020)	Yönetmelik-5
	Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2006)	Yönetmelik-6
Yönerge	Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi (2023)	Yönerge-1
Rehber	Bilgi ve İletişim Güvenliği Rehberi (2020)	Rehber-1
Standartlar	NFPA 75 Bilgi Teknolojisi Ekipmanları Koruma Standardı (2020)	Standart-1
	NFPA 232 Belge Koruma İçin Standart (2022)	Standart-2
	ISO/IEC 27001:2022 Bilgi Güvenliği, Siber Güvenlik ve Kişisel Gizliliğin	Standart-3

Korunması-Bilgi Güvenliği Yönetim Sistemleri–Gereklilikler	
ISO/IEC 27002:2022 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması-Bilgi Güvenliği Kontrolleri	Standart-4
ISO 15489-1:2016 Bilgi ve Dokümantasyon-Belge Yönetimi Standardı	Standart-5
ISO 30300:2020 Bilgi ve Dokümantasyon-Belge Yönetim Sistemi-Temel İlkeler ve Sözlükler	Standart-6
ISO 30301:2019 Bilgi ve Dokümantasyon-Belgeler için Yönetim Sistemleri– Gereklilikler	Standart-7
ISO 30302:2022 Bilgi ve Dokümantasyon-Belgeler için Yönetim Sistemleri-Uygulama Rehberleri	Standart-8
TS 13298:2015 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı	Standart-9
TSE K 523:2016 Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri	Standart-10
TOPLAM	**28**

6.1. GİZLİLİK SÜREÇLERİNE İLİŞKİN BULGULAR VE DEĞERLENDİRME

Veri, bilgi ve belgelerin gizlilik süreçleri kapsamında incelenen araştırma belgelerinden elde edilen bulgular belge türlerine göre Tablo 10'da gösterilmiştir. Gizlilik süreçleri bileşeninin alt kategorilerine bulgular ve değerlendirmeler alt başlıklar altında sunulmaktadır.

Tablo 10. Araştırma Kapsamında İncelenen Belgelerde Gizlilik Süreçlerine Ait Kavramların Geçme Sıklığı

Gizlilik Süreçleri Bileşeni Kategorileri	**Belge Türü**	**Geçme Sıklığı**	
		N	**%**
Gizlilik Nedenleri	Kanunlar	5	22,7
	Kararname	0	0,0
	Genelgeler	1	4,5
	Yönetmelikler	2	9,1
	Yönerge	1	4,5
	Rehber	1	4,5
	Standartlar	2	9,1
Gizlilik Sınıflandırma Düzeyleri	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	1	4,5
	Yönetmelikler	2	9,1
	Yönerge	1	4,5
	Rehber	1	4,5
	Standartlar	2	9,1
Sınıflandırılabilecek Veri, Bilgi ve Belge Türleri	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	1	4,5
	Yönerge	0	0,0
	Rehber	0	0,0

	Standartlar	0	0,0
Sınıflandırma Yetkileri	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	1	4,5
	Yönerge	0	0,0
	Rehber	0	0,0
	Standartlar	0	0,0
Gizlilik Süresi	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	0	0,0
	Yönerge	0	0,0
	Rehber	0	0,0
	Standartlar	0	0,0
Gizliliğinin Değerlendirilmesi	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	1	4,5
	Yönerge	0	0,0
	Rehber	0	0,0
	Standartlar	0	0,0
Toplam		**22**	**100**

6.1.1. Gizlilik Nedenleri ile Gizlilik Düzeylerine İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerin 12'sinde veri, bilgi ve belgelerin gizliliğine yönelik farklı kavramlara yer verildiği görülmüştür. Gizlilik nedenleri olarak tespit edilen kavramlar ile bu kavramların varlık bulduğu yasal ve idari düzenlemeler ile standartlar Tablo 11'de sunulmaktadır.

Tablo 11. Gizlilik Nedenlerine İlişkin Kavramlar

Gizlilik Nedenleri	**Belge Kodu**
Milli Güvenliğin ve Savunmanın Sağlanması	Kanun-2 Kanun-3 Kanun-7 Genelge-2 Yönetmelik-3 Yönerge-1 Rehber-1 Standart-9
Devletin Dış İlişkilerinin Korunması	Kanun-2 Kanun-3 Yönetmelik-3 Yönerge-1
Milli Menfaatlerin Korunması	Genelge-2 Yönetmelik-3 Yönerge-1 Rehber-1 Standart-9
Kamu Düzeninin ve Güvenliğinin Sağlanması	Kanun-7 Yönetmelik-3

	Yönerge-1 Standart-9
Ekonomik Güvenliğinin Sağlanması	Kanun-7
Özel Hayatın Gizliliğinin Korunması	Kanun-2 Kanun-3 Kanun-5 Kanun-6
İstihbarat Faaliyetlerinin Gizliğinin Sağlanması	Yönetmelik-3
Teknoloji Faaliyet ve Menfaatlerin Korunması	Yönetmelik-3
Haberleşmenin Gizliliğinin Sağlanması	Kanun-2
Ticari Sırların Korunması	Kanun-2
Gerçek veya Tüzel Kişilerin Güvenliğinin Sağlanması	Genelge-2 Yönetmelik-3 Yönerge-1
Adli ve İdari Soruşturmanın Gizliliğinin Sağlaması	Yönetmelik-3
Kişisel Verilerin Korunması	Kanun-3 Kanun-5 Kanun-6 Kanun-7 Genelge-2

Tablo 11'de sunulan gizlilik nedenleri kapsamında veri, bilgi ve belgelere yetkisiz erişimlerin engellenmesi amacıyla gizlilik sınıflandırması yapılmaktadır. Araştırma kapsamında incelenen belgelerin 7'sinde farklı hassasiyetlik düzeylerinde gizlilik derecelerinin belirlendiği görülmüştür. Gizlilik dereceleri ve bu gizlilik derecelerinin kullanıldığı varlıklar Tablo 12'de sunulmaktadır.

Tablo 12. Veri, Bilgi ve Belgelerde Kullanılan Gizlilik Dereceleri

Belge Adı	**Gizlilik Dereceleri**	**Gizlilik Derecelerinin Kullanıldığı Varlıklar**
E-Yazışma Projesi Hakkındaki Başbakanlık Genelgesi (Genelge No: 2017/21)	• Çok Gizli • Gizli • Özel • Hizmete Özel	• Mesaj • Doküman
Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022)	• Çok Gizli • Gizli • Hizmete Özel	• Belge
Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2006)	• Gizli	• Veri
Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi (2023)	• Çok Gizli • Gizli • Özel • Hizmete Özel	• Bilgi • Belge • Malzeme • Proje
Bilgi ve İletişim Güvenliği Rehberi (2020)	• Çok Gizli • Gizli • Özel • Hizmete Özel • Kritik Bilgi/Veri	• Veri
TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı (2015)	• Çok Gizli • Gizli • Özel • Hizmete Özel • Tasnif Dışı	• Bilgi • Belge • Evrak • Mesaj • Doküman
TSE K 523 Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri (2016)	• Çok Gizli	• Fiziksel/Elektronik Bilgi

	• Gizli • Özel • Hizmete Özel • Ticari Gizli • Ticari Özel • Kişiye Gizli • Kişiye Özel • Tasnif Dışı	Varlıkları • Yazılım Bilgi Varlıkları • İnsan • Soyut Değerler (İtibar, İmaj Vb.) • Hizmetler • Projeler

Veri, bilgi ve belgelerinin gizlilik düzeylerine göre standart şekilde sınıflandırmasının amacının veri, bilgi ve belgeleri farklı güvenlik düzeylerinde ilgili gizlilik derecesiyle ilişkilendirerek bunların muhafaza, güvenlik, erişim ve iş süreci yönetimlerinin tutarlı bir şekilde sürdürülmesi olduğu görülmüştür. Bu bağlamda, farklı yasal ve idari düzenlemeler ile standartların kapsamı içerisinde çeşitli gizlilik düzeyleri belirlenmiştir.

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022) ile belirlenen gizlilik dereceleri sadece kamu kurum ve kuruluşlarında oluşturulan veya sağlanan belgelerin güvenliğine yönelik kullanılmaktadır. Bu kapsamda belgeler taşıdıkları güvenlik ağırlıklarına göre ilgili gizlilik derecesiyle ilişkilendirilmekte olup, fiziki veya elektronik ortamlarda yönetilmektedir.

Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2006) ile belirlenen gizlilik sınıflandırılmasıyla kurum kapsamında sahip olunan verilerin kişisel bilgilerin tespitinin önlenmesi amaçlanmakta olup, bunların istatistiki amaçlarla kullanımına ilişkin düzenlemeler yapılmıştır.

Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi'nde (2023) belirtilen gizlilik dereceleri savunma sanayii kapsamında kamu kurum ve kuruluşları ile savunma sanayinde faaliyet gösteren paydaşlar tarafından kullanılmaktadır. Bu gizlilik dereceleri bilgi, belge, malzeme ve projeler ile ilişkilendirilerek gerekli güvenlik önlemlerinin alınması amaçlanmıştır.

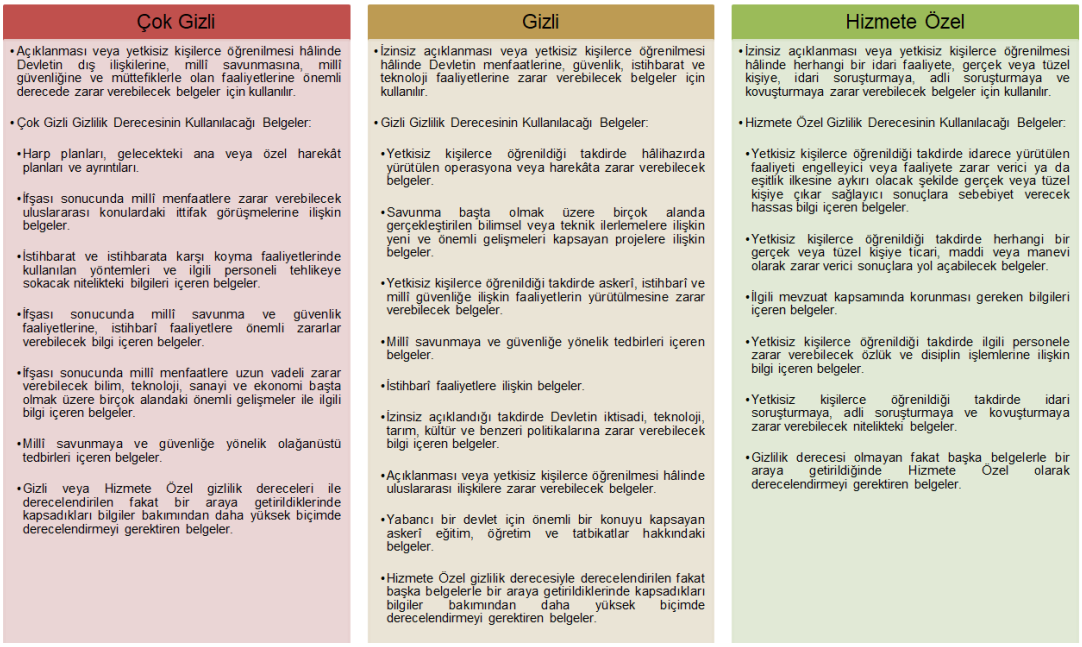
Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nin (2019) gereği oluşturulan Bilgi ve İletişim Güvenliği Rehberi'nde (2020) kamu kurum ve kuruluşları ile kritik altyapı hizmeti sağlayan işletmeler tarafından veri/bilgi güvenliğine yönelik kullanılacak gizlilik dereceleri belirlenmiştir. Rehberde veri/bilgiler farklı güvenlik düzeylerinde gizlilik dereceli veri/bilgi ve kritik veri/bilgi olarak kategorize edilmiştir.

TS 13298 standardı çerçevesinde, EBYS'deki erişim haklarının farklı güvenlik düzeylerine göre düzenlemesi amacıyla bilgi, belge, evrak, mesaj ve dokümanlara yönelik farklı gizlilik dereceleri belirlenmiştir.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığının KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliği (2017) gereği, kamu kurum ve kuruluşlarının KamuNET sanal ağına entegrasyonu çerçevesinde bilgi varlıklarına ilişkin gizlilik sınıflandırılmasının TSE K 523 Kriterine göre yapılması gerekmektedir. Bu sınıflandırma kriterinde bilgi varlıkları ile bu bilgi varlıklarıyla ilişkilendirilecek gizlilik dereceleri tanımlanmıştır.

6.1.2. Sınıflandırılabilecek Veri, Bilgi ve Belge Türlerine İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerin 1'inde (Gizlilik Dereceli Belgelerde…, 2022) nesnel ölçütlerle gizlilik sınıflandırması yapılmasına yönelik belge türlerinin belirlendiği görülmüştür. Bu bağlamda, belge yönetim süreçlerinde kullanılabilecek gizlilik dereceleri ve bu gizlilik derecelerinin kullanıldığı belgeler Şekil 36'da gösterilmiştir.



Şekil 36. Gizlilik Derecelerinin Kullanıldığı Belgeler (Gizlilik Dereceli Belgelerde…, 2022)

Kamu kurum ve kuruluşlarının iş süreçleri ve faaliyetlerinde üretilen veya sağlanan veri ve bilgilerin güvenliğine yönelik gizlilik derecelerinin net bir tanımının yapılması, hangi gizlilik derecelerinin hangi veri ve bilgilerle ilişkilendirileceğine yönelik nesnel ölçütlerin belirlenmesinin gerektiği değerlendirilmektedir.

6.1.3. Gizlilik Sınıflandırması ve Yetkilendirmesi Yapmaya Yetkili Makam ve Kişilere İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerden sadece 1'inde (Gizlilik Dereceli Belgelerde…, 2022) gizlilik sınıflandırması ve yetkilendirmesi yapmaya yetkili makam ve kişiler belirlenmiştir. Kamu kurum ve kuruluşlarında belgelere gizlik sınıflandırması yapan ve personeli gizlilik düzeyi ile yetkilendiren makam ve kişiler Tablo 13'de sunulmaktadır.

Tablo 13. Gizlilik Sınıflandırması ve Yetkilendirmesi Yapan Makam ve Kişiler

Gizlilik Derecesi	Belgeye Gizlilik Derecesi Vermeye Yetkili Makam/Kişi	Personeli Gizlilik Düzeyi ile Yetkilendirecek Makam/Kişi
Çok Gizli	Üst Yönetici	Üst Yönetici
Gizli	Birim Yöneticisi	Birim Yöneticisi
Hizmete Özel	Birim veya Alt Birim Yöneticisi	Birim veya Alt Birim Yöneticisi

Yetkisiz erişimlerin önlenmesi maksadıyla yapılan gizlilik sınıflandırması ile erişim yetkisi verilecek personelin yetkilendirilmesi aynı makam ve kişiler tarafından yapılmaktadır. Bu bağlamda, söz konusu sınıflandırma ve yetkilendirmelerin bilmesi gereken prensibi temelinde şekillendiği görülmüştür. Ayrıca, belgelerin hassasiyetlik derecelerindeki farklılık yetkili makam ve kişi düzlemlerine de yansımıştır.

6.1.4. Gizliliğin Süresi ve Değerlendirilmesine İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerde gizlilik sürelerinin en fazla ne kadar olacağı hakkında kesin ifadeye yer verilmemiştir. Bununla birlikte, Türkiye'de gizlilik dereceli belgelere yönelik gizlilik süresinin belirlenmesi ve değerlendirilmesi kapsamında süreli gizlilik yöntemi ve komisyon yapılarının oluşturulduğu görülmüştür (Gizlilik Dereceli Belgelerde…, 2022).

Süreli gizlilik uygulaması ile belgelerin gizlilik durumun sona ereceği zamana veya olaya yönelik kararlar belgelerin üretilmesi sırasında verilmektedir. Belirlenen zamana gelindiğinde veya olay gerçekleştiğinde/sona erdiğinde söz konusu gizlilik derecesi düşürülmekte, kaldırılmakta ya da gizlilik dereceli belge imha edilmektedir. Süreli gizlilik uygulaması kapsamında belirlenecek gizlilik süresinin en fazla kadar olacağı veya olay hakkında nesnel ölçütün ne olacağı ifade edilmemiştir.

Belgelerin gizlilik süresinin değerlendirildiği diğer bir yöntem ise, gizlilik dereceli belgeyi üreten kamu kurum ve kuruluşu tarafından oluşturulan Gizlilik Dereceli Belgeleri Değerlendirme Komisyonlarıdır (Gizlilik Dereceli Belgelerde… Yönetmelik, 2022). Söz konusu komisyonların oluşturulma yapısı, toplanma zamanları ile verebilecekleri kararlar Tablo 14'de gösterilmiştir.

Tablo 14. Gizlilik Dereceli Belgeleri Değerlendirme Komisyonlarının Yapısı

Komisyonun	**Çok Gizli Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu**	**Gizli ve Hizmete Özel Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu**
Yapısı	• Belgeyi üreten kurum bünyesinde toplanmaktadır. • En az üç üyeden oluşmaktadır. 1. Başkan: İdarenin en üst yöneticisi veya yetki vereceği yönetici. 2. Üye: Belgeyi hazırlayan birimden bir yönetici. 3. Üye: Belgeyi hazırlayan birimden işlem personeli.	• Belgeyi üreten kurum bünyesinde toplanmaktadır. • En az üç üyeden oluşmaktadır. 1. Başkan: Belge sahibi birim yöneticisi veya yetki vereceği yönetici. 2. Üye: Belgeyi hazırlayan alt birimden bir yönetici. 3. Üye: Belgeyi hazırlayan alt birimden bir personel.
Toplanma Zamanı	• Sonu çift rakamla biten yıllarda toplanmaktadır. • Belgeyi üreten birim veya sahip olan kurumun teklifi üzerine olağanüstü olarak toplanabilmektedir.	• İdarenin belirleyeceği zamanlarda toplanmaktadır. • Belgenin kurum arşivine devredilmesi durumunda olağanüstü olarak toplanabilmektedir.
Verebileceği Kararlar	• Gizliliğin Devamı • Gizliliğin Düşürülmesi (Sadece gizli) • Gizliliğin Kaldırılması • Belgenin İmhası	• Gizliliğin Devamı • Gizliliğin Kaldırılması

6.2. GİZLİLİK DERECELİ BELGELERİN YÖNETİMİNE İLİŞKİN BULGULAR VE DEĞERLENDİRME

Gizlilik dereceli belgelerin yönetimi kapsamında incelenen araştırma belgelerinden elde edilen bulgular belge türlerine göre Tablo 15'de gösterilmiştir. Gizlilik dereceli belgelerin yönetimi bileşeninin kategorilerine ait bulgular ve değerlendirmeler alt başlıklar altında sunulmaktadır.

Tablo 15. Araştırma Kapsamında İncelenen Belgelerde Gizlilik Dereceli Belgelerin Yönetimine İlişkin Kavramların Geçme Sıklığı

Gizlilik Dereceli Belgelerin Yönetimi Bileşeni Kategorileri	**Belge Türü**	**Geçme Sıklığı**	
		N	**%**
Gizlilik Dereceli Belgelerin Yönetimiyle İlişkili Yapılar	Kanunlar	1	5,9
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	3	17,6
	Yönerge	0	0,0
	Rehber	0	0,0
	Standartlar	0	0,0
Gizlilik Dereceli Belge Süreçleri	Kanunlar	2	11,8
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	3	17,6
	Yönerge	1	5,9
	Rehber	0	0,0
	Standartlar	5	29,4
Belge Süreçlerinin Gerçekleştirileceği Ortamlar	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	2	11,8
	Yönerge	0	0,0
	Rehber	0	0,0
	Standartlar	0	0,0
Toplam		**17**	**100**

6.2.1. Gizlilik Dereceli Belgelerin Yönetimi ile İlişkili Olan Yapılara Ait Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerin 4'ünde gizlilik dereceli belgelerin yönetimi ile ilişkili olan yapıların oluşturulduğu görülmüştür. Bu yapılar, gizlilik dereceli birimler, Çok Gizli Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu, Gizli ve Hizmete Özel Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu, Arşiv Belgesi Gizlilik Değerlendirme Komisyonu ve Bilgi Edinme Değerlendirme Kurulu'dur.

Kamu kurum ve kuruluşlarında gizlilik dereceli belgeyi üreten veya gizlilik dereceli belgeye sahip olan kurum ve kuruluşlarda, gizlilik dereceli birimlerin neler olduğu Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik'te (2022) belirtilmiştir. Bu yönetmeliğe göre, çok gizli ve gizli gizlilik dereceli bilgi ve belgeleri üreten ve koruyan birimler, bilgi işlem birimleri, teftiş ve denetim birimleri, personel birimleri, özel kalem müdürlükleri gizlilik dereceli birimlerdir. Yönetmelik, gizlilik dereceli birimlerde görev yapacak kişiler için güvenlik soruşturması ile arşiv araştırmasının eş zamanlı yapılmasını zorunlu kılmaktadır.

Çok Gizli Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu belgeyi üreten kamu kurum ve kuruluşları tarafından oluşturulmaktadır. Komisyon biri başkan olmak üzere en az üç kişiden oluşmakta olup, olağanüstü durumlar haricinde sonu çift yıllarda toplanarak geçmiş yıllarda üretilen çok gizli gizlilik dereceli belgelere ilişkin gizlilik derecesinin değerlendirilmesi ile bu gizliliğin düşürülmesi, kaldırılması veya belgenin imha edilmesine yönelik karar alabilmektedir. Komisyonun kararlarına ilişkin işlemler Çok Gizli Belge Bürosu tarafından yerine getirilmektedir (Gizlilik Dereceli Belgelerde…, 2022).

Gizli ve Hizmete Özel Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu belgeyi üreten kamu kurum ve kuruluşları tarafından oluşturulmaktadır. Komisyon biri başkan olmak üzere en az üç kişiden oluşmakta olup olağanüstü durumlar haricinde (belgelerin kurum arşivine devri) kurum ve kuruluşun belirlediği zaman periyodunda toplanarak gizli veya hizmete özel gizlilik dereceli belgelere ilişkin gizlilik derecesinin değerlendirilmesi ile bu gizliliğin devam etmesi veya gizliliğin kaldırılmasına yönelik karar alabilmektedir. Komisyonun kararlarına yönelik işlemler belge sahibi birim tarafından yerine getirilmektedir (Gizlilik Dereceli Belgelerde…, 2022).

Arşiv Belgesi Gizlilik Değerlendirme Komisyonu Devlet Arşivleri Başkanlığı tarafından oluşturulmaktadır. Komisyon biri başkan olmak üzere en az beş kişiden oluşmakta olup, Devlet Arşivleri Başkanlığında bulunan gizlilik dereceli arşiv belgelerinin araştırmaya açılması kapsamında, belgelerin gizlilik niteliğinin değerlendirilmesi ve uygun görülmesi halinde bu belgelerin gizliliklerinin kaldırılması kararı alabilmektedir. Komisyonun aldığı kararlar Devlet Arşivleri Başkanının onayı sonrası kesinleşmektedir (Arşivlerden Yararlanma Usul…, 2021).

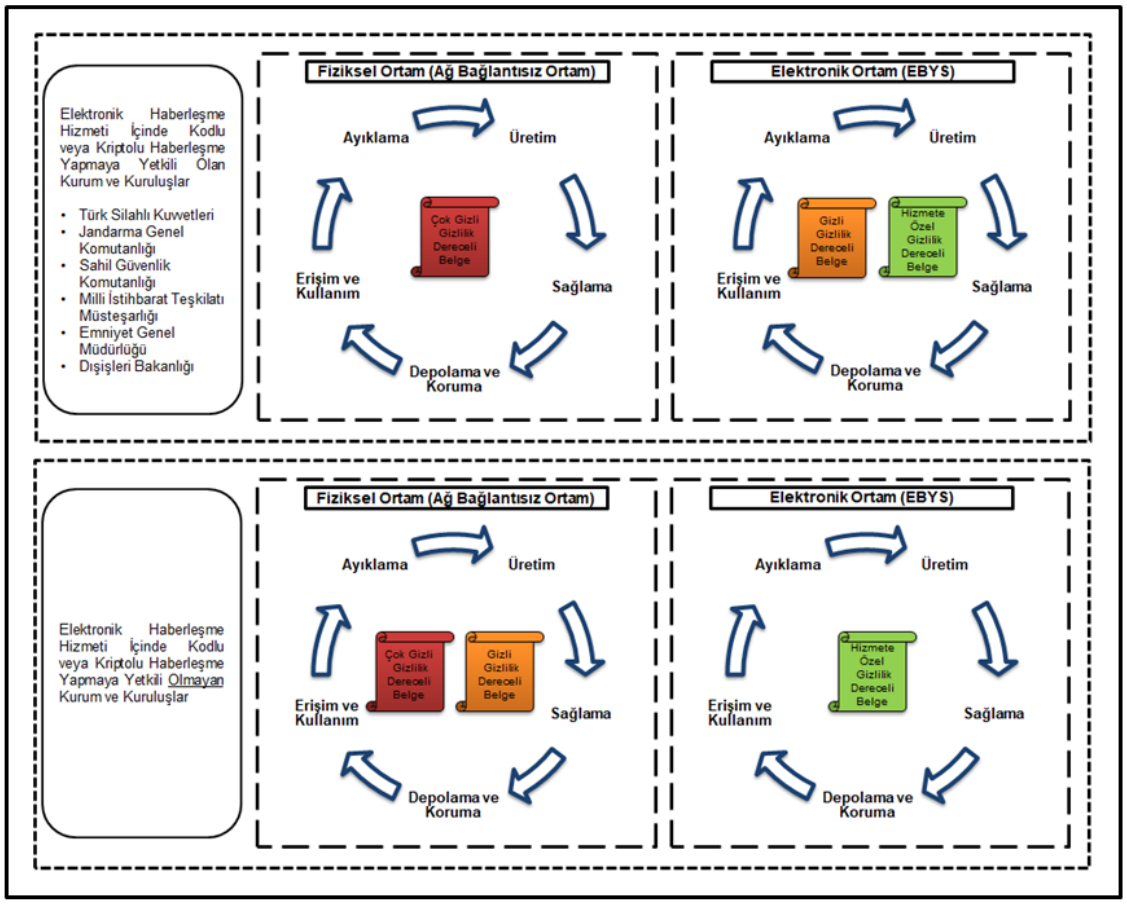
Bilgi Edinme Hakkı Kanunu (2003, mad. 14) gereği oluşturulan Bilgi Edinme Değerlendirme Kurulu Adalet Bakanlığı koordinesinde bulunmakta olup, Cumhurbaşkanı tarafından atanan dokuz üyeden meydana gelmektedir. Kurul, bilgi edinme talebi kabul edilmeyen kişilerin yapacakları itirazlara yönelik (yargı yoluna başvurmadan ikinci bir seçenek olarak) ilgili kurumun kararlarını değerlendirmekte ve ilgili kurumu bağlayıcı kararlar verebilmektedir. Söz konusu kararlar itirazın kabulü, reddi, kısmen kabulü veya kısmen reddi yönünde olabilmektedir (Bilgi Edinme Değerlendirme Kurulu, 2023b).

6.2.2. Gizlilik Dereceli Belgelerin Yönetim Süreçlerine ve Ortamlarına İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerin 13'ünde gizlilik dereceli belgelerin yönetim süreçlerine ve ortamlarına yönelik düzenlemelerin yapıldığı görülmüştür. Türkiye'de özel güvenlik gerektiren belgelerin yönetimine yönelik yapılan yasal ve idari düzenlemeler ile geliştirilen uygulamalar doğrultusunda, belgelere, içerdikleri bilgilerin hassasiyetliklerine göre gizlilik sınıflandırılması yapılmaktadır. Bu sınıflandırmayla, bir gizlilik derecesine sahip olan belgenin yönetim süreçleri ile güvenlik ve erişim düzenlemelerine yönelik standart uygulamalar geliştirilmiştir. Gizlilik sınıflandırılması yapılmayan belgelere yönelik bilmesi gereken prensibi uygulanmaktadır (Gizlilik Dereceli Belgelerde…, 2022, mad. 31). Bilmesi gereken prensibi, yalnızca işlerinin bir parçası olarak belgelere erişim sağlayabilen, belgeleri inceleyen, değerlendiren ve korumaktan sorumlu olan kişileri kapsamaktadır (Güvenlik Soruşturması, 2022, mad. 4). Gizlilik sınıflandırılması yapılmayan, fakat özel güvenlik gerektiren belgelerin (hukuki belgeler ile kişisel bilgileri içeren sağlık belgeleri, eğitim belgeleri, mali belgeler vb.) yönetimine ilişkin standart uygulamalar ile politikalar geliştirilmemiştir.

Gizlilik dereceli belgelerin yönetimi, belgelerin taşıdıkları gizlilik derecesine göre fiziksel ya da elektronik ortamlarda farklı güvenlik esaslarına göre yürütülmektedir. Hizmete özel gizlilik dereceli belgelerin yönetimi elektronik ortamlarda diğer gizlilik dereceli belgelerin yönetimi ise fiziki ortamlarda gerçekleştirilmektedir (Resmi Yazışmalarda…Yönetmelik, mad. 25, 2020). Bununla birlikte, Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik'e göre (2010) elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili

olanlar tarafından gerekli güvenlik önlemlerinin alınması koşuluyla, güvenli e-imza ile onaylanan gizlilik dereceli belgelerin elektronik ortamda da gönderebileceği ifade edilmektedir (Resmi Yazışmalarda…Yönetmelik, mad. 31, 2020). Bu bağlamda, Türkiye'de gizlilik dereceli belgelerin yönetimi konusunda kurum ve kuruluşlar arasında farklılıklar bulunmaktadır. Her bir kurum ve kuruluşta, gizlilik dereceli belgelerin yönetimi farklı ortamlarda (fiziksel ve elektronik ortam) yürütülmektedir. Türkiye'de kurum ve kuruluşlar düzlemlerinde belgelerin yaşam döngüsü boyunca gizlilik derecelerine göre yönetileceği ortamlar Şekil 37'de gösterilmiştir.



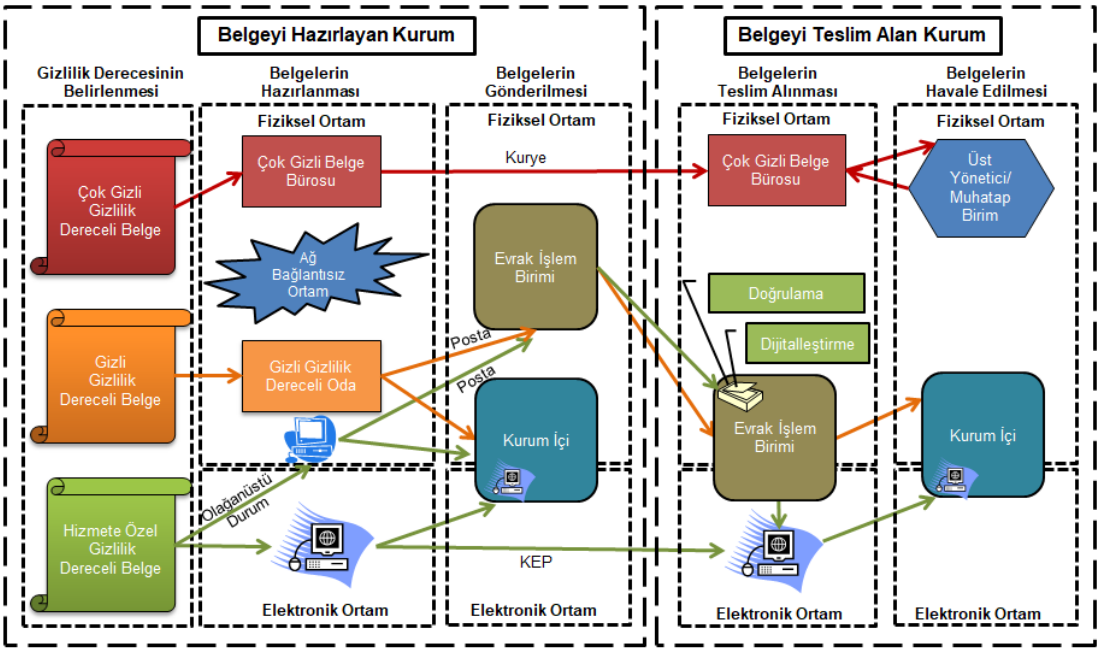
Şekil 37. Kurum ve Kuruluş Düzlemlerinde Gizlilik Dereceli Belgelerin Yönetildiği Ortamlar

Çok gizli gizlilik dereceli belgelerin yönetimi bu amaçla özel olarak oluşturulmuş Çok Gizli Belge Bürosu koordinatörlüğünde, gizli gizlilik dereceli belgelerin yönetimi gerekli güvenlik önlemleri alınan fiziki ortamlarda, hizmete özel gizlilik dereceli belgelerin yönetimi ise olağanüstü durumlar haricinde sadece elektronik ortamda (EBYS)

yürütülmektedir (Elektronik İmza Kanunu, 2004; Gizlilik Dereceli Belgelerde…, 2022; Resmi Yazışmalarda…Yönetmelik, 2020).

Olağanüstü durumlarda fiziksel olarak hazırlanan ve gönderilen hizmete özel gizlilik dereceli belgeler muhatap kurum tarafından dijitalleştirilerek kurumun EBYS'sine ithali sağlanmakta ve elektronik olarak ilgili birimlere havale edilmektedir. EBYS'de hazırlanan ve güvenli e-imzalı olan fakat elektronik iletimin mümkün olmadığı durumlarda belgeyi fiziksel olarak teslim alan muhatap kurum belgenin güvenli e-imzalı nüshasına e-Devlet üzerinden ulaşması, kurumun EBYS'sine dahil etmesi, şifreleme sertifikasıyla açması, EBYS'ye kaydederek ilgili birimlerine havale etmesi gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022).

Gizlilik dereceli belgelerin farklı güvenlik düzeylerinde yönetilmesi kurum ve kuruluşlarda hibrit bir belge yönetim süreçleri ortaya çıkarmıştır. Gizlilik dereceli belgeler taşıdıkları gizlilik derecelerine göre ilgili süreçlerde varlık bulmaktadırlar. Bu bağlamda, elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili olmayan kurum ve kuruluş düzleminde gizlilik dereceli belgelerin hazırlanması, gönderimi ve havale edilmesi Şekil 38'de gösterilmiştir.



Şekil 38. Gizlilik Dereceli Belgelerin Hazırlanması, Gönderilmesi ve Havale Edilmesi

6.3. GÜVENLİK ÖNLEMLERİNE İLİŞKİN BULGULAR VE DEĞERLENDİRME

Güvenlik önlemleri kapsamında incelenen araştırma belgelerinden elde edilen bulgular belge türlerine göre Tablo 16'da gösterilmiştir. Güvenlik önlemi bileşeninin kategorilerine ait bulgular ve değerlendirmeler alt başlıklar altında sunulmaktadır.

Tablo 16. Araştırma Kapsamında İncelenen Belgelerde Güvenlik Önlemlerine İlişkin Kavramların Geçme Sıklığı

Güvenlik Önlemleri Bileşeni Kategorileri	**Belge Türü**	**Geçme Sıklığı**	
		N	**%**
Belge Güvenliği	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	1	3,4
	Yönerge	1	3,4
	Rehber	0	0,0
	Standartlar	3	10,3
Fiziksel Güvenlik	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	0	0,0
	Yönetmelikler	2	6,9
	Yönerge	1	3,4
	Rehber	1	3,4
	Standartlar	6	20,7
Personel Güvenliği/Güvenirliliği	Kanunlar	1	3,4
	Kararname	0	0,0
	Genelgeler	1	3,4
	Yönetmelikler	2	6,9
	Yönerge	0	0,0
	Rehber	1	3,4
	Standartlar	2	6,9
Bilgisayar Donanım ve Yazılım Güvenliği	Kanunlar	0	0,0
	Kararname	0	0,0
	Genelgeler	1	3,4
	Yönetmelikler	1	3,4
	Yönerge	1	3,4
	Rehber	1	3,4
	Standartlar	3	10,3
Toplam		**29**	**100**

6.3.1. Belge Güvenliğine İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerinin 5'inde belge güvenliğine yönelik, belge süreçlerinin (üretme, gönderme, teslim alma, çoğaltma vb.) güvenliğinin sağlanmasına, erişim süreçlerine ve belgelerin muhafazasına ilişkin düzenlemelerin yapıldığı görülmüştür. Söz konusu araştırma belgelerinde, belgelerin tüm ilgi, ek ve ilişkili

belgeler ile birlikte bütün olarak, özniteliği bozulmadan muhafaza edilmesi ve belgelere yetkisiz erişimin engellenmesi gerektiği vurgulanmaktadır.

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te (2022) gizlilik dereceli belgelerin özgünlük, güvenilirlik, bütünlük ve kullanılabilirliğinin sağlanmasına, yetkisiz kişilerin gizlilik dereceli belgelere erişiminin sınırlandırılmasına ve engellemesine, herhangi bir ihlal durumunun tespit edilmesi durumunda yerine getirilecek hususlara ilişkin düzenlemeler yapılmıştır. Yönetmelik kapsamında gizlilik dereceli belgelerin ilgili gizlilik derecesine sahip kişiler tarafından uygun ortamlarda hazırlanması veya alınması, onay süreçlerinin tamamlanması, gönderilmesi veya havale edilmesi, muhafaza edilmesi ve imha edilmesi veya arşive devredilmesi gerekmektedir. Yönetmelik çerçevesinde gizlilik dereceli belgelerin güvenliğine yönelik alınacak tedbirler gizlilik düzeylerine göre belirlenmiş olup, söz konusu güvenlik önlemleri ve bu tedbirlerine ait yönetmelik maddeleri Tablo 17'de gösterilmiştir.

Tablo 17. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022) Kapsamında Belge Süreçlerinde Alınacak Güvenlik Önlemleri

Uygulanacak Güvenlik Önlemi	**Çok Gizli**	**Gizli**	**Hizmete Özel**
Genel güvenlik önlemleri	Madde 9	Madde 9	Madde 9
Çok Gizli Evrak Bürosunda uygulanacak önlemler	Madde 13	-	-
Belgelerin hazırlanması kapsamında uygulanacak önlemler	Madde 5 Madde 8 Madde 14	Madde 5 Madde 8 Madde 23	Madde 5 Madde 8 Madde 23
Belgelerin gönderilmesi, teslim alınması ve havale edilmesi kapsamında uygulanacak önlemler	Madde 15 Madde 16	Madde 24 Madde 25	Madde 24 Madde 25
Belgelerin muhafaza edilmesi ve sayımı kapsamında uygulanacak önlemler	Madde 17	Madde 22	Madde 22
Belgelerin çoğaltılması, tercüme edilmesi ve alıntılanması kapsamında uygulanacak önlemler	Madde 18	Madde 26	Madde 26
Belgelerin gizlilik deresinin düşürülmesi veya kaldırılması ile imha edilmesi (sadece çok gizli) kapsamında uygulanacak önlemler	Madde 19 Madde 20	Madde 27	Madde 27
Belgelerin kurum arşivine sevkinde uygulanacak önlemler	-	Madde 28	Madde 28

ISO 27001 (2022) ve ISO 27002 (2022) standartlarında, kurumsal gerekliliklerin zaman içerisindeki değişimlerine karşı belgelerin gerçekliği, güvenilirliği, bütünlüğü ve kullanılabilirliğinin korunması kapsamında, belge süreçlerinin güvenliğine yönelik

politika ve prosedürlerine ilişkin gereklilikler tanımlanmıştır. Bu gereklilikler, belgelerin güvenliğine yönelik kurumsal sınıflandırma prosedürlerine karşılık gelen bilgi güvenliği kategorileri çerçevesinde şekillenmiştir.

Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi'nde (2023) gizlilik dereceli bilgi, belge ve malzemenin gönderilmesi, devredilmesi, muhafazası, çoğaltılması, tercüme edilmesi, taşınması ve imhasına yönelik güvenlik önlemlerinin belirlendiği görülmüştür. Söz konusu güvenlik önlemleri Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te (2022) belirlenen tedbirlere benzer hatlara sahip olup, biçim ve şekil bakımından farklı uygulamaları içermektedir.

TS 13298 (2015) standardında belge güvenliği kapsamında EBYS'nin sahip olması gereken erişim haklarına, kullanıcı profillerine ve rollerine, belge sahipliğine, günlük işlem kayıtlarına ve sistem güvenirliğine yönelik kriterler belirlenmiştir.

6.3.2. Fiziksel Güvenliğe İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerinin 10'unda fiziksel güvenliğe yönelik düzenlemelerin yapıldığı görülmüştür. Fiziksel güvenliğin belgelerin bulunduğu gizlilik dereceli birimlerin mekânsal durumunun gizliliğini, belgeler ile belgelerin muhafaza edildiği ve elektronik belgelerin depolandığı sunucuların bulunduğu mekânların fiziksel zararlardan (doğal afet, yangın, su baskını, sıcaklık, rutubet, hayvan tahribatı vb.) korunmasına yönelik alınacak tedbirleri içerdiği görülmüştür.

Belgelerin muhafaza edildiği ve elektronik belgelerin depolandığı sunucuların bulunduğu mekânların fiziksel zararlardan korunması amacıyla, uygun depolama çevresinin oluşturulması, alt yapı gereklerinin karşılanması, koruyucu malzemenin kullanılması (yangın söndürme sistemi vb.), belge kayıplarının önlenmesi kapsamında tahliye planı/felaket kurtarma planlarının oluşturulması, bu planların uygulanması ve kontrol edilmesi gerekmektedir (Cumhurbaşkanlığı Dijital Dönüşüm…, 2020a; Devlet Arşiv Hizmetleri…, 2019; Gizlilik Dereceli Belgelerde…, 2022; ISO 15489, 2016; ISO/IEC 27001, 2022; ISO/IEC 27002, 2022, NFPA 75, 2020; NFPA 232, 2022; TS 13298, 2015).

Savunma sanayi faaliyetleri kapsamında yürütülen gizlilik dereceli projelere ait bilgi, belge ve malzemelerin bulunduğu tesislerde alınması gereken fiziki güvenlik önlemlere

yönelik koruyucu ve önleyici tedbirler belirlenmiştir. Söz konusu tesislerde 5188 Sayılı Özel Güvenlik Hizmetlerine Dair Kanun'da (2004) belirtilen fiziki koruma tedbirlerinin alınması gerekmektedir (Milli Savunma Bakanlığı…,2023).

Kamu kurum ve kuruluşlarında gizlilik dereceli belgelerin fiziki güvenliğine yönelik oluşturulması gereken erişim engellerinin belgelerin sahip oldukları gizlilik düzeylerine göre belirlenmiştir (Gizlilik Dereceli Belgelerde…, 2022). Örneğin, çok gizli gizlilik dereceli belge süreçlerinde yer alan personel için (büro personeli, kurye vb.) yetki kartı düzenlenmekte iken, gizli gizlilik dereceli belge süreçlerinde yer alan personelin yetkililik durumunu gösteren herhangi bir uygulama belirlenmemiştir.

6.3.3. Personel Güvenliği/Güvenirliliğine İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerinin 7'sinde personel güvenliği/güvenirliğine yönelik düzenlemelerin yapıldığı görülmüştür. Bir kişinin kamu görevine başlayabilmesi için yeterli güvenilirlikte olup olmadığının tespiti amacıyla arşiv araştırması yapılmaktadır. Stratejik önemi bulunan kurum ve kuruluşların üst düzey yöneticileri, kritik öneme sahip projelerde görev yapacak personel ile gizlilik dereceli birim veya kısımlarda çalışacak personel için arşiv araştırması ve güvenlik soruşturması birlikte yapılmaktadır (Cumhurbaşkanlığı Bilgi…, 2019, mad. 17; Gizlilik Dereceli Belgelerde…., 2022, mad. 10 (1); Güvenlik Soruşturması…, 2021, mad. 6; Güvenlik Soruşturması… , 2022, mad. 9).

ISO/IEC 27001 (2022) ve ISO/IEC 27002 (2022) standartlarında personel güvenliği kapsamında, çalışanların bir güvenlik soruşturma sürecinden geçirilmesi gerektiği belirtilmektedir. Bu süreçten sonra işe alınan personel ile gizlilik sözleşmesi yapılmalı ve personele görev sorumlulukları ile kurumsal bilgi güvenliği hususlarının bildirilmesi gerekmektedir. Herhangi bir bilgi güvenliği ihlalinden sorumlu olan personel hakkında resmi bir disiplin süreci gerçekleştirilmelidir. Bu bağlamda, kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde personel güvenliğine yönelik genel güvenlik tedbirleri, eğitim ve farkındalık faaliyetleri ve tedarikçi ilişkileri güvenliğine yönelik hususlar belirlenmiştir (Cumhurbaşkanlığı Dijital Dönüşüm…, 2020a).

6.3.4. Bilgisayar Donanım ve Yazılım Güvenliğine İlişkin Bulgular ve Değerlendirme

Araştırma kapsamında incelenen belgelerinin 7'sinde belge süreçlerinin yürütüldüğü bilgisayar donanım ve yazılımların güvenliğine yönelik düzenlemelerin yapıldığı görülmüştür. Farklı belge yönetim süreçleri (fiziki veya elektronik ortam) kapsamında kullanılan bilgisayarların donanım ve yazılım bileşenlerine yönelik alınması gereken temel güvenlik önlemleri belirlenmiştir (Cumhurbaşkanlığı Bilgi…, 2019; Gizlilik Dereceli Belgelerde…, 2022; Milli Savunma Bakanlığı…, 2023; TS 13298, 2015). Gizlilik dereceli belgelere yönelik kullanılan bilgisayarların donanım ve yazılım bileşenlerinin kurumsal BYGS ve Bilgi ve İletişim Güvenliği Rehberi (2020) ile çerçevelenen temel ilkelere uygun olarak kullanılması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022, mad. 9). Yapılan incelemede bu rehberin ISO/IEC 27001 (2022) ve ISO/IEC 27002 (2022) standartlarıyla uyumlu olduğu görülmüştür. Bu rehber uygulama süreci, varlık gruplarına yönelik güvenlik tedbirleri, uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri ve sıkılaştırma tedbirleri olmak üzere dört temel bileşenden oluşmaktadır. Rehber kapsamında uygulanması gereken asgari güvenlik tedbirleri Tablo 18'de sunulmaktadır.

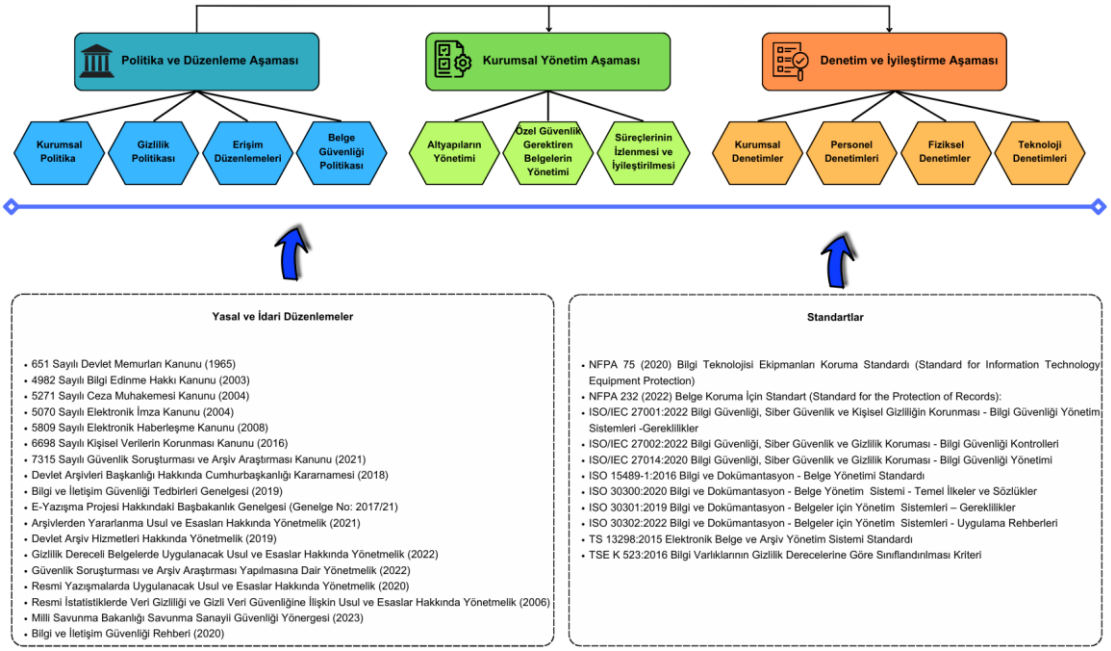
Tablo 18. Bilgi ve İletişim Güvenliği Rehberi (2020) Kapsamında Alınacak Asgari Güvenlik Tedbirleri

Varlık Gruplarına Yönelik Güvenlik Tedbirleri		Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri	Sıkılaştırma Tedbirleri
1. Ağ ve Sistem Güvenliği • Donanım Varlıklarının Envanter Yönetimi • Yazılım Varlıklarının Envanter Yönetimi • Tehdit ve Zafiyet Yönetimi • E-Posta Sunucusu ve İstemcisi Güvenliği • Zararlı Yazılımlardan Korunma • Ağ Güvenliği • Veri Sızıntısı Önleme • İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi • Sanallaştırma Güvenliği • Siber Güvenlik Olay Yönetimi • Sızma Testleri ve Güvenlik Denetimleri • Kimlik Doğrulama ve Erişim Yönetimi • Felaket Kurtarma ve İş Sürekliliği Yönetimi • Uzaktan Çalışma **2. Uygulama ve Veri Güvenliği** • Kimlik Doğrulama • Oturum Yönetimi • Yetkilendirme • Dosyaların ve Kaynakların Güvenliği • Güvenli Kurulum ve Yapılandırma • Güvenli Yazılım Geliştirme • Veri Tabanı ve Kayıt Yönetimi • Hata Ele Alma ve Kayıt Yönetimi • İletişim Güvenliği • Kötücül İşlemleri Engelleme • Dış Sistem Entegrasyonlarının Güvenliği	**3. Taşınabilir Cihaz ve Ortam Güvenliği** • Akıllı Telefon ve Tablet Güvenliği • Taşınabilir Bilgisayar Güvenliği • Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları) **4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği** • Ağ Servisleri ve İletişimi • Dâhili Veri Depolama • Kimlik Doğrulama ve Yetkilendirme • API ve Bağlantı Güvenliği • Diğer Güvenlik Tedbirleri **5. Personel Güvenliği** • Genel Güvenlik Tedbirleri • Eğitim ve Farkındalık Faaliyetleri • Tedarikçi İlişkileri Güvenliği **6. Fiziksel Mekânların Güvenliği** • Genel Güvenlik Tedbirleri • Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri • Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)	**1. Kişisel Verilerin Güvenliği** • Kayıt Yönetimi • Erişim Kayıtları Yönetimi • Yetkilendirme • Şifreleme • Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme • Aydınlatma Yönetimi • Açık Rıza Yönetimi • Kişisel Veri Yönetim Sürecinin İşletilmesi **2. Anlık Mesajlaşma Güvenliği** • Genel Güvenlik Tedbirleri **3. Bulut Bilişim Güvenliği** • Genel Güvenlik Tedbirleri **4. Kripto Uygulamaları Güvenliği** • Kriptografik Algoritmalar ve Kullanımı • Şifreleme ve Anahtar Yönetimi • Kriptografik Uygulamalar **5. Kritik Altyapılar Güvenliği** • Genel Güvenlik Tedbirleri • Enerji Sektörü Özelinde Güvenlik Tedbirleri • Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri 6. **Yeni Geliştirmeler ve Tedarik** • Genel Güvenlik Tedbirleri	1. **İşletim Sistemi Sıkılaştırma Tedbirleri** • Genel Sıkılaştırma Tedbirleri • Linux İşletim Sistemi Sıkılaştırma Tedbirleri • Windows İşletim Sistemi Sıkılaştırma Tedbirleri **2. Veri Tabanı Sıkılaştırma Tedbirleri** • Genel Sıkılaştırma Tedbirleri 3. **Sunucu Sıkılaştırma Tedbirleri** • Web Sunucusu Sıkılaştırma Tedbirleri • Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

7. BÖLÜM

KAMU KURUMLARINDA ÖZEL GÜVENLİK GEREKTİREN BELGELERE YÖNELİK BİR MODEL ÖNERİSİ

Çalışmada, Türkiye'de kamu kurumlarında özel güvenlik gerektiren belgelere yönelik uygulamalar literatür çerçevesinde modellenmiştir. Model oluşturulurken çalışma konusuna ilişkin idari ve yasal mevzuat, ulusal ve uluslararası standartlar, uygulama örnekleri, projeler ile benzer model çalışmaları değerlendirilmiştir. Bu modelde, özel güvenlik belgelerin yönetim süreçlerinin tanımlanması ve iyileştirilmesi amaçlanmıştır. Bu kapsamda, özel güvenlik gerektiren belgelerin yönetim süreçlerinin geliştirilmesine yönelik oluşturulan modelin aşamaları Şekil 39'da sunulmaktadır. Modelde belgelerin yönetimi üç aşamada sunulmuştur. Modelin ilk aşaması politika ve düzenleme unsuru, ikinci aşama kurumsal yönetim unsuru, üçüncü aşama ise denetim ve iyileştirme unsuru olarak tanımlanmaktadır.



Şekil 39. Özel Güvenlik Gerektiren Belgelere Yönelik Uygulama Modeli

Modelin üç aşamasının altında bulunan bileşenler özel güvenlik gerektiren belge yönetim süreçlerinin temel aşamalarını ve bileşenlerini oluşturmaktadır. Söz konusu her bileşen gizlilik dereceli belge süreçlerinin tamamlayıcısı rolündedir. Modelin

aşamaları birbirleriyle ilişki bir şekilde tanımlanmakla birlikte, uygulama açısından farklı süreçleri içerebilmektedir. Bu sebeple, politika ve düzenlemesi aşamasını kapsayan bileşenler kurumsal yönetim aşamasını etkilemekte olup, aynı zamanda kurumsal yönetim aşamasını kapsayan bileşenler ise denetim ve iyileştirme aşamasını etkilemektedir. Bu bağlamda, aşamalar kendileriyle ilişkili bir şekilde tanımlanmakla birlikte, bu aşamalar uygulama süreçleri ve zamanları bakımından farklılık göstermektedir.

Model sürecinin son kısmında modelin oluşturulması kapsamında yararlanılan yasal ve idari düzenlemeler ile standartlar bulunmaktadır. Model bilişenlerine yönelik oluşturulan uygulama örneklerine esas teşkil eden söz konusu yasal ve idari düzenlemeler ile standartlar model bileşenin yanında gösterilmektedir.

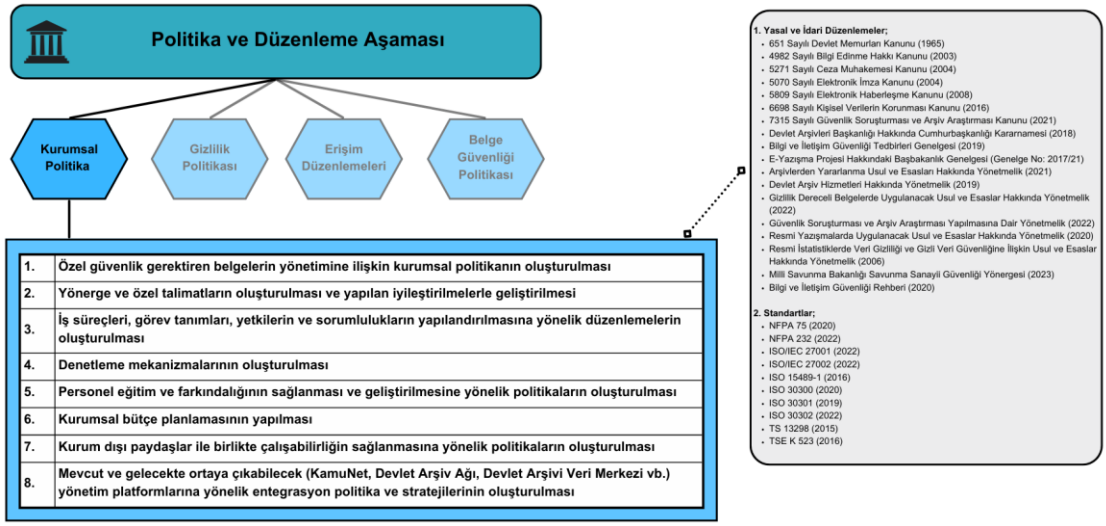
7.1. POLİTİKA VE DÜZENLEME AŞAMASI

Çoğu devlet yönetimde şeffaflığı, toplumun yönetime katılmasını ve bilgi edinme hakkının kullanılmasını en iyi şekilde gerçekleştirmek için yasal ve idari düzenlemelerin yanı sıra e-devlet ve açık veri gibi birçok uygulamalar oluşturmuşlardır. Ayrıca, kişisel ve ulusal güvenliğinin korunması amacıyla devletin elinde bulunan veri, bilgi ve belgelere erişim kısıtlamaları uygulanmaktadır. Ulusal ve kişisel güvenliğin sağlanması amacıyla veri, bilgi ve belgelerin gizlilik derecesiyle sınıflandırılarak yetkisiz erişimin engellenmesi ve bilgi edinme hakkının kullanılmasına yönelik oluşturulan kısıtlamalar yasal ve idari düzenlemelerde varlık bulmaktadır. Söz konusu erişim kısıtlaması ile yasal ve idari düzenlemeler devletin organik yapısında bulunan kamu kurumları tarafından oluşturulan politika ve uygulamalarla gerçekleştirilmektedir. Bu kapsamda, modelin bu aşamasında kurumsal politika, gizlilik politikası, erişim düzenlemeleri ve belge güvenliği politikası bileşenleri ele alınmaktadır.

7.1.1. Kurumsal Politika

Devlet yönetimi tarafından gizlilik dereceli belge süreçlerine ilişkin belirlenen politika ve düzenlemelerin yanı sıra devletin vücudunu oluşturan kamu kurumlarının bu kapsamda politikalar geliştirilmesi ve bu yönde eylemlerde bulunmaları önemlidir. Bu sebeple kurumların, gizlilik dereceli belge yönetimine ilişkin politika oluşturmaları bu bileşen kapsamında yer almaktadır. Araştırmada, gizlilik dereceli belgelerin yönetimine ilişkin

hususların Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2020) ve Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022)'te yer aldığı, gizlilik derecesine sahip olmayan belgelere yönelik ise sadece bilmesi gereken prensibinin uygulandığı tespit edilmiştir. Bahse konu yönetmeliklerde gizlilik dereceli belgelerin yönetimine yönelik temel ilkeler belirlenmiş olmakla birlikte, belgelere yönelik gizlilik süresini, gizlilik dereceli belirlemeye yönelik nesnel ölçütleri ve bunlara ilişkin standartlar ile süreçleri, erişim kural ve sorumluluklarını, KamuNet vb. uygulamalarla birlikte çalışabilirliğinin sağlanmasına ilişkin uygulamalara yönelik güvenlik gerekliliklerini kapsamadığı anlaşılmıştır. Bu bağlamda, kurumsal politikalara ilişkin uygulama örnekleri ile bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 40'a sunulmaktadır.

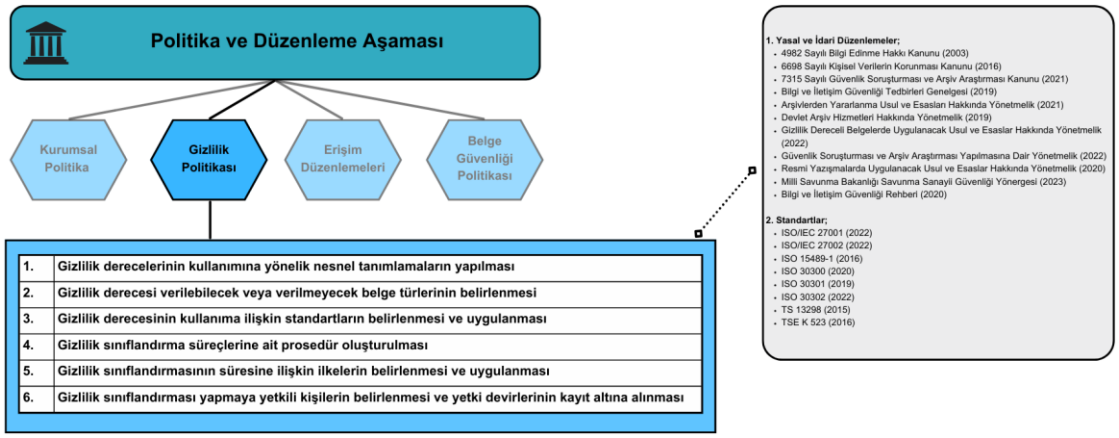


Şekil 40. Kurumsal Politika Bileşeni

Kurumsal politika bileşeni kurumun ihtiyaç ve hedeflerini karşılamak için özel güvenlik gerektiren belgelerin yönetimine ilişkin süreçleri kapsamaktadır. Bu politika, kuruma ait özel güvenlik gerektiren belgelerinin yönetilmesiyle birlikte, güvenlik, denetim, iyileştirme ve eğitim faaliyetlerini kapsamalıdır. Kurum tarafından politika belirlendikten sonra onaylanmalı, bilmesi gereken prensibine göre kurum bünyesinde yayınlanmalı, uygulanmalı ve denetlenmelidir. Kurumsal politika yönerge ve özel talimatlarla desteklenmeli ve bunlar ortaya çıkan güncel durumlar karşısında iyileştirilmelidir.

7.1.2. Gizlilik Politikası

Geniş anlamda gizlilik politikası, yasal ve idari düzenlemelerle yürürlüğe konulan bir dizi politikayı ifade etmektedir. Bu politika güvenlik gerekçesiyle özel güvenlik gerektiren belgelere erişimin kısıtlanmasıdır. Bu erişim sınırlandırılmasının amacı ulusal ve kişisel güvenliğin sağlanarak muhtemel zararların önüne geçilmesidir. Bu kapsamda, özel güvenlik gerektiren belgelere yönelik gizlilik politikası oluşturulmalı, bilmesi gereken prensibine göre yayınlanmalı ve uygulanmalıdır. Model önerisinde gizlilik politikasına ilişkin uygulama örnekleri ile bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 41'de sunulmaktadır.



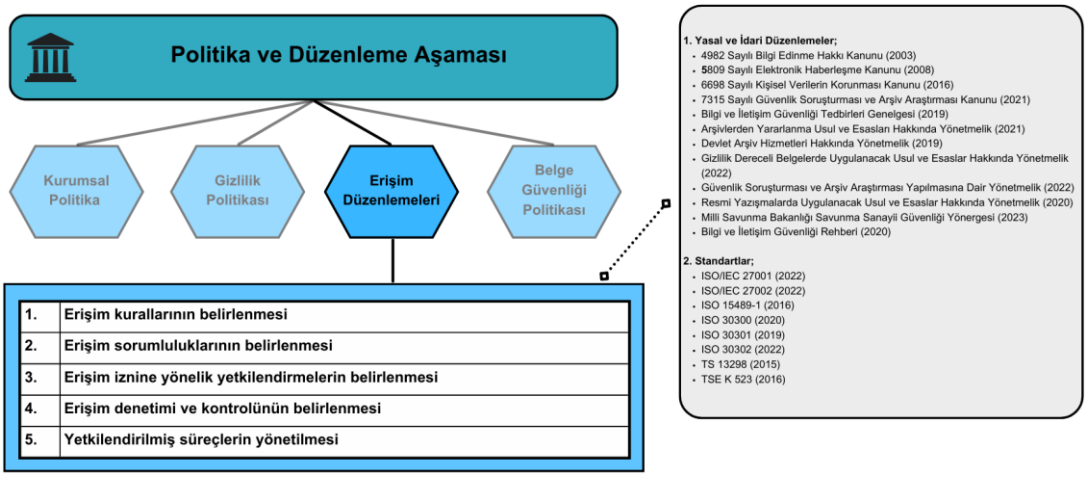
Şekil 41. Gizlilik Politikası Bileşeni

Kurumlarda bulunan ve özel güvenlik gerektiren belgelere yönelik herhangi bir ifşa, kişisel, kurumsal, ulusal ve uluslararası menfaatlerin zarar görmesine neden olabilecektir. Bu sebeple, bu belgeler etkin ve sistemli bir şekilde yönetilmelidir. Bu bağlamda, bilmesi gereken prensinin etkin bir şekilde kullanılması, gizlilik derecelerinin net bir tanımının yapılması ve hangi gizlilik derecelerinin hangi belgelere kullanılacağının tespit edilmesi önemli bir husustur. Ayrıca kurumsal olarak özel güvenlik gerektiren belge tür ve gruplarının belirlenmesi iş yükünü azaltacaktır. Gizlilik dereceli belgelere yönelik standart uygulamalar idari düzenlemelerle belirlenmiştir (Resmi Yazışmalarda Uygulanacak Usul…, 2020; Gizlilik Dereceli Belgelerde Uygulanacak…, 2022). Kurum tarafından, idari düzenlemelerde belirtilen standartlar ile kurumsal olarak belirlenen standartların uygulanması sağlanmalıdır. Kurum tarafından, ifade ettiği anlamlar göz önüne alınarak, hangi bilgi ve veriyi içeren belgelerin hangi gizlilik derecesiyle ilişkilendirileceğine yönelik bir "Belgelere Gizlilik Derecesi Verme

Prosedürü" belirlenmelidir. Bu prosedürle, gizlilik derecelerinin belirlenmesi kurum içerisinde kişilerin tasarrufuna bırakılmayacak olup, gereğinden fazla veya düşük gizlilik derecesinin kullanılmasının önüne geçilmesi sağlanacak ve belgenin korunma gereksinimleri ile belgelere erişim ihtiyacı arasında dengeli bir köprü kurulacaktır. Belgelerin gizlilik derecesiyle sınıflandırılması ilave sistem, donatınım, depolama ve personel gerektirmesi sebebiyle bütçelerde yer alan maliyet kalemlerini artırmasının yanı sıra, bilgi edinme hakkını sınırlamakta birlikte, şeffaflık ve toplumun yönetime katılımının engelleyicisi olmaktadır. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022) ile süreli gizlilik uygulaması hayata geçirilmiştir. Bu bağlamda, gizlilik sınıflandırma süresine ilişkin ilkelerin belirlenmesi ve uygulanması süreli gizlilik pratiğinin efektif olarak kullanılmasını sağlayacaktır. Gizlilik derecesi vermeye yetkili kişilerin açıkça belirlenmesi ve bu kişiler tarafından yapılacak olan yetki devirlerinin kayıt altına alınması önemli bir husustur. Bu bağlamda, gizlilik derecesi verme yetkilerinin resmi yazı ile kayıt altına alınması önerilmektedir.

7.1.3. Erişim Düzenlemeleri

Devletler, kurumsal belgeye erişimi kısıtlamak için politikalar geliştirmişlerdir. Örneğin kurumlarca bir belgenin hizmete özel gizlilik dereceyle sınıflandırılması bu belgenin kamuya açıklanmasını engellemektedir. Özel güvenlik gerektiren belgelerin yetkisiz olarak paylaşılması veya açıklanması halinde devletin ve kişilerin menfaatlerine farklı düzeylerde zarar verilmesinin önlenmesi maksadıyla gizlilik sınıflandırılması yapılmaktadır. Söz konusu menfaatlerin korunması amacıyla yapılan bu sınıflandırma temelde bilmesi gereken prensibine göre yetkili kişilerin gizlilik dereceli belgelere erişim sağlamaları, yetkisiz kişilerin ise bu belgelerle ilişkisinin kesilmesi esasına dayanmaktadır. Bu bağlamda, erişmek isteyen kişi ve erişilmek istenilen belge durumu söz konusundur. Erişim yönetimin ideali, yetkisiz erişimin engellenerek, yetkili erişimin ise hızlı ve doğru bir şekilde yerine getirilmesidir. Bu kapsamda, erişim sağlamak isteyen ile erişilmek istenilen arasında bir benzer yetki ve yeterlilik bulunması gerekmektedir. Bu sebeple, kurumsal olarak erişim kurallarının, yetki ve sorumluluklarının, erişim kontrollerinin belirlenmesi ile yetkili erişim süreçlerinin yönetilmesi önem arz etmektedir. Model önerisinde erişim düzenlemeleri bileşenine ilişkin uygulama örnekleri ile bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 42'de sunulmaktadır.



Şekil 42. Erişim Düzenlemeleri Bileşeni

Kurum çalışanlarının gizlilik dereceli belgelere erişim sağlayabilmeleri için sahip olması gereken temel hususlar ilgili yasal/idari düzenlemelerle belirlenmiştir. Söz konusu belgelere erişim sağlayabilmesi için kişinin sahip olması gereken temel hususlar Tablo 19'da gösterilmektedir. Bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelere yönelik erişimler bilmesi gereken prensibine göre yapılmaktadır.

Tablo 19. Gizlilik Dereceli Belgelere Erişim Sağlayacak Kişide Bulunması Gereken Temel Nitelikler

Temel Nitelikler	Yasal/İdari Düzenleme veya Öneri
Erişim sağlamak isteyen kişinin işi gereği bilme ihtiyacının olması gerekmektedir.	Önerilmektedir
Bilmesi gereken prensibine göre personel erişim yetkisi alacağı birimde çalışmalıdır.	Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022)
İlgili gizlilik düzeyi çerçevesinde yetkili yönetici tarafından gizlilik yetkilendirilmesi yapılmalıdır.	
Güvenlik soruşturması ve arşiv araştırmasının yapılmış olması (Çok gizli ve gizli dereceli belgelere erişim kapsamında yapılacak yetkilendirmeler çerçevesinde personelin güvenlik soruşturması ve arşiv araştırması birlikte yapılmaktadır) gerekmektedir.	Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik (2022)
Erişim sağlamak isteyen kişi ile kurum arasında bir güvenlik veya gizlilik sözleşmesi yapılmalıdır.	Önerilmektedir

Özel güvenlik gerektiren belgelerin üretilmesi, paylaşılması, teslim alınması, muhafaza edilmesi, imha edilmesi veya arşivlenmesi gibi süreçlerde yer alacak kişilerin erişim yetkilendirilmeleri kurumsal olarak belirlenen kurallar çerçevesinde yapılmalıdır. Bu bağlamda, tüm kurum çalışanlarını bir gizlilik derecesiyle yetkilendirmeyen (aşçı, şoför, temizlik görevli gibi), bir gizlilik derecesine sahip kişinin bu gizlilik derecesine haiz her

belgeye nüfus etmesini engelleyen, bilmesi gereken prensibini etkin bir şekilde uygulayan, erişim sağlayan kişinin sorumluluğunu ve uyması gereken tedbirleri bildiren veya hatırlatan, erişimlerin kayıt altına alınmasını sağlayan (fiziki olarak veya EBYS özellikleri kullanılarak), tayin ve emeklilik gibi görevin sonlanmasıyla erişim yetkilerinin anında iptal edilmesini ve bu yetki iptalini ilgili birimlerle bildirilmesini sağlayan, belgelerin arşive teslimi ve arşivden yararlanma usulleri belirleyen kurallar oluşturulmalıdır.

Özel güvenlik gerektiren belgelere fiziksel ve elektronik olarak erişilebilmektedir. Fiziksel erişim bina, oda gibi korunan bölgelere yönelik erişimlerdir. Bu bağlamda, bir personelin binaya girişinde kullandığı akıllı kart, odaya girmesi için sahip olduğu anahtar vb. hususlar fiziksel erişimin denetleyicisi olabilmektedir. Elektronik erişim ise, bir bilgisayar sistemi veya ağına yönelik erişimlerdir. Elektronik erişim denetimi ile kimlerin hangi sistemlere girebileceği ve hangi görevleri gerçekleştirebileceği belirlenebilmektedir. Güvenliği sağlanan bir kaynağın yetkisiz kullanımını önlemek maksadıyla kullanılan birçok strateji, kimlik doğrulama, yetkilendirme ve izlenebilirliği içeren üç yönlü bir yaklaşım kullanmaktadır. Bir personelin kimliği parola, kimlik numarası, akıllı kart gibi denetimler ile doğrulanmakta ve bundan sonra ki aşamada erişim kontrol listeleri, fiziksel erişim kontrolleri gibi yetkilendirme kontrolleri yordamıyla yetkili kişilerin korunan kaynağa erişimi sağlanmaktadır. Bir belgenin korunabilmesi ve güvenliğinin sağlanabilmesi için, erişim sağlamak isteyen kişi hakkında bilgi sahibi olunması gerekmektedir. Bu bağlamda, Kim ve Solomon (2019, ss. 127-128) tarafından tanımlanan ve aşağıda sunulan erişim kontrollünün dört elamanının kullanılması önerilmektedir.

- Kimlik Tanımlama: Bir varlığa ulaşmak isteyen kişinin kim olduğunun tanımlanması.
- Kimlik Denetleme/Doğrulama: Erişim sağlamak isteyen kişinin kimliğinin doğrulanması.
- Yetkilendirme: Erişim sağlamak isteyen kişinin net bir şekilde nelere ulaşabileceği konusunda yetkilendirmenin yapılması.
- İzlenebilirlik: Bir kişinin erişim eylemlerinin izlenebilmesi.

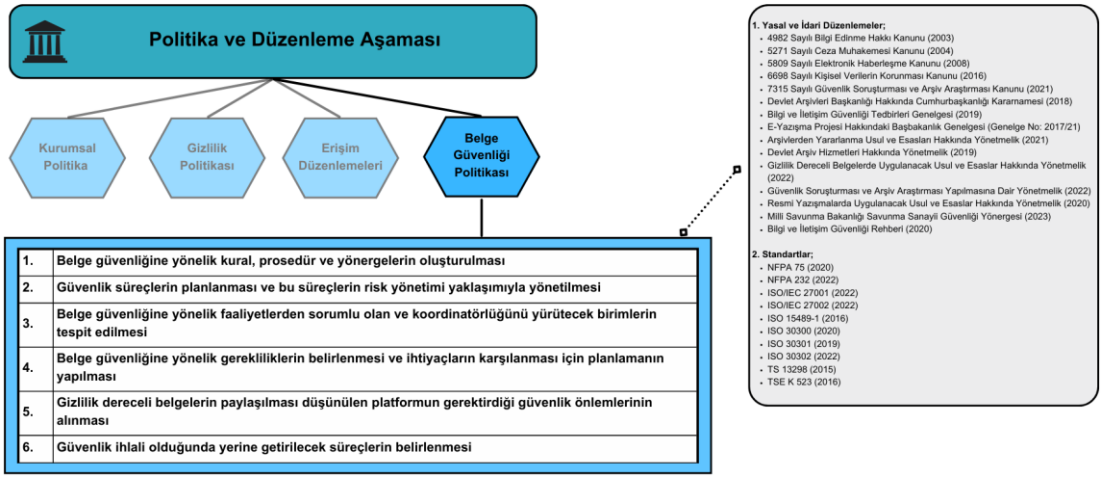
Özel güvenlik gerektiren belgelere nüfus etmeyi gerektiren faaliyetlerin (belgelerin üretilmesi, havale edilmesi, teslim edilmesi veya alınması, çoğaltılması, çeviri

yapılması, imha edilmesi, kurum arşivine devredilmesi vb.) yetkilendirilmiş süreçlerde yönetilmesi önem arz etmektedir. Bu kapsamda, yetkilendirilmiş erişim süreçlerinin bilmesi gereken prensibi ile yetkililik düzeylerinin birlikte uygulanması, erişimin kişinin yetkili olduğunun tespitinden sonra gerçekleştirilmesi, üretme, onaylama ve gönderilme süreçlerinde belgenin görünmesini engelleyici uygulamaların kullanılması ve bu uygulamaların yetkisiz erişimleri tespit edecek şekilde dizayn edilmesi, erişim ihlallerinde uygulanacak hal tarzlarının ve yerine getirilecek hususların belirlenmesi önerilmektedir.

7.1.4. Belge Güvenliği Politikası

Özel güvenlik gerektiren belgeleri üreten ve muhafaza eden kamu kurum ve kuruluşları bu belgelerin güvenliğini almakla yükümlüdürler. Bu sebeple, kurumsal çerçevede belgelerin güvenliğinin sağlanması maksadıyla kural, prosedür ve yönergeler ile standartları kapsayan belge güvenliği politikası oluşturulmalı ve kurum çapında tutarlı olarak uygulanmalıdır. Özel güvenlik gerektiren belgelerin korunmasını ve yetkisiz erişime karşı önlem alınmasını amaçlayan bu politika, kimin hangi belgelere erişimin olması gerektiğini, belgelerin özgünlüğünün korunmasının sağlanmasının yanı sıra, yetkisiz erişimin engellenmesi için hangi unsurların nasıl koruma altına alınacağını, belgelerin yeni uygulamalar üzerinden paylaşılmasına yönelik entegre olunacak uygulamaların güvenlik gerekliliklerini, kurumsal olarak uygulanan belge güvenliği uygulamasının maliyetinin belirlenmesi ve ihtiyaç duyulacak gereklilikler (personel, fiziki mekanlar, güvenlik ekipmanları, bilgisayar donanım ve yazılımları vb.) kapsamında bütçe planlamalarını içermelidir. Bu bağlamda, belge güvenliği politikasına ilişkin uygulama örnekleri ile bu bileşen kapsamında bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 43'de sunulmaktadır.

.



Şekil 43. Belge Güvenliği Politikası Bileşeni

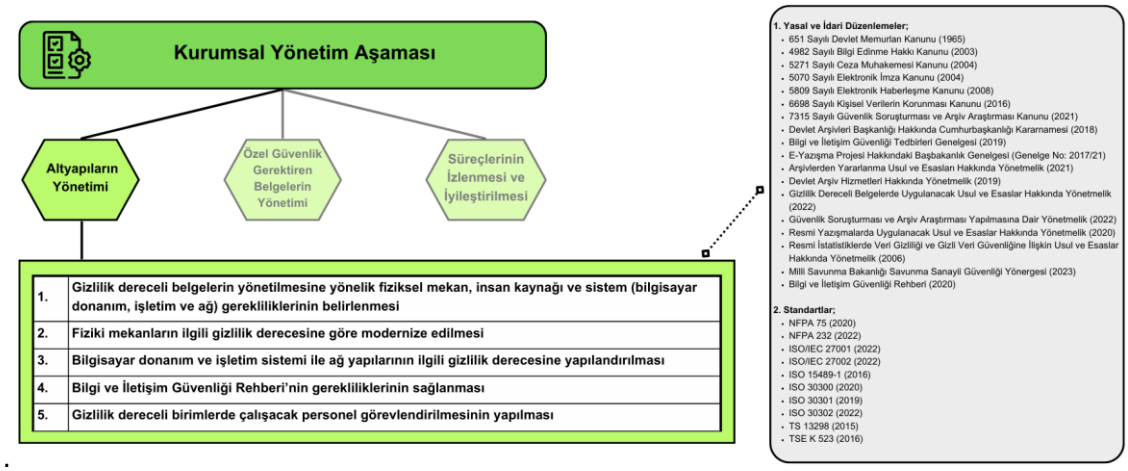
Güvenlik süreçleri belge güvenliği, fiziki ortam güvenliği, personel güvenliği/güvenilirliği, teknoloji (bilgisayar donanım, işletim ve ağ) güvenliği bileşenlerden oluşmalı ve risk yönetimi yaklaşımıyla yönetilmelidir. Güvenlik süreçleri birçok bileşenden meydana gelmekte olup, kamu kurumlarında ve bunların taşra teşkilatlarında bu bileşenlerin yönetilmesinden sorumlu olan birimler ile genel koordinatör birimlerinin oluşturulması güvenlik süreçlerin etkin bir şekilde yönetilmesini sağlayacaktır. Gizlilik dereceli belgeler yetkili personel marifetiyle güvenlik düzeylerine göre oluşturulmuş mekanlarda ve sistemlerle yönetilmektedir. Bu kapsamda, gizlilik dereceli birimlerin tespit edilmesi ile bu birimleri barındıran fiziki mekanların güvenlik gereklilikleri ve bu birimlerde çalışacak personelin niteliklerinin belirlenmesi gerekmektedir. Bu tespitten sonra mevcut durumun değerlendirilmesi ve gerekliliklerin belirlenerek, eksik hususların tamamlanması için kısa, orta ve uzun vadeli planlar yapılmalıdır. Bilgi ve iletişim teknolojisindeki ilerlemelerle birlikte özel güvenlik gerektiren belgelerin paylaşımına yönelik yeni uygulamaların (Kamu Sanal Ağı, Devlet Arşiv Ağı, Devlet Arşivi Veri Merkezi, Ulusal Kamu Entegre Veri Merkezi, Bütünleşik Arşiv Yönetim Sistemi vb.) güvenlik gereklilikleri belirlenmeli ve uygulanmalıdır. Belge güvenliği ihlali olması durumunda yerine getirilecek süreçler anlaşılabilir, tam, doğru, hızlı bir şekilde yönetilecek şekilde tasarlanmalıdır. Bu süreç, ihlalin tespit edildiği anda uygulanacak hal tarzlarından ihlale konu soruşturmanın yapılmasına kadar olan bütün bileşenleri kapsamalıdır.

7.2. KURUMSAL YÖNETİM

Kişisel, kurumsal, ulusal ve uluslararası menfaatlerin korunması maksadıyla belge yönetim süreçlerinde gizlilik sınıflandırılması yapılarak belgelerin oluşturulması, sağlanması, paylaşılması, imha edilmesi veya arşivlenmesi süreçlerinin güvenli bir şekilde yapılması ön görülmüştür. Ayrıca, bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelerin (hukuki belgeler ile kişisel bilgileri içeren sağlık belgeleri, eğitim belgeleri, mali belgeler vb.) yönetim süreçlerinin bilmesi gereken prensibi ile gerçekleştirilmesi gerekmektedir. Bu bağlamda, özel güvenlik gerektiren belgelerin tüm ilgi, ek ve ilişkili belgeleriyle birlikte bir bütün olarak, özniteliği bozulmadan muhafaza edilmesi ve bu belgelere yetkisiz erişimin engellenmesi gerekmektedir. Bu kapsamda, modelin bu aşamasında altyapılar, özel güvenlik gerektiren belgelerin yönetimi ile süreçlerinin izlenmesi ve iyileştirilmesi bileşenleri ele alınmaktadır.

7.2.1. Altyapıların Yönetimi

Kamu kurumlarında farklı gizlilik derecesine sahip belgeler ile bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgeler üretilmekte veya teslim alınmaktadır. Gizlilik dereceli belgelerin yönetimi ilgili gizlilik derecesine göre oluşturulan ortamlarda (fiziki veya elektronik) gerçekleştirilmektedir. Bu ortamlarda yürütülen süreçlerin belgelerin sahip olduğu gizlilik derecesine göre farklı fiziki mekanlarda, sistemlerle ve farklı yetki düzeylerine sahip kişilerce yürütülmesi gerekmektedir. Belgelerin ilgili hassasiyetlik derecesinin gerektirdiği güvenlik düzeylerine yönetilmesi farklı altyapı gereksinimlerini ortaya çıkarmaktadır. Bu altyapılar personel, fiziki mekan, bilgisayar donanım, işletimi ve ağlar ile diğer bilgi sistemi gerekliliklerinden oluşmaktadır. Bu bağlamda, altyapıların yönetimine ilişkin uygulama örnekleri ile bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 44’de sunulmaktadır.



Şekil 44. Altyapıların Yönetimi Bileşeni

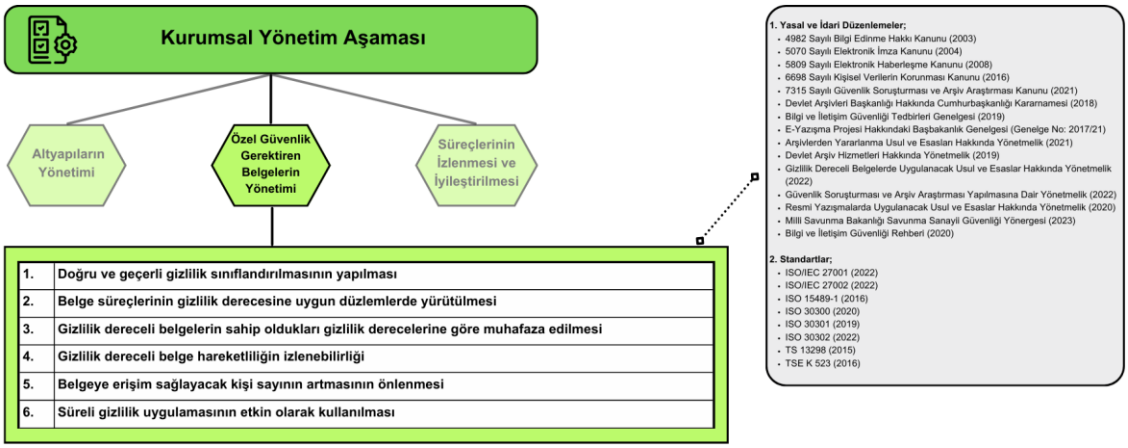
Gizlilik dereceli belgelerin farklı güvenlik düzeylerinde yönetilmesi kurum ve kuruluşlarda hibrit bir belge yönetim süreçleri ortaya çıkarmıştır. Gizlilik dereceli belgeler taşıdıkları gizlilik derecelerine göre ilgili süreçlerde varlık bulmaktadırlar (Gizlilik Dereceli Belgelerde…,2022; Resmi Yazışmalarda…Yönetmelik, 2020). Bu bağlamda gizlilik dereceli belgelerin yönetilmesine yönelik fiziksel mekan, insan kaynağı ve sistem (bilgisayar donanım, işletim ve ağ) gerekliliklerinin belirlenmesi gerekmektedir. Kamu kurumlarında gizlilik dereceli birim ve kısımlarının mekânsal durumu ile doğal afet, yangın, su baskını vb. alt yapılı gereklilikleri, bu birimlere yönelik erişim yönetimi kapsamındaki gereklilikler birimin ilgili gizlilik derecesine (Çok gizli veya gizli) tasarlanmalıdır. Gizlilik dereceli belgelerin yönetimi, yasal/idari mevzuatın gereği olarak taşıdıkları gizlilik derecesine göre fiziksel ortam (ağ bağlantısı bulunmayan ortam) ya da elektronik ortamda (EBYS) farklı güvenlik esaslarına göre yürütülmektedir **(**Gizlilik Dereceli Belgelerde…, 2022). Bu bağlamda, bilgisayar donanım, işletim ve ağ yapılarının buna göre dizayn edilerek yönetilmesi önemli bir husustur. Gizlilik dereceli belgelerin iş süreçleri kapsamında kullanılan bilgisayarların donatınım ve yazılım bileşenlerinin kurumsal BYGS ile Bilgi ve İletişim Güvenliği Rehberi ile çerçevelenen temel ilkelere uygun olarak kullanılması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022, mad. 9).

Kurum çalışanları belge süreçlerinin temel bileşenleri arasında yer almakla birlikte, çalışma kapsamında yapılan literatür incelemesinde çalışanların bilgi güvenliği zincirinin en zayıf halkasını oluşturduğu görülmüştür. Bu kapsamda, gizlilik dereceli belge yönetimi süreçlerinde görev alacak personelin güvenilirliğinden tam olarak emin

olunması önemli bir husustur. Personel güvenilirliğine yönelik, yasal ve idari düzenlemelerde gizlilik dereceli birim ve kısımlarda çalışacak personelin güvenlik soruşturması ve arşiv araştırmasının birlikte yapılması gerekmektedir (Gizlilik Dereceli Belgelerde…., 2022, mad. 10 (1); Güvenlik Soruşturması…, 2021, mad. 6; Güvenlik Soruşturması… , 2022, mad. 9). Bununla birlikte, modelde önerildiği gibi, gizlilik dereceli belge yönetim süreçlerinde görev alması planlanan personel ile kurumsal olarak bir güvenlik veya gizlilik sözleşmesinin imzalanmasından sonra gerekli gizlilik yetkilendirilmesinin verilmesi ve görevlendirilmenin yapılması önerilmektedir.

7.2.2. Özel Güvenlik Gerektiren Belgelerin Yönetimi

Kamu kurumlarında bulunan ve özel güvenlik gerektiren belgelerin yetkisiz olarak paylaşılması kişisel, kurumsal, ulusal ve uluslararası menfaatlere önemli derecede zarar verebilmektedir. Bu sebeple, özel güvenlik gerektiren belgelerin etkin ve sistemli bir şekilde yönetilmesi önem arz etmektedir. Özel güvenlik gerektiren belgelerin yönetimi, belgelerin sahip oldukları hassasiyet derecesinin gerektirdiği güvenlik seviyelerinde ve ortamlarda üretilmesi, alınması, muhafaza edilmesi, paylaşılması, çoğaltılması, tercüme edilmesi, imha edilmesi veya arşive devredilmesi süreçlerini kapsamaktadır. Belgelerin içerdiği veri ve bilgilerin hassasiyetlik dereceleri ve bu sebeple güvenlik düzeylerine göre korunma gereklilikleri, bu belgeleri diğer belgelerden ayıran özelliktir. Bir belgenin bir gizlilik derecesiyle ilişkilendirilmesi gizlilik dereceli belge yönetimi süreçlerin ilk aşaması olmakla birlikte, süreçlerin ilgili gizlilik derecesinin gerektirdiği düzlemlerde (fiziki veya elektronik ortam) güvenli bir şekilde yürütülmesi ile etkin ve yetkili erişimin sağlanmasının temelini oluşturmaktadır. Bunun yanı sıra belgelerin gizliliğine yönelik sınıflandırma gereklilikleri, sınıflandırma düzeyleri, sınıflandırma yetkisi ve sınıflandırma prosedürleri gizlilik dereceli belgelerin yönetiminde kilit faktörler olduğu değerlendirilmektedir. Ayrıca, bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelerin yönetim süreçlerinin bilmesi gereken prensibi ile gerçekleştirilmesi, bilgi edinme taleplerinin bu doğrultuda karşılanması ve erişim haklarının bu çerçevede düzenlenmesi çok önemlidir. Özel güvenlik gerektiren belgelerin yönetimine ilişkin uygulama örnekleri ile bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 45’de sunulmaktadır.



Şekil 45. Özel Güvenlik Gerektiren Belgelerin Yönetimi Bileşeni

Modelde bahsedildiği üzere bir belgenin bir gizlilik derecesiyle ilişkilendirilmesi gizlilik dereceli belge yönetiminin ilk ve temel adımıdır. Bu sebeple, gizlilik derecelerinin net bir tanımının yapılması ve hangi gizlilik derecelerinin hangi belgelere kullanılacağının tespit edilmesi önemli bir hususdur. Bu kapsamda, kurumsal gizlilik derecesi verme prosedürün oluşturulması ve kullanılması ile gizlilik derecesi vermeye yetkili kişilerin belirlenmesi ve kayıt altına alınması doğru ve geçerli sınıflandırma yapılmasını temin edecektir.

Türkiye'de gizlilik dereceli belge yönetim süreçleri, kurum yapılarına ve gizlilik derecesinin gerekliliklerine göre farkı düzlemlerde yapılmaktadır. Elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili olanlar (Kamu kurum…, 2010) tarafından yürütülecek gizlilik dereceli belge yönetim süreçleri elektronik ortamda gerçekleştirilebilirken (Resmi Yazışmalarda…Yönetmelik, mad. 31, 2020), diğer kamu kurumlarının süreçleri ise belgenin gizlilik derecesinin gerektirdiği ortamlarda (fiziki veya elektronik) yürütülmektedir. Bu bağlamda, kamu kurumlarında çok gizli gizlilik dereceli belge süreçleri bu amaçla özel olarak oluşturulmuş Çok Gizli Belge Bürosu koordinatörlüğünde, gizli gizlilik dereceli belgelerin yönetimi gerekli güvenlik önlemleri alınan fiziki ortamlarda, hizmete özel gizlilik dereceli belgelerin yönetimi ise olağanüstü durumlar haricinde sadece elektronik ortamda (EBYS) yürütülmektedir (Elektronik İmza Kanunu, 2004; Gizlilik Dereceli Belgelerde…, 2022; Resmi Yazışmalarda…Yönetmelik, 2020).

Özel güvenlik gerektiren belgelerin tüm ilgi, ek ve ilişkili belgeleriyle birlikte bir bütün olarak, özniteliği bozulmadan muhafaza edilmesi ve bu belgelere yetkisiz erişimin engellenmesi gerekmektedir. Özel güvenlik gerektiren belgeler nitelikleriyle doğru

orantılı ortamlarda ve koşullarda muhafaza edilmeli ve güvenliği sağlanmalıdır. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022) kapsamında, elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili olmayan kamu kurum düzleminde, belgelerin gizlilik düzeylerine göre muhafaza edilmesi gereken yerler Tablo 20'de gösterilmiştir.

Tablo 20. Gizlilik Dereceli Belgelerin Muhafaza Edileceği Yerler

Gizlilik Derecesi	*Belgenin Muhafaza Edileceği Yer*
Çok Gizli	*Çok Gizli Belge Bürosunda* *(Belge büro dışında ise çelik kasada veya kilitli dolaplarda) muhafaza edilir.*
Gizli	Güvenli odalarda veya kilitli dolaplarda muhafaza edilir.
Hizmete Özel	EBYS'de (şifreli veya kriptolu olarak) muhafaza edilir.

Gizlilik dereceli belgelere yönelik alınacak güvenlik tedbirleri kapsamında, gizlilik dereceli belgelerin üretildiği, kullanıldığı ve muhafaza edildiği alanlar (dolap, kasa, oda, bina) ile belgeleri barındıran bilgi ve iletişimin sistemlerinin bulunduğu alanların ilgili gizlilik derecesi çerçevesinde fiziksel ve teknik güvenlik önlemleri alınması gerekmektedir. Belgelerin muhafaza edildikleri dolap, kasa ve odalara erişimi kısıtlayan anahtar, manyetik kart veya şifreler gizlilik dereceli belge niteliğinde muhafaza edilmelidir (Gizlilik Dereceli Belgelerde…, 2022, mad. 9). Ayrıca, belgelerin yetkisiz kişiler tarafından erişilebilecek ve görülebilecek şekilde açıkta bırakılmaması ve bu belgelerin oluşturulduğu bilgisayar ekranlarının dışarıdan bakıldığında gözükmeyecek şekilde konumlandırılması, bilgisayarların kullanılmadığı zaman kapatılması, muhafazası sağlanan gizlilik dereceli belgelere yetkisiz erişimi engelleyen basit ama etki bir yöntemdir.

Gizlilik dereceli belgeler üretildikten ve teslim alındıktan sonra kurumsal kayıt sistemine dahil edilmektedir. Belgelerin teslim alınma, çoğaltma, tercüme etme vb. hareketliğine yönelik eylemler ile erişim sağlayan kişilerin bilgileri kayıt altına alınmalı ve güvenlik süreçleri kapsamında izi sürülebilir olmalıdır. Belge yönetim süreçlerinde yapılan bazı hatalar bilmesi gereken prensibi kapsamında yetkisiz erişim sağlayan kişi sayısının

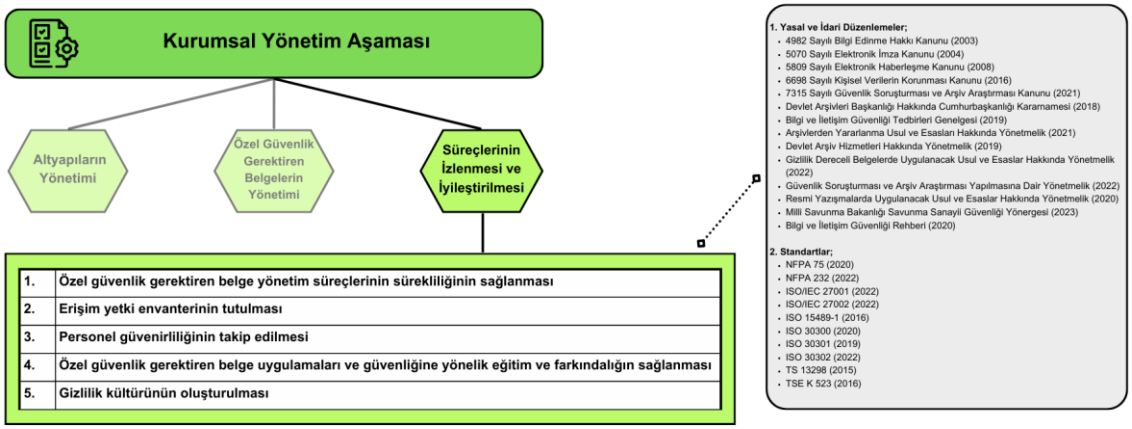
artmasına neden olmaktadır. Söz konusu yetkisiz erişimin, belgelerin paraf, onay, çoğaltma vb. işlemlerinin yetkili kişi tarafından yürütülmemesi, erişimde bilmesi gereken prensibinin kullanılmaması, belgenin dağıtımda uygun muhatap idarelerin seçilmesi, belgenin izlenebilirliğinin kontrol edilmemesi, farklı idareleri ilgilendiren eklerin dağıtımdaki tüm idarelere gönderilmesiyle gerçekleşebileceği değerlendirilmektedir.

Türkiye'de mevcut yasal ve idari düzenlemelerde gizlilik dereceli belgelerin gizliliği en fazla ne kadar süreli olacağı kesin olarak ifade edilmemekle birlikte, belgelerin gizliliğin düşürülmesi veya kaldırılması belgeyi üreten kamu kurumlarının bünyesinde oluşturulan Gizlilik Dereceli Belgeleri Değerlendirme Komisyonları veya süreli gizlilik uygulaması ile gerçekleştirilmektedir. Gizlilik Dereceli Belgeleri Değerlendirme Komisyonları belli zamanlarda toplanmakta ve değerlendirmesi gereken bir yığın gizlilik dereceli belge ile karşılaşmaktadır. Belgenin gizlilik derecesinin belirlenmesi esnasında verilecek olan süreli gizliğe ilişkin bilgiler belgenin üzerinde veya elektronik belgenin ise üst verisinde belirtilmekte ve belirlenen tarihe gelindiğinde veya olay gerçekleştiğinde ya da son bulduğunda, bir komisyon kararı veya yazışmaya gerek duyulmadan, belge üzerinde bulunan talimata göre işlem yapılmaktadır. Bu durum komisyonların ve güvenlik süreçlerinin iş yükünü azaltmasının yanı sıra belgeye ulaşmak isteyen kişi ve idarelerin erişim engellerini kaldıracaktır. Bu bağlamda, kamu kurumları tarafından oluşturulması önerilen gizlilik derecesi verme prosedürlerinde süreli gizlilik pratiğinin efektif olarak kullanılması tavsiye edilmektedir.

7.2.3. Süreçlerinin İzlenmesi ve İyileştirilmesi

Özel güvenlik gerektiren belgeler güvenlik esasları temelinde oluşturulan politika ve uygulamalarla yönetilmekte olup, bu politika ve uygulamalar çerçevesince gizlilik gereklilikleri değişmediği sürece, belgeler mevcut hassasiyetliklerini korumaktadırlar. Kurumsal politika ve uygulamalara yönelik süreçlerin doğru ve tedbirli bir şekilde yürütülmesi iş verimliliğini artırmakta ve iş sürekliliğini sağlamakla birlikte, güvenlik risklerini engellemekte veya azaltmaktadır. Bu sebeple, kurumsal özel güvenlik gerektiren belge yönetim süreçlerinin esnetilmeyen güvenlik uygulamaları çerçevesinde, sürekli olarak doğru bir şekilde yapıldığını kontrol edecek, yanlış uygulamaları ve sorumluları tespit edecek ve bildirecek mekanizmaların geliştirilmesi önemlidir. Süreçlerin izlenmesi ve iyileştirilmesine yönelik uygulama örnekleri ile bu

bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 46'da sunulmaktadır.



Şekil 46. Süreçlerinin İzlenmesi ve İyileştirilmesi Bileşeni

Doğası gereği bir yaşam döngüsü içerisinde varlık bulan özel güvenlik gerektiren belgelerin yönetilmesi kapsamında, personele farklı süreçlerde farklı roller (gizlilik derecesi belirleme, erişim yetkisi verme, tercüme etme, çoğaltma, imha etme, kurye olarak görevlendirilme vb.) verilmekte ve erişim yetkilendirilmesi yapılmaktadır. Ayrıca bir kişi çalıştığı birim haricinde farklı birimlerin yetki alanındaki süreçlerde (kurul, komisyon üyeliği vb.) birden fazla role sahip olabilmektedir. Söz konusu rolleri sona erdiren hususların (emeklilik, atama, görevlendirme gibi) olması durumunda, bu rollerin gerektirdiği erişim yetkilerine hızlı bir şekilde son verilmesi çok önemlidir. Bu kapsamda, bireysel olarak sahip olunan tüm rollerin ve erişim yetkilerinin envanterinin tutulması ve personelin kurum veya birimden ayrılmadan önce erişim yetkilerinin sona erdirilmesine yönelik uygulamaların yürütülmesi tavsiye edilmektedir. Ayrıca, kurum çalışanlarının güvenirliliklerin izlenmesi ve gerekli görüldüğünde erişim yetkilerinin sınırlandırılması veya kaldırılmasına yönelik süreçlerin oluşturulması önerilmektedir.

Gizlilik dereceli belgelerin yönetimi kapsamında alınan güvenlik önlemleri ve uygulamalara yönelik farkındalığın sağlanması maksadıyla verilecek eğitimlere ait koordinasyon ve stratejiler Cumhurbaşkanlığı tarafından belirlenmekte olup, kamu kurumlarınca alınan kurumsal güvenlik önlemlerini kapsayan açıklamalar çalışanlara tebliğ edilebilmektedir (Gizlilik Dereceli Belgelerde…,2022). Bununla birlikte özel güvenlik gerektiren belgelere yönelik, personele, güvenlik temelinde oluşturan kurumsal politikalar ve güncel tedbirler ile yetkilerin gerektirdiği sorumlulukların ve hal

tarzlarının tebliğ edilerek kayıt altına alınması tavsiye edilmektedir. Özel güvenlik gerektiren belgelerin korunmasına yönelik sadece fiziki ve teknolojik önlemlerin alınması yeterli değildir. Belge yönetim süreçlerinde yetkili olan personelin görevlerini kurumsal güvenlik politikalarına saygılı ve bağlı olarak yapması olası güvenlik ihlallerinin engellenmesi veya ortadan kaldırılmasındaki en önemli silahtır. Bu kapsamda, kurumsal gizlilik politikalarını da kapsayan, kurum çalışanlarına güvenlik eğitimleri veya konferansları verilerek kurumsal olarak gizlilik kültürünün oluşturulması sağlanmalıdır (Özdemirci ve Torunlar, 2015, s.56).

7.3. DENETİM VE İYİLEŞTİRME

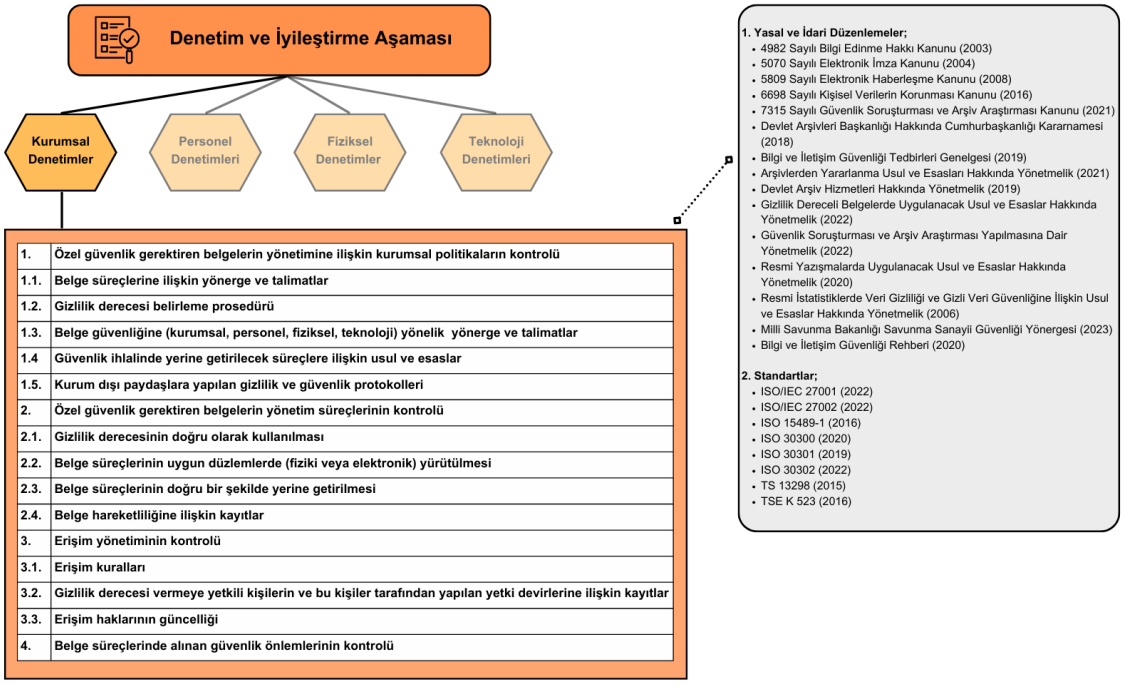
Yönetim fonksiyonlarının bir bileşeni olan denetim, kurumsal faaliyetlerinin önceden belirlenen hedef ve kurallara uygun bir şekilde yürütülüp yürütülmediğinin tespit edilmesi maksadıyla yapılan bir incelemelidir (Bozkurt, 2013, s.57). Yönetimin sorumluğunda bulunan denetim faaliyetleri iç denetim ve dış denetim olarak ayrılmakta olup, iç denetim kurumların organik yapısında bulunan yapılarla, dış denetim ise kurum yapında bulunmayan kurum, kuruluş veya kişiler tarafından yürütülen faaliyetlerdir (Aslan, 2010, s.64). Türkiye'de iç denetim uygulamalarına yönelik bir çok yasal ve idari düzenleme yapılmış (İç Denetçilerin Çalışma…, 2006; Kamu İç Denetim…, 2013; Kamu Malî Yönetimi…, 2003) ve kamu kurumlarında doğrudan üst yöneticiye bağlı iç denetim birimi başkanlıkları veya iç denetçi mekanizmaları oluşturulmuştur. Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde (2019) Bilgi ve İletişim Güvenliği Rehberinin uygulanmasına yönelik denetim mekanizmalarının oluşturulması ve bu uygulamanın yılda en bir kez denetleneceği belirtilmektedir. Kamu kurumları tarafından söz konusu rehberin uygulanmasına yönelik denetimlerin yapıldığı yıllık faaliyet raporlarında görülmüştür. Çalışma kapsamında yapılan incelemede, gizlilik dereceli belge süreçlerinin ve alınması gereken güvenlik önlemlerinin değerlendirilmesine ilişkin bir denetleme mekanizmasından söz edilmemiştir. Bu kapsamda, model önerisinin son aşamasını oluşturan denetim ve iyileştirmelere yönelik uygulama örneklerinin kamu kurumlarının iç denetim mekanizmalarına veya denetleme ve değerlendirme süreçlerine entegre edilmesi tavsiye edilmektedir.

Modelin bu aşamasında kurumsal denetim mekanizmasının yapısında bulunan denetlenecek birimlerin ve denetimde görevli olacakların belirlenmesi, denetçilerin sorumlulukların tanımlanması, denetim sürecinin gerçekleştirilmesi, denetim raporunun

hazırlanması ve denetim sonuçlarının değerlendirilmesi süreçleri kapsam dışında tutulmakla olup, gizlilik dereceli belgelerin kurumsal bilgi güvenliği yönetim sistemi ve gizlilik politikası ile yürürlükte bulunan yasal ve idari düzenlemelere göre uygun ve güvenli bir şekilde yönetilmesine yönelik standartların belirlenmesi amaçlanmaktadır. Bu kapsamda, modelin bu aşaması kurumsal denetimler, personel denetimleri, fiziksel denetimler ve teknoloji denetimleri olarak dört bileşenden oluşmaktadır. Söz konusu denetimler personel güvenirliğini ilgilendiriyorsa personel denetimleri, fiziksel varlıklar ile ilgilisiyle fiziksel denetimleri, bilgisayar donatım, yazılım ve ağ hususlarını ilgilendiriyorsa teknolojik denetimleri ve diğer hususlar ise kurumsal denetimler bileşeninin kapsamına girmektedir.

7.3.1. Kurumsal Denetimler

Özel güvenlik gerektiren belgelerin yönetimine ilişkin önerilen modelde, kurumsal politikaların geliştirilmesi, bu politikaların yetkili yönetici tarafından onaylanması, kurumsal olarak paylaşılması, değişen yasal ve idari düzenlemeler ile standartlarda yapılan değişikliklerle birlikte güncellenmesi önerilmiştir. Bu politika, belge yönetim süreçlerinin gereksinimlerini, yasal ve idari düzenlemelere uyumlu yönerge ve özel talimatları, süreçlerin kim tarafından ve nasıl gerçekleştirileceğini, mevcut güvenlik önlemlerini, öngörülen güvenlik risklerini, erişim yönetimini, belgenin ve belgenin bulunduğu fiziksel mekanlar ile bilgisayar donanım, yazılım ve ağ güvenliği ile güvenlik ihlallerinde yerine getirilecek hususlara yönelik usul ve esasları içermelidir. Ayrıca bu politika, özel güvenlik gerektiren belge yönetim süreçlerinin yürütüldüğü ortamlarda geçici olarak bulunacak veya çalışacak olan kurum dışı paydaşlar ile kurum arasında güvenlik veya gizlilik sözleşmesinin yapılması ve paydaşlar tarafından yerine getirilen eylemlerin bu protokol çerçevesinde yapıldığının kontrol edilmesine yönelik prosedürleri içermelidir. Kurumsal politika kapsamında önerilen söz konusu hususların gerçekleştirilmesine ilişkin modelde belirtilen süreçlerin kontrol edilmesine yönelik uygulama örnekleri ve bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 47'de sunulmaktadır.



Şekil 47. Kurumsal Denetimler Bileşeni

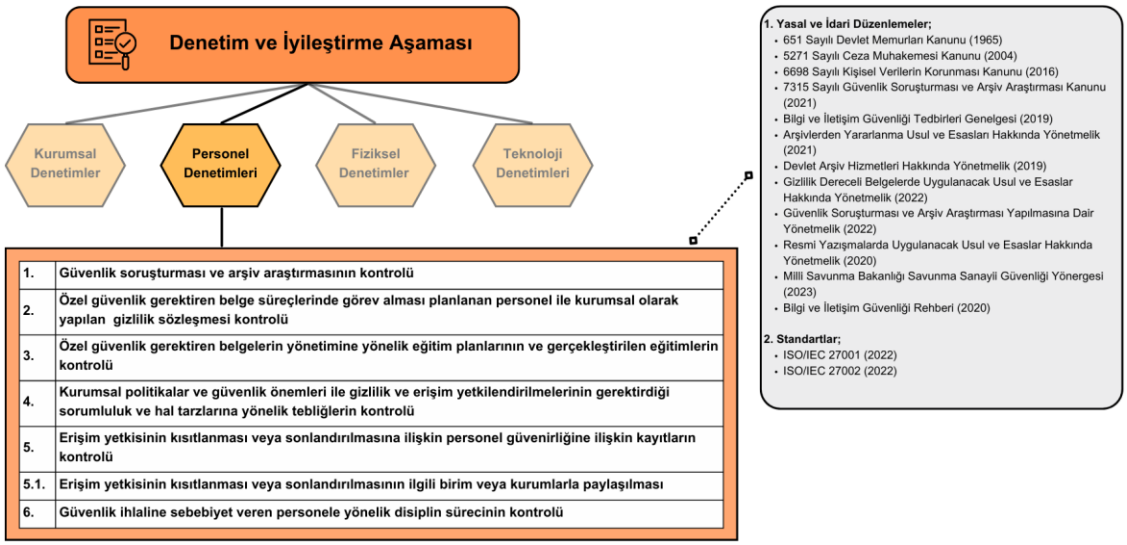
Gizlilik dereceli belgelerin yönetim süreçleri bir belgelenin bir gizlilik derecesiyle ilişkilendirilmesi başlamaktadır. Gizlilik derecesinin belirlenmesinden sonra belgeler uygun düzlemlerde (fiziki veya elektronik) varlık bulmalıdır. Belgeler sahip olduğu gizlilik derecesine göre uygun mekânlarda üretilmeli ve muhafaza edilmeli, yetkili kişiler tarafından onaylanmalı, teslim alınmalı, paylaşılmalı, muhafaza edilmeli, çoğaltılmalı, tercüme edilmeli, alıntılanmalı, gizlilik derecesi düşürülmeli/kaldırılmalı, imha edilmeli veya arşivlenmelidir. Gizlilik dereceli belgelerin üzerinde veya üst verisinde bulunması gereken gizlilik işaretinin, güvenlik numarasının, sayfa ve nüsha sayısının, çoğaltma, tercüme, alıntılama ve gizlilik derecesi düşürme/kaldırmaya ilişkin kayıtların kontrolünün yapılması gerekmektedir. Belgelerin hareketliğine ilişkin kayıtlar bu amaçla oluşturulmuş formlara (Çok Gizli Belge Devir-Teslim Tutanağı, Çok Gizli Belge Büro, İşlem ve Kurye Personeli İmza Örnekleri Listesi, Çok Gizli Belge Yetki Listesi, Giden/Gelen Çok Gizli Belge Kayıt Defteri, Çok Gizli Belge Takip Kontrol Formu, Çok Gizli Belge Senedi, Çok Gizli Belge Sayım Listesi, Çok Gizli Belge İmha Tutanağı, Gizli Belge Zimmet Formu) düzenli olarak ithal edilmelidir. Bununla birlikte, bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelerin hareketliliğine ilişkin kayıtların (devir-teslim tutanakları, kayıt defterleri, belge teslim senetleri, imha tutanakları, zimmet formları, fotokopi çekim istek formları) güncel ve düzenli olarak tutulması ve belgenin izlenebilirliği sağlanmalıdır.

Kurumsal gizlilik politikası kapsamında, gizlilik derecesi vermeye yetkili kişiler ve bu kişiler tarafından yapılacak olan yetki devirleri açıkça belirlenmeli, resmi yazı ile kayıt altına alınmalıdır. Özel güvenlik gerektiren belgelere yönelik erişim yetkilerinin bilmesi gereken prensibi temelinde personelin çalıştığı veya ilişkili olduğu birimler düzeyinde verilmesi gerekmektedir. Bu temelde oluşturulan erişim kuralları, bilmesi gereken prensibiyle erişim hakkının tanımlanmış olmasını, erişim yetkilendirmelerinin yetkili kişilerce resmi olarak verilmiş olduğunu, erişimlerin sadece yetkilendirilmiş kişilerce yapıldığını, erişim yetkilerinin gerektirdiği sorumlulukların bilinmesini, erişim kısıtlamalarının veya sonlandırılmasının kayıt altına almasını ve bunun ilgili birimlere bildirilmesini, erişimlere ait kayıtların günlük olarak düzenli bir şekilde tutulmasını kapsamalıdır.

7.3.2. Personel Denetimleri

Belgelerin yönetim süreçlerinin temel unsuru olan çalışanlar en önemli güvenlik risklerinin arasında yer almaktadırlar. Bu sebeple, özel güvenlik gerektiren belge yönetim süreçlerinde yetkilendirilecek çalışanların güvenilirliklerinden tam olarak emin olunması ve bu personelin belge süreçleri uygulamalarına ve güvenlik önlemlerine yönelik farkındalıklarının azami seviyede olması gerekmektedir. Bu bağlamda, özel güvenlik gerektiren belgelere yönelik alınan güvenlik önlemleri ve uygulamalarına ilişkin farkındalığın sağlanması maksadıyla eğitim programının yapılması ve bu eğitimlerin personele verilmesi gerekmektedir. Bununla birlikte, güvenlik temelinde oluşturan kurumsal politikalar ve güncel tedbirler ile verilen gizlilik ve erişim yetkilerinin gerektirdiği sorumlulukların ve hal tarzlarının personele tebliğ edilmesi ve kayıt altına alınması gerekmektedir. Personelin güvenirliliğine yönelik herhangi bir işlem (idari veya adli soruşturma vb.) sebebiyle erişim yetkisinin kısıtlanması veya sonlandırılmasına ilişkin bilgi ve belgelerin kayıt altına alınması ve ilgili birim veya kurumlarla paylaşılması gerekmektedir. Kamu kurumlarına ilk defa atanacak kişiler ile yeniden memuriyet görevine başlayacaklar hakkında arşiv araştırması, gizlilik dereceli birim ve kısımlarda çalışacak personele yönelik güvenlik soruşturması ve arşiv araştırmasının birlikte yapılması gerekmektedir (Gizlilik Dereceli Belgelerde…., 2022; Güvenlik Soruşturması…, 2021; Güvenlik Soruşturması…, 2022). Bununla birlikte, modelde önerildiği gibi, özel güvenlik gerektiren belge süreçlerinde görev alması planlanan personel ile kurumsal olarak bir güvenlik veya gizlilik sözleşmesinin yapılması, bu sözleşmeden sonra gerekli gizlilik ve erişim yetkilendirilmesinin yapılması

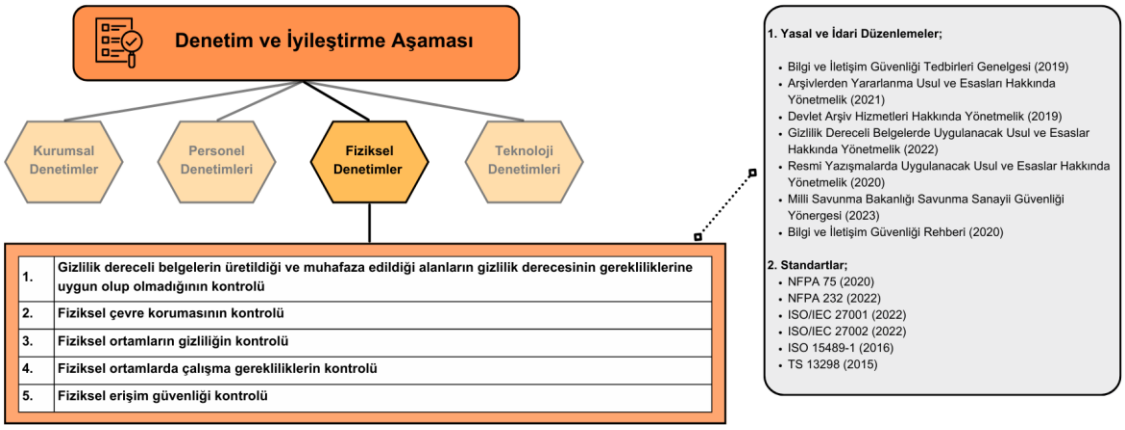
gerekmektedir. Kurumsal gizlilik politikası kapsamında özel güvenlik gerektiren belgelerin güvenlik ihlaline sebebiyet veren personel hakkında yapılan disiplin süreçlerine ait belgelerin kontrolü yapılmalıdır. Bu kapsamda, model önerisinin personel denetimleri bileşenine yönelik uygulama örnekleri ve bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 48'de sunulmaktadır.



Şekil 48. Personel Denetimleri Bileşeni

7.3.3. Fiziksel Denetimler

Özel güvenlik gerektiren belgelerin yönetimi, yasal ve idari mevzuatın gereği olarak gizlilik derecesine göre fiziksel ortamda (ağ bağlantısı bulunmayan ortam) ya da elektronik ortamda (EBYS) farklı güvenlik esaslarına göre yürütülmektedir (Gizlilik Dereceli Belgelerde…, 2022). Kamu kurumlarındaki gizlilik dereceli birim ve kısımlar ile EBYS'ye ait uygulama ve veri depolama için kullanılan sunucuların bulunduğu ortamların mekânsal durumu, doğal afet, yangın, su baskını vb. alt yapılı ihtiyaçları, güvenlik tedbirleri ile erişim yönetimi kapsamındaki gereklilikler birimin ilgili gizlilik derecesine tasarlanmış olması gerekmektedir. Bu kapsamda, model önerisinin fiziksel denetimler bileşenine ilişkin uygulama örnekleri ve bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 49'da sunulmaktadır.



Şekil 49. Fiziksel Denetimler Bileşeni

Gizlilik dereceli belgelerin üretildiği ve muhafaza edildiği alanların gizlilik derecesinin gerekliliklerine uygun olup olmadığının kontrolü kapsamında, gizlilik dereceli belgelerin bulunduğu alanların (Çok Gizli Belge Bürosu, güvenli alanlar ve EBYS'lere ait uygulama ve veri depolama için kullanılan sunucuların bulunduğu alanlar) ilgili gizlilik derecesinin gerekliliklerine göre tasarlanmış ve donatılmış olması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022).

Fiziksel çevre korumasının kontrolü kapsamında, özel güvenlik gerektiren belgelerin muhafaza edildiği alanların doğal afet, su basması, yangın, hayvan tahribatı gibi fiziksel ve çevresel tehditlerin potansiyel sonuçlarını belirlemek için risk değerlendirilmesi yapılmalı, uygun koruma kontrolleri tanımlanmalı ve kurtarma planları yapılmalıdır (Devlet Arşiv Hizmetleri…, 2019; Gizlilik Dereceli Belgelerde…, 2022; NFPA 75, 2020; NFPA 232, 2022).

Fiziksel ortamların gizliliğin kontrolü kapsamında, gizlilik dereceli belgelerin üretildiği ve muhafaza edildiği gizlilik dereceli birim ve kısımlar ile bilgi işlem sunucularının bulunduğu fiziksel ortamların tesis içerisindeki yeri bilmesi gereken prensibine göre yetkili personel tarafından bilinmesi sağlanmalıdır (Gizlilik Dereceli Belgelerde…, 2022; ISO/IEC 27002, 2022).

Fiziksel ortamlarda çalışma gerekliliklerin kontrolü kapsamında, özel güvenlik gerektiren belgelerin üretildiği ve muhafaza edildiği ortamlarda çalışmak için güvenlik önlemleri tasarlanmalı ve uygulanmalıdır. Güvenlik ve kaza risklerinin azaltılması maksadıyla, söz konusu ortamlarda yürütülecek belge yönetim süreçleri ile diğer işlemlerin mesai bittikten sonra devam etmesi halinde, bu durumun bilinmesi ve kayıt

altına alınması gerekmektedir. Mesai bitiminde odayı en son terk eden personel tarafından gerekli güvenlik tedbirlerinin kayıt altına alınarak kapının kilitlenmesi ve bu hususun başka bir güvenlik sağlayıcısı (güvenlik personeli, nöbetçi personel) tarafından kontrol edilmesi önerilmektedir. Gizlilik dereceli birim ve kısımlara erişim sağlayan kişilerin yanlarında fotoğraf makinesi, video kamerası, cep telefonu, bilgisayar gibi veri ve bilgi transferi yapabilecek kayıt cihazları ile güvenlik zafiyetine neden olabilecek silahların bulunmaması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022; ISO/IEC 27002, 2022).

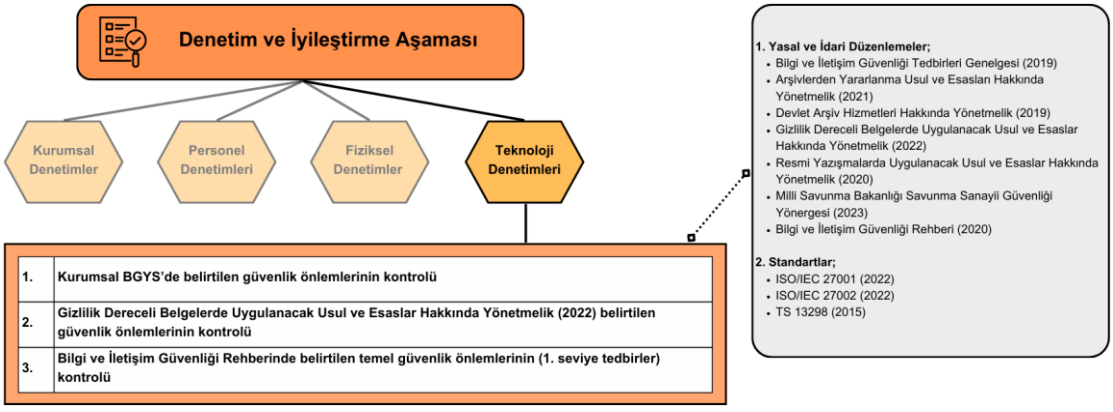
Fiziksel erişim güvenliği kontrolü kapsamında, özel güvenlik gerektiren belgelerin bulunduğu dolap, kasa ve odalara yönelik fiziksel erişim engelleri oluşturulmalı ve erişim güvenliği sağlanmalıdır. Bu bağlamda, özel güvenlik gerektiren belgelerin bulunduğu birim ve kısımlara girmeye yetkili kişilerinin belirlenerek kayıt altına alınması, oda ve dolap anahtarlarının sınırlı sayıda çoğaltılması ve kayıt altına alınması, belgelerin muhafaza edildiği dolapların içerisinde ne olduğunu anlaşılamayacak, kolaylıkla tahrip edilemeyecek (demir, çelik malzemeden oluşan), açılamayacak (dolapların çift kilitli olarak tasarlanması) ve taşınamayacak (dolapların duvara veya yere monte edilmesi) şekilde dizayn edilmesi, erişim kartı ve şifre gibi iki faktörlü kimlik doğrulamanın kullanımı, temizlik, bakım ve onarım gibi işlerin gizlilik dereceli birim veya kısım personelinin refakatinde yapılması, bu işlerin kayıt altına alınması ve bu işlerden önce belgelerin görülemeyecek şekilde muhafaza edilmiş olması gerekmektedir. Söz konusu dolap, kasa ve oda anahtar, manyetik kart ya da şifreler gizlilik dereceli belge niteliğinde muhafaza edilmelidir (Gizlilik Dereceli Belgelerde…, 2022; ISO/IEC 27002, 2022; Milli Savunma Bakanlığı…, 2023).

7.3.4. Teknoloji Denetimleri

Gizlilik dereceli belgelerin yönetim süreçleri kapsamında kullanılan bilgisayarların donatınım ve yazılım bileşenlerinin kurumsal BYGS ile Bilgi ve İletişim Güvenliği Rehberi ile çerçevelenen temel ilkelere (1. seviye tedbirler) uygun olarak kullanılması gerekmektedir (Gizlilik Dereceli Belgelerde…, 2022, mad. 9). Model önerisinin teknoloji denetimleri bileşenine ilişkin uygulama örnekleri ve bu bileşene esas teşkil eden yasal ve idari düzenlemeler ile standartlar Şekil 50'de sunulmaktadır. Bu bileşen kapsamında kurumsal BGYS, Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022) ve Bilgi ve İletişim Güvenliği Rehberi'nde (2020) belirtilen güvenlik

önemlerinin alınması gerekmektedir. Söz konusu yönetmelik ve rehberde belirtilen güvenlik önlemlerine ilave olarak özel güvenlik gerektiren belgelerin güvenliğinin sağlanması kapsamında kurumsal BGYS'nde bulunması önerilen güvenlik tedbirleri şunlardır:

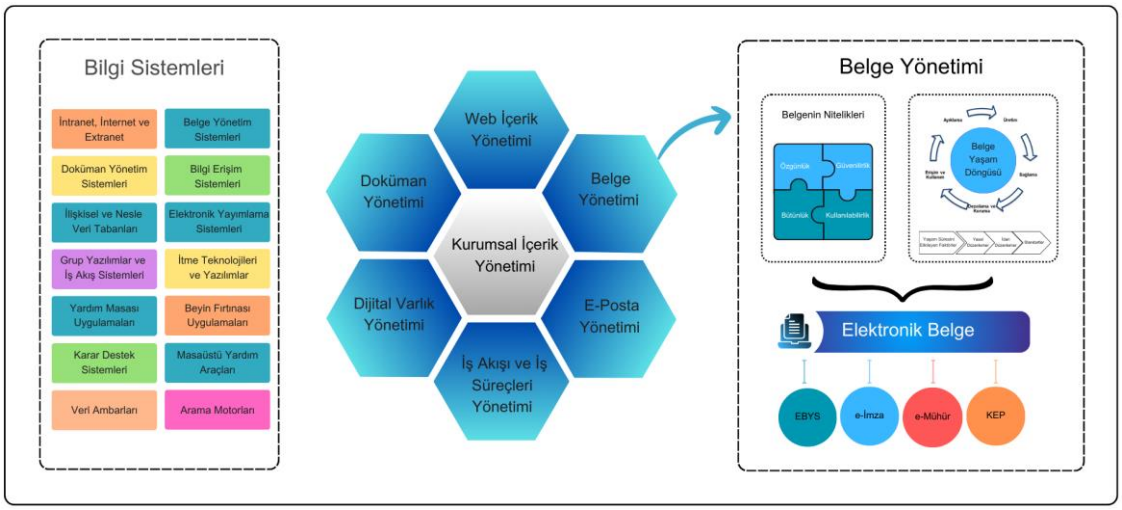
- Yazılım güvenliğine yönelik yetkili kullanıcılar haricinde bilgisayara yazılım yüklemesinin engellenmesi ve yapılan bu uygulamanın kayıt altına alınması,
- Donanım güvenliğine yönelik, bilgisayar donanımlarına ilişkin bakım ve onarım ile ilgili işlemlerin sadece yetkili teknik personel tarafından yürütülmesi ve yetkisiz personelin bu işlemleri yaptığının tespit edilmesine yönelik önlemlerin (kasa açılış yerlerinin etiketlenmesi vb.) alınması,
- Bilgisayar ve veri depolama aygıtlarının kurum dışına çıkışının kayıt altına alınması,
- Onarım maksadıyla kurum dışına çıkarılacak bilgisayarların sabit disk ve hafıza kartlarının çıkarılması,
- Bilgisayarların ve veri depolama aygıtlarının içerdikleri gizlilik derecesine göre etiketlenmesi,
- Veri depolama aygıtlarının sadece yetkili kişilerce kullanılması ve kullanımlarının kayıt altına alınması tavsiye edilmektedir.



Şekil 50. Teknoloji Denetimleri Bileşeni

SONUÇ VE ÖNERİLER

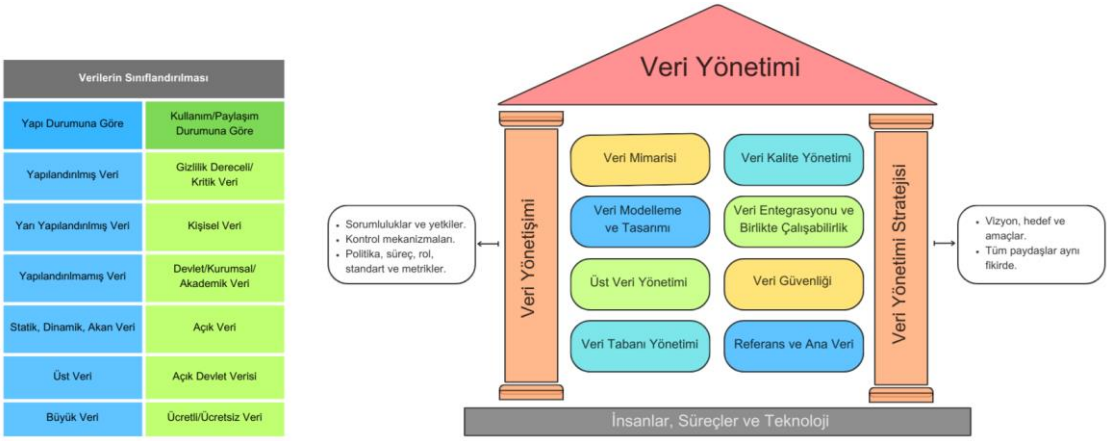
Bilgi ve iletişim teknolojisinin gelişmesiyle birlikte kamu kurum ve kuruluşlarında veri, bilgi ve belgelerin oluşturulması, elde edilmesi, işlenmesi ve paylaşılması eskiye oranla daha kolay ve hızlı bir şekilde gerçekleştirilmektedir. Kurum ve kuruluşlarda veri, bilgi ve belgeler farklı iş süreçlerinde ve farklı sistemlerle çeşitli kurumsal yapılarda varlık bulmaktadırlar. Bu bağlamda, kurumsal bilgi sistemleri, kurumsal içerik yönetim sistemleri, belge yönetimi ve elektronik belgeye yönetimi uygulamaları ve bunların gereklilikleri çalışmamız kapsamında literatüre dayalı olarak kavramsallaştırılmış ve Şekil 51'de gösterilmiştir.



Şekil 51. Kurumsal Veri, Bilgi ve Belgelerin Varlık Bulduğu Sistemler

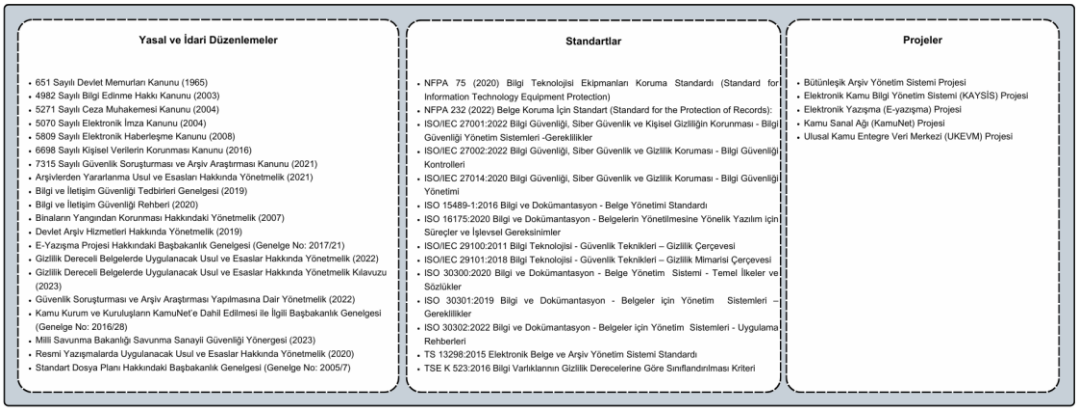
Kamu kurum ve kuruluşları iş süreçlerini yerine getirirken ve diğer kurum, kuruluş ve vatandaşlarla ile etkileşimlerinde çok çeşitli ve büyük miktarda veri üretmekte veya sağlamaktadırlar. Veriler kurum personeli ya da bilgi sistemleri tarafından kurumun faaliyet alanına ve amacına uygun hale gerilerek kamusal bilgi ve belgeye dönüştürülmektedir. Değerli bilgi kaynağı olan verilerin önemin fark edilmesi, bilgiye erişim süreçlerinin değişmesi, bilgi edinme hakkı, yönetimde şeffaflık, toplumun yönetime katılımı, hesap verilebilirlik, bilgi toplumu ve bilgi ekonomisi, e-devlet, açık erişim, açık veri ve açık devlet verisi olgularının sonucu olarak kamu kurum ve kuruluşları verilerine ilişkin anlayışlarını değiştirmiştir. Kamu kurum ve kuruluşlarında, kişisel veriler, ulusal güvenliği tehlikeye sokacak veriler, fikri mülkiyet kapsamındaki veriler, ekonomik değeri olan veriler gibi paylaşılması durumunda devletin ve kişilerin menfaatlerine zarar verebilecek veriler bulunmaktadır. Bu sebeple verilerinin

paylaşılmasının getireceği büyük faydaların yanı sıra, korunmasını gerektiren hususlar da bulunmaktadır. Bu bakış açısıyla, veri uygulamaları çalışmamız kapsamında literatüre dayalı olarak kavramsallaştırılmış ve Şekil 52'de gösterilmiştir.



Şekil 52. Veri Uygulamaları

Kamu kurum ve kuruluşları faaliyetlerini yasal ve idari düzenlemelerle yerine getirmektedir. Söz konusu düzenlemeler ile kamu kurum ve kuruluşları tarafından gerçekleştirilen projelerde ulusal ve uluslararası standartlara uyum sağlanacağı belirtilmiştir. Çalışmamız kapsamında Şekil 53'de gösterilen yasal ve idari düzenlemeler ile standart ve projeler incelenmiş olup, bunlar model önerisinin temelini oluşturmuştur.



Şekil 53. Veri, Bilgi ve Belge Yönetimi Kapsamında İncelenen Yasal ve İdari Düzenlemeler ile Standart ve Projeler

Türkiye'de özel güvenlik gerektiren belgelerin yönetimine yönelik yapılan yasal ve idari düzenlemeler ile geliştirilen uygulamalar doğrultusunda, içerdikleri bilgilerin hassasiyetliklerine göre belgelere gizlilik sınıflandırılması yapılmaktadır. Gizlilik dereceli belgelerin yönetim süreçleri ile güvenlik ve erişim düzenlemelerine yönelik temel gereklilikler belirlenmiştir. Gizlilik sınıflandırılması yapılmayan belgelerin yönetim süreçleri ise sadece bilmesi gereken prensibiyle gerçekleştirilmektedir. Gizlilik sınıflandırılması yapılmayan belgelerin bilmesi gereken prensibi dışındaki tüzel veya gerçek kişilerle paylaşımı, Bilgi Edinme Hakkı Kanunu çerçevesinde yapılan talebin değerlendirilmesi sonucunda yapılmaktadır. Çalışmamız kapsamında yapılan incelemede, gizlilik sınıflandırılması yapılmayan fakat özel güvenlik gerektiren belgelerin (hukuki belgeler ile kişisel bilgileri içeren sağlık belgeleri, eğitim belgeleri, mali belgeler vb.) yönetimine ilişkin belge süreçlerine, alınması gereken güvenlik önlemlerine, bilgisayar donanım ve bileşenlerinin ne şekilde kullanılacağına yönelik standart uygulamaların ve politikaların geliştirilmediği görülmüştür. Bu bağlamda, araştırmanın ana hipotezinin "*Türkiye'de, kamu kurumlarında kamusal bilgi ve veri yönetimi politikaları çerçevesinde özel güvenlik gerektiren belgelerin yönetimine dönük bütünsel (holistic) politikalar oluşturulmadığı için ilgili belge serilerine dönük gizlilik derecelerinin tanımlanması, bu belgelerin düzenlenmesi, kullanımı, arşivlenmesi korunması ve süreçlerde teknolojik araçların kullanımında belirsizlikler yaşanmaktadır"* doğrulandığı görülmektedir.

Türkiye'de yasal ve idari düzenlemelerde veri, bilgi ve belge gizliliğine ilişkin hükümler bulunmaktadır. Bu düzenlemelerde çok farklı konu ve alanlarda sır ve gizlilik hususları belirtilmekte olup, bu kavramlar sıklıkla birlerinin yerine kullanılmıştır. Sır ve gizlik nedenlerinin, devletin dış ilişkilerinin, millî savunmasının, millî güvenliğinin ve müttefiklerle olan faaliyetlerinin, menfaatlerinin, güvenlik, istihbarat ve teknoloji faaliyetlerinin ve kişisel mahremiyetin korunmasına yönelik olgulardan oluştuğu görülmüştür. Kamu kurum ve kuruluşları tarafından üretilen, iş süreçlerinde kullanılan ve paylaşılan veri, bilgi ve belgelerin güvenliğinin sağlanması maksadıyla gizlilik sınıflandırılması yapılarak yetkisiz kişilerin erişimi engellenmektedir. Söz konusu erişim engeli kurum dışı paydaşlara ve kurum içerisinde bilmesi gereken prensibine göre kurum personeline uygulanmaktadır. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022) ile üç adet milli gizlilik derecesi (Çok Gizli, Gizli ve Özel) belirlenmiştir. Bu gizlilik derecelerinin sadece belgelere yönelik olduğu, belgelerin varlık bulduğu bilgisayar donatım ve işletim sistemleri ile veri kayıt cihazlarını, yürütülen

faaliyet ve projeleri kapsamadığı tespit edilmiştir. Ayrıca, bir kaç standart ve idari düzenlemede veri, bilgi ve belgelerin güvenliğine yönelik gizlilik dereceleri belirlenmiş olup, bu gizlilik derecelerinin sadece ilgili standart ve idari düzenlemelerle sınırlı olduğu görülmüştür (Cumhurbaşkanlığı Dijital Dönüşüm…, 2020a; Milli Savunma Bakanlığı…, 2023; Resmi İstatistiklerde Veri…, 2006; TS 13298, 2015; TSE K 523, 2016). Bu kapsamda, milli gizlilik derecelerinin sadece belgelere yönelik olduğu, bir bütün olarak veri, bilgi ve belgelere yönelik nesnel ölçütleri içeren ulusal çapta gizlilik sınıflandırma standartlarının bulunmadığı tespit edilmiştir. Bu bağlamda, araştırmanın "*Veri, bilgi ve belgelere yönelik yapılan gizlilik sınıflandırılması, ulusal güvenlik ve uluslararası menfaatler ile kişisel mahremiyetin korunması amacıyla yetkisiz erişimin engellenmesi ile ilgili düzenlemeler yetersizdir*" alt hipotezi doğrulanmıştır.

Bir belgeye gizlilik sınıflandırması yapılması, kurumsal ve kişisel gizliliğin resmi olarak tespit edilmesine yönelik bir prosedür olmakla birlikte, kişilerin bilgi edinme hakkını kısıtlayan ve idari işlemlere yetkililik kazandırma sürecidir. Kişisel, kurumsal, ulusal ve uluslararası menfaatlerin korunması amacıyla yapılan gizlilik sınıflandırılması aynı zamanda gizlilik dereceli belge yönetiminin çekirdeğini oluşturmaktadır. Çalışma kapsamında yapılan literatür incelemesinde yasal ve idari düzenlemeler ile standart ve rehberlerde, veri, bilgi ve belgelere yönelik temelde aynı amaçla farklı gizlilik düzeyleri tanımlanmıştır. Gizlilik belgelerin yönetimi bağlamında belgelere yönelik "Çok Gizli", "Gizli" ve "Hizmete Özel" olmak üzere üç adet milli gizlilik derecesi belirlenmiştir (Gizlilik Dereceli Belgelerde…,2022). Belgelerinin gizlilik düzeylerine göre standart şekilde sınıflandırmasının amacı, gizlilik dereceli belge yönetim süreçlerinin gizlilik derecesinin gerektirdiği düzeylerde gerçekleştirilmesi ile muhafaza, güvenlik ve erişim yönetimlerinin tutarlı bir şekilde sürdürülmesidir. Kamu kurum ve kuruluşlarında üretilen belgelerin gizlilik sınıflandırılma gereklilikleri ve hangi belgelerin hangi gizlilik derecesiyle ilişkilendirileceği belirlenmiştir. Gizlilik derecesinin doğru kullanımı belge yönetimi süreçlerinin verimli bir şekilde yönetilmesini, hesap verilebilir ve şeffaf bir yönetim anlayışının etkin bir şekilde sürdürülebilmesini ve bilgi edinme taleplerinin doğru bir şekilde karşılanmasını sağlamaktadır. Gizlilik derecesinin yanlış kullanımı ise iş süreçlerinin yoğunluğunun ve maliyetinin artmasına, yerine getirilen faaliyetlerin gecikmesine, güvenlik ve hak ihlallerinin yaşanmasına sebep olmaktadır.

Erişim düzenlemeleri temelde yetkili kişilerin ilgili belgelere erişim sağlamaları, yetkisiz kişilerin ise bu belgelerle ilişkisinin kesilmesi esasına dayanmaktadır. Erişim

düzenlemeleri kapsamında, kamu kurum ve kuruşlarında bir belgenin ilgili gizlilik derecesiyle ilişkilendirilmesi ve bir personelin bilmesi gereken prensibine göre bir gizlilik düzeyi ile yetkilendirilmesi aynı makam veya kişi tarafından yapılmaktadır. Bilginin hassasiyetlik derecelerindeki farklılık, söz konu yetkilendirme düzeylerini de etkilemiştir. Kurum çalışanlarının gizlilik dereceli belgelere erişim sağlayabilmesi için sahip olması gereken temel gereklilikler yasal ve idari düzenlemelerle belirlenmiştir. Bu düzenlemeler; bilmesi gereken prensibine göre personelin erişim yetkisi alacağı birimde çalışması (Gizlilik Dereceli Belgelerde…, 2022), ilgili gizlilik düzeyi çerçevesinde yetkili yönetici tarafından gizlilik yetkilendirilmesinin yapılması (Gizlilik Dereceli Belgelerde…, 2022), güvenlik soruşturması ve/veya arşiv araştırmasının yapılmış olmasıdır (Güvenlik Soruşturması…, 2022). Ayrıca, bir gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelere yönelik erişimler, bilmesi gereken prensibi temelinde kurumsal yetkilendirmelere göre yapılmaktadır. Bu belgelerin bilmesi gereken prensibi dışında, tüzel veya gerçek kişilere paylaşılması ise Bilgi Edinme Hakkı Kanunu (2003) kapsamında yapılacak talebin incelenmesi sonucunda yapılmaktadır (Gizlilik Dereceli Belgelerde…, 2022, mad. 31). Bu bağlamda, araştırmanın "*Gizlilik sınıflandırılmasının yapılması ve personelin erişim yetkilendirilmesi sürecindeki tutarsızlıkların önüne geçilebilmesi için belgeyi üreten birim düzeyinde tüm kurumsal yapılarda süreçlerin tanımlanması, gizlilik düzeylerine göre kişi ve makamların yetkilendirmelerinin yapılması gerekmektedir*" alt hipotezi doğrulanmıştır.

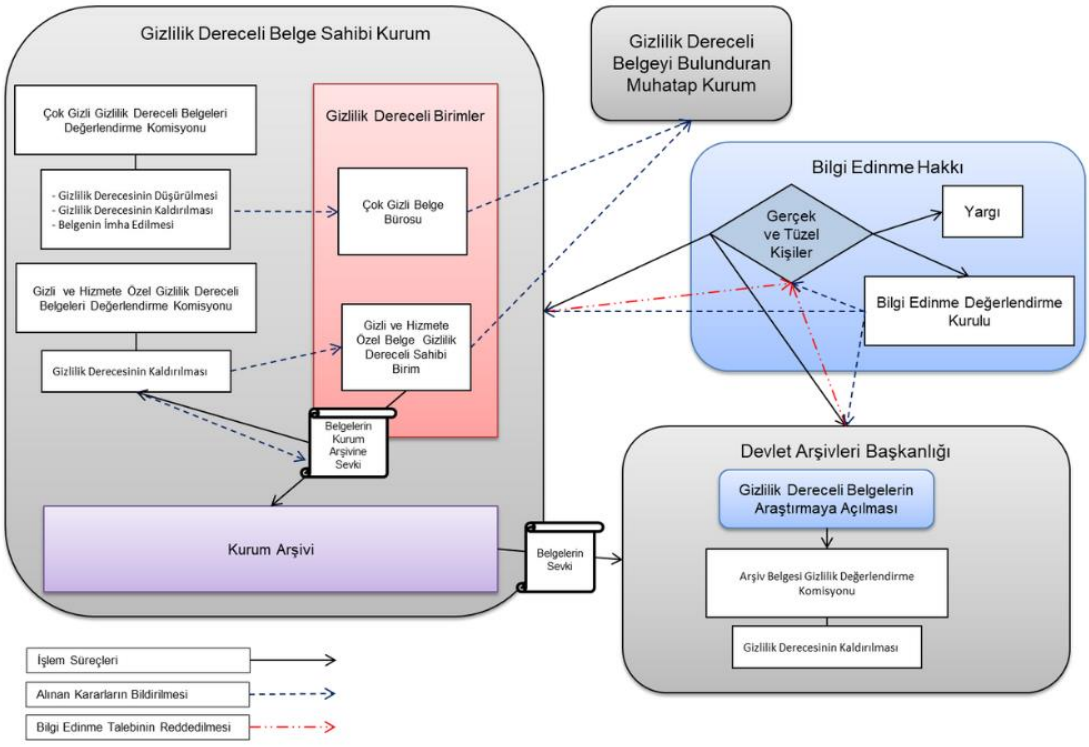
Gizlilik süresi, gizlilik sınıflandırılmasının son bulacağı zamanı ifade etmekle birlikte, ulusal ve kişisel gizlilik değerinin zamanla azalacağı gerçeğini yansıtmaktadır. Çalışma kapsamında yapılan incelemede, yasal mevzuat ve idari düzenlemelerde belgelerin gizlilik sürelerine yönelik ifadeye yer verilmediği görülmüştür. Bununla birlikte, belgelerin gizliliğine yönelik süreli gizlilik yönteminin belirlendiği tespit edilmiştir. Süreli gizlilik uygulaması, gizlilik durumun sona ereceği zamanın veya olayın belgelerin üretilmesi sırasında karar verilmesidir. Belirlenen zamana gelindiğinde veya olay gerçekleştiğinde/sona erdiğinde belge üzerindeki veya EBYS'nin üst verisinde bulunan talimata göre gizlilik derecesi düşürülmekte, kaldırılmakta ya da belge imha edilmektedir. Süreli gizlilik uygulaması kapsamında, belirlenen gizlilik süresinin en fazla ne kadar olacağı veya olay hakkında nesnel ölçütün ne olacağı belirtilmemiştir. Bu bağlamda, süreli gizlilik uygulamasında süre ve olay olgularının kurum ve kuruluşların takdirine bırakıldığı görülmüştür. Bu bağlamda, araştırmanın "*Uygulamada gizlilik*

sınıflandırılması yapılan belgelerin gizliliğinin en fazla ne kadar süre devam edeceği belirsizdir" alt hipotezi doğrulanmıştır.

Gizlilik dereceli belgeyi üreten ve bu belgeyi ilk defa bir gizlilik derecesiyle ilişkilendiren kurum ve kuruluşlar tarafından gizlilik dereceli belgelerin gizlilik derecesinin değerlendirilmesi, düşürülmesi veya kaldırılması ile bu belgelerinin imha edilmesi kararları alınmaktadır. Söz konu kararlar, kurum ve kuruluşların organik yapılarından oluşturulan "Gizlilik Dereceli Belgeleri Değerlendirme Komisyonları" tarafından verilmektedir. Arşivleri Başkanlığına sevk edilen ve burada arşivlenen belgeler, arşive aktarıldıkları sırada sahip oldukları gizlilik derecesini korumakta olup, bu gizliliğin kaldırılmasına yönelik karar ilgili kurum, kuruluş ve idarenin görüşü alındıktan sonra Devlet Arşivleri Başkanlığınca verilmektedir. Devlet Arşivleri Başkanlığına devredilen gizlilik dereceli arşiv belgelerinin araştırmaya açılması kapsamında, yapılacak gizlilik değerlendirilmesi ve bu gizliliğin kaldırılma işlemleri Devlet Arşivleri Başkanlığı tarafından oluşturulan "Arşiv Belgesi Gizlilik Değerlendirme Komisyonu" tarafından yürütülmektedir. Gizlilik dereceyi belgeyi üreten kurum ve kuruluşun yetkili temsilcisi bu komisyonun doğal üyesi olarak görev yapmaktadır. Bu bağlamda, araştırmanın "*Türkiye'de, belgelerin gizlilik derecesinin düşürülmesi, kaldırılması veya belgenin imha edilmesine yönelik, belgeyi oluşturan kamu kurumunu merkeze alan bir politika bulunmaktadır*" alt hipotezi doğrulanmıştır.

Gizlilik dereceli belgelerin yönetimiyle ilişkili olarak, kamu kurum ve kuruluşlarında hangi birimlerin gizlilik dereceli birim olduğu, belgelerin gizlilik derecesinin değerlendirilmesi, gizlilik derecesinin düşürülmesi/kaldırılması ile imha edilmesi, arşiv belgelerinin gizlilik niteliğinin değerlendirilmesi ve uygun görülmesi halinde gizlilik derecesinin kaldırılması ve bilgi talebi itirazlarına yönelik belge sahibi kurum haricinde farklı yapılar oluşturulmuştur. Gizlilik dereceli belgelerin yönetimine ilişkin oluşturulan bu yapılar farklı kurumsal düzlemlerde ve farklı amaçlarla iş süreçlerini yerine getirmektedir. Bu yapıların gizlilik dereceli belgelerin yönetimiyle ilişkileri Şekil 54'de gösterilmiştir. Söz konusu yapıların haricinde Türkiye'de ulusal boyutta; gizlilik sınıflandırılmasına ve gizlilik dereceli belgelerin yönetimi ile gizlilik derecesine sahip olmayan fakat özel güvenlik gerektiren belgelerin yönetimine yönelik standart politika ve uygulamaları geliştirecek, kamu kurum ve kuruluşları tarafından gizlilik dereceli belgelere yönelik oluşturulan kurumsal yönergeleri gözden geçirecek ve onaylayacak, gizlilik dereceli belge yönetim süreçlerinin yasal ve idari düzenlemelere uygunluğunun

denetlemesi için politika ve yönergeler geliştirecek, gizlilik dereceli belgelerin yönetimine ilişkin istatistiki verileri toplayacak, analiz edecek ve raporlayacak, gizlilik dereceli belgelerin yönetimi kapsamında kamu kurum ve kuruluşları ile kişiler tarafından yapılan şikâyet, öneri ve itirazlar hakkında işlem yapacak ve koordinasyonu sağlayacak bir kurul veya komisyon yapısının bulunmadığı tespit edilmiştir. Bu bağlamda, araştırmanın "*Gizlilik dereceli belgelerin yönetimi ile gizlilik dereceli arşiv belgelerinin gizliliğinin kaldırılması ve bilgi edinme hakkının kullanılması kapsamında, ulusal boyutta bir koordinasyon kurulu oluşturulmamıştır*" alt hipotezi doğrulanmıştır.



Şekil 54. Gizlilik Dereceli Belgelerin Yönetimiyle İlişkili Yapılar

Türkiye'de gizlilik dereceli belgelerin yönetimi, belgelerin sahip olduğu gizlilik derecesine göre farklı ortamlarda ve farklı güvenlik düzeylerinde gerçekleştirilmektedir. Hizmete özel gizlilik dereceli belgelerin yönetimi olağanüstü durumlar haricinde elektronik ortamlarda diğer gizlilik dereceli belgelerin yönetimi ise fiziki ortamlarda gerçekleştirilmektedir. Bununla birlikte, elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili olanlar tarafından gerekli güvenlik önlemlerinin alınması şartıyla güvenli e-imza ile onaylanan gizlilik dereceli belgeler elektronik ortamda yönetilebilmektedir. Bu sebeple, gizlilik dereceli belgelerin yönetimi

konusunda farklı kamu kurum ve kuruluşlarında farklı belge yönetim düzlemlerinin oluşturulması gerekmektedir. Aynı kurum ve kuruluşta gizlilik dereceli belgelerin yönetimi fiziki veya elektronik ortamlarda (EBYS), özel olarak oluşturulmuş Çok Gizli Belge Büroları ve güvenli alanlarda gerçekleştirilmelidir. Belgelerin sahip oldukları gizlilik derecesine göre farklı güvenlik düzeylerinde ve ortamlarda yönetilmesi, kurum ve kuruluşlarda hibrit bir belge yönetim süreçlerinin ortaya çıkmasına sebep olmaktadır. Bu bağlamda, "*Gizlilik dereceli belgelerin yönetim süreçlerinin gizlilik derecesinin gerektirdiği farklı ortamlarda ve güvenlik önlemleriyle yapılmasına dönük hibrit belge yönetim uygulamaların geliştirilmesi gerekmektedir*" alt hipotezi doğrulanmıştır.

Araştırmamızın temel araştırma sorusunun "*Kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimi nasıl yapılmalıdır?*" cevaplanması kapsamında konuyla ilgili literatür, yasal ve idari düzenlemeler, standartlar, rehberler incelenmiş ve analiz edilerek betimlenmiştir. Analiz sonuçları ve geliştirilen modeller çerçevesinde kamu kurumlarında özel güvenlik gerektiren belgelerin yönetimine ilişkin bir model önerilmiştir. Model, özel güvenlik gerektiren belgelerin yönetim süreçlerinin tamamlayıcısı rolünde ve birbirleriyle ilişkili olan üç temel aşamada tasarlanmıştır. Modelin ilk aşaması olan politika ve düzenleme bileşeninde, kurumsal politika, gizlilik politikası, erişim düzenlemeleri ve belge güvenliği politikası süreçleri ele alınmıştır. Kurumsal yönetim aşamasında altyapıların yönetimi, özel güvenlik gerektiren belgelerin yönetimi ile süreçlerinin izlenmesi ve iyileştirilmesi bileşenleri ele alınmıştır. Son aşama olan denetim ve iyileştirme unsurunda ise kurumsal denetimler, personel denetimleri, fiziksel denetimler ve teknoloji denetimleri oluşturulmuştur.

Gizlilik dereceli belgelerin yönetilmesi kapsamında oluşturulan yapılar ile yasal ve idari düzenlenmeler incelendiğinde, Türkiye'de gizlilik dereceli belge yönetim uygulamalarının esnetilmeyen bir güvenlik anlayışıyla yürütülmek istendiği görülmüştür. Süreli gizlilik uygulaması ile kurumsal yapılarca oluşturulan Gizlilik Dereceli Belgeleri Değerlendirme Komisyonlarıyla belgelerin gizlilik değerlendirilmesinin yapılarak süresiz bir gizlilik anlayışının kırılması amaçlanmıştır. Gizlilik gerekçesiyle bilgi edinme talebi karşılanmayan bir kişinin, bu karara itiraz edebilmesi kapsamında yargı yolu haricinde başvuru yapabileceği Bilgi Edinme Değerlendirme Kurulunun oluşturulması, kurumlar tarafından gizlilik gerekçesiyle belgelerin tekelleştirilmesinin önüne geçilerek şeffaflığın ve bilgi edinme hakkının etkin olarak kullanılmasının amaçlandığı görülmüştür.

Araştırmamızda elde edilen sonuçlar doğrultusunda Türkiye'de gizlilik dereceli belge uygulamalarına yönelik geliştirilen öneriler aşağıda sunulmaktadır.

- Gizlilik dereceli belge yönetiminin etkinliğini artırmak ve maliyetini azaltmak, gizlilik dereceli belgeleri etkin bir şekilde korumak ve gizlilik değeri kaybolan belgelerin tasnifini zamanında yapmak için gizlilik süresinin açık bir şekilde belirlenmesi gerekmektedir. Bu kapsamda, yasal ve idari düzenlemeler yapılmalıdır.
- Devlet Arşivleri Başkanlığına bağlı olarak çalışacak "Gizlilik Dereceli Belge Güvenliği Kurulu" oluşturulmalıdır. Bu kurul, gizlilik dereceli belge yönetimi ve denetimi için ayrıntılı uygulama kurallarını oluşturmalı, gizlilik ve güvenlik eğitimlerine yönelik politikalar geliştirmeli, gizlilik dereceli belgelerin yönetimine yönelik istatistiki veriler toplamalı, analiz etmeli ve raporlamalı, gizlilik dereceli belgelerin yönetimi ile ilgili araştırma ve geliştirme projelerinin yönetilmesini sağlamalıdır.
- Kamu kurum ve kuruluşları tarafından oluşturulan gizlilik dereceli belgenin yeni bir forma entegre edilmesi, değiştirilmesi veya işlenmesi durumlarında, elde edilen bilgilerden oluşturulan yeni bir belgenin sahip olacağı gizlilik derecesinin belirlenmesine için ikincil/türev gizlilik derecesi belirleme prosedürleri oluşturulmalıdır. Bu prosedürler, belgelerin içerdiği bilgilerin hassasiyetine ve kaynak belgenin gizlilik derecesine dayalı olarak, yeni belgenin gizlilik düzeyini belirlemek amacıyla etkin bir şekilde uygulanmalıdır.
- Belgelerin ilk defa gizlilik derecesiyle sınıflandırılmasına yönelik kurumsal düzeyde bilmesi gereken prensibine dayalı ve süreç tabanlı bir gizlilik derecesi verme prosedürü oluşturulmalıdır. Bu prosedür, belgenin gizlilik sınıflandırmasına esas olan bilgileri içerip içermediğinin tespit edilmesini, belgenin sahip olduğu bilginin hassasiyetlik ve potansiyel zararın ne olacağının belirlenerek sınıflandırmaya ilişkin etki değerlendirilmesinin yapılması ve etki düzeyine göre gizlilik derecesinin belirlenmesini, süreli gizlilik uygulaması kapsamında gizliliğin ne zaman veya hangi olayda son bulacağının belirlenmesini içermelidir.
- Kamu kurum ve kuruluşlarında gizlilik dereceli belgelerin yönetim süreçlerinin ve güvenlik önlemlerinin yetkin bir şekilde gerçekleştirilmesi amacıyla mevcut durumun sürekli olarak gözden geçirmesi ve politikaların güncellenmesi kapsamında, risk yönetimi temeline dayanan, planlı veya plansız olarak denetleme ve değerlendirmeler yapılmalıdır.

- Gizlilik dereceli belge yönetimin başlangıç ve en temel aşamasını oluşturan gizlilik derecesi belirme konusunda belge süreçlerinde yetkili tüm personele kurumsal gizlilik politikası kapsamında yılda en bir kez gizlilik derecesi belirleme eğitimi verilmelidir.

KAYNAKÇA

ABD Başkanı 12958 Sayılı Yürütme Emri (1995). Classified National Security Information. https://www.presidency.ucsb.edu/documents/executive-order-12958-classified-national-security-information.

ABD Başkanı 13526 Sayılı Yürütme Emri (2009). Classified National Security Information. https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

ABD Savunma Bakanlığı (2019). Original Classification Authority (OCA) Desktop Reference. https://www.cdse.edu/Portals/124/Documents/jobaids/information/oca-desktop-reference.pdf?ver=34atHKwTzpR8rPvBoKj8ig%3d%3d

Adeoti Adekeye, W. B. (1997). The importance of management information systems. Library Review, 46(5), 318-327. https://doi.org/10.1108/00242539710178452

AIIM (2023a). What is Enterprise Content Management (ECM)? https://www.aiim.org/resources/glossary/electronic-records-management adresinden 09 Nisan 2023 tarihinde alınmıştır.

AIIM (2023b). What is Electronic Records Management (ERM)? https://www.aiim.org/resources/glossary/enterprise-content-management adresinden 09 Nisan 2023 tarihinde alınmıştır.

AIIM (2023c). What is Web CMS (or WCM)? https://www.aiim.org/what-is-web-20 adresinden 09 Nisan 2023 tarihinde alınmıştır.

AIIM (2023d). What is Email Management? https://www.aiim.org/what-is-email-management-emm adresinden 09 Nisan 2023 tarihinde alınmıştır.

Akgün, A. Ç. ve Çiçek, N. (2022). Dijital Çağda değişen belge olgusunun arşivcilikte düzenleme ve tanımlamaya etkisi: Literatüre dayalı bir inceleme. *Bilgi ve Belge Araştırmaları,* (17), 33-58. https://doi.org/10.26650/bba.2022.17.1127615

Alberghini, E., Cricelli, L. ve Grimaldi, M. (2014). A methodology to manage and monitor social media inside a company: a case study, *Journal of Knowledge Management, 18*(2), 55- 277. https://doi.org/10.1108/JKM-10-2013-03922

Anayasa Mahkemesi (2014). Anayasa Mahkeme Kararı (Karar sayısı: 2014/74). https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf

Aras, B. (2011). Devlet sırrı kavramı ve uygulamada yaşanan sorunlar. https://www.ajindex.com/dosyalar/makale/acarindex-1423934992.pdf adresinden 03 Ekim 2023 tarihinde alınmıştır.

Arıkan, R. (2013). *Araştırma yöntem ve teknikleri* (2. Baskı). Nobel Yayıncılık.

Arslantekin, S. (2003). Veri madenciliği ve bilgi merkezleri. *Türk Kütüphaneciliği*, *17*(4), 369-380.

Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik (2021). T.C. Resmi Gazete, Tarih: 02 Ekim 2021, Sayı:31616. https://www.devletarsivleri.gov.tr/varliklar/dosyalar/mevzuat/arastirmaesaslari2021.pdf

Aslan, B. (2010). Bir yönetim fonksiyonu olarak iç denetim. *Sayıştay Dergisi*, (77), 63-86.

Avrupa Konseyi (1981). Avrupa Konseyi kişisel verilerin otomatik işlenmesine ilişkin olarak bireylerin korunması hakkındaki Avrupa Sözleşmesi (Sayı:108). https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/ak/turkce/108_tur.pdf

Aydın, C. ve Özdemirci, F. (2011). Elektronik belgelerin arşivlenmesinde gerçekliğin ve bütünlüğün korunması. *Bilgi Dünyası, 12*(1), 105-127. https://doi.org/10.15612/BD.2011.224

Bhatt, G. D. (2001). Knowledge management in organizations: Examining the interaction between technologies, techniques, and people, *Journal of Knowledge Management*, *5*(1), 68-75. https://doi.org/10.1108/13673270110384419

Bakanlar Kurulu Kararı (2012). Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar (Karar no. 2012/3842). https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm

Barutçugil, İ. (2002). *Bilgi Yönetimi* (2. Baskı). Kariyer Yayıncılık.

Başbakanlık Genelgesi (2005). Standart dosya planı (Genelge no. 2005/7). https://resmigazete.gov.tr/eskiler/2005/03/20050325-10.htm

Başbakanlık Genelgesi (2016). Kamu kurum ve kuruluşların KamuNet'e dahil edilmesi (Genelge no. 2016/28). https://resmigazete.gov.tr/eskiler/2016/12/20161203.htm

Başbakanlık Genelgesi (2017). e-Yazışma projesi (Genelge no. 2017/21). https://www.resmigazete.gov.tr/eskiler/2017/10/20171014-11.pdf

Bayter, M. (2022). Dünyada ve ülkemizde RDA'ya geçiş. *Türk Kütüphaneciliği, 36*(1), 54-73. https://doi.org/10.24146/tk.991593

Bayter, M. (2023). Türkiye'de kataloglama eğitimi. *Külliye, 4*(2), 59-80. https://doi.org/10.48139/aybukulliye.1267015

Belghith, O., Skhiri, S., Zitoun, S. ve Ferjaoui, S. (2021, Mayıs, 298-309). A survey of maturity models in data management. 2021 IEEE 12th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT), Cape Town, South Africa. https://doi.org/10.1109/ICMIMT52186.2021.9476197

Bilgi Edinme Değerlendirme Kurulu (2023a). Bilgi Edinme Değerlendirme Kurulu Hakkında. https://bedk.adalet.gov.tr/SayfaDetay/Hakkimizda adresinden 26 Ekim 2023 tarihinde alınmıştır.

Bilgi Edinme Değerlendirme Kurulu (2023b). Bilgi edinme değerlendirme kurulu kararları. https://bedk.adalet.gov.tr/SayfaDetay/kararlar13072021121109 adresinden 26 Ekim 2023 tarihinde alınmıştır.

Bilgi Edinme Hakkı Kanunu (2003). T.C. Resmi Gazete, Tarih: 24 Ekim 2003, Sayı: 25269. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4982&MevzuatTur=1&MevzuatTertip=5

Bilgi ve İletişim Kurumu (2023). https://www.btk.gov.tr/kayitli-elektronik-posta-mevzuat adresinden 24 Nisan 2023 tarihinde alınmıştır.

Bilim ve Teknoloji Yüksek Kurulu (2013). Ulusal veri merkezi çalışmalarının yapılması. https://www.tubitak.gov.tr/sites/default/files/62_2013_104.pdf adresinden 24 Eylül 2023 tarihinde alınmıştır.

Bozkurt, P. (2016). Denetim Kavramı ve Denetim Anlayışındaki Gelişmeler. *Denetişim*, (12), 56-62.

Brookes, N. ve Clark, R. (2009, Mayıs, 285-296). Using maturity models to improve project management practice. POMS 20th Annual Conference, Florida, U.S.A.

Cırıkoğlu, R. (2023). *Bilgi ve belge yönetimi ile istihbarat arasındaki ilişki* [Yüksek Tezi]. Ankara Üniversitesi.

Civelek, D. Y. ve Turan, H. K. (2010). Kurumlar arası e-yazışma çalışma raporu: 1. Ankara: Devlet Planlama Teşkilatı. http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2014/04/DPT_eYazisma_Calisma_ Raporu_Eylul2010.pdf adresinden 07 Nisan 2023 tarihinde alınmıştır.

Carey, E. (2017). Information management standard - Australian government. *IQ: The RIMPA Quarterly Magazine, 33*(4), 16–19. https://search.informit.org/doi/10.3316/informit.216955075365943

Ceza Muhakemesi Kanunu (2004). T.C. Resmi Gazete, Tarih: 17 Aralık 2004, Sayı: 25673. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf

Cleven, A. ve Wortmann, F. (2010, Ocak, 1-10). Uncovering four strategies to approach master data management. Proceedings of the 43rd Hawaii International Conference on System Sciences, Hawai, U.S.A. https://doi.org/10.1109/HICSS.2010.488

CMMI (2019). Data Management Maturity (DMM). https://stage.cmmiinstitute.com/dmm adresinden 02 Kasım 2022 tarihinde alınmıştır.

CMMI (2023a). Data Management Maturity (DMM). https://www.cmmiinstitute.com/data-management-maturity adresinden 10 Ocak 2023 tarihinde alınmıştır.

CMMI (2023b). CMMI Levels of Capability and Performance. https://cmmiinstitute.com/learning/appraisals/levels adresinden 07 Nisan 2023 tarihinde alınmıştır.

Cooke, D. (2002). Project management maturity models: Does it make sense to adopt one? *Project Management, 1*(4).

Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (2019). T.C. Resmi Gazete, Tarih: 06 Temmuz 2009, Sayı: 30823. https://cbddo.gov.tr/mevzuat/2019-12- sayili-bilgi- guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020a). Bilgi ve iletişim güvenliği rehberi. https://cbddo.gov.tr/bgrehber adresinden 06 Kasım 2022 tarihinde alınmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020b). Veri sözlüğü yazılımı kullanım kılavuzu. https://cbddo.gov.tr/projeler/ulusalverisozlugu/dokumanlar/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı (2019). On birinci kalkınma planı (2019-2023). https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023a). KamuNet projesi. https://cbddo.gov.tr/projeler/kamu-net/ adresinden 06 Kasım 2022 tarihinde alınmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023b). Açık veri projesi. https://cbddo.gov.tr/projeler/acik-veri/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023c). Ulusal veri sözlüğü projesi. https://cbddo.gov.tr/projeler/ulusalverisozlugu/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023d). KAYSİS projesi. https://cbddo.gov.tr/projeler/kaysis/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023e). e-Yazışma projesi. https://cbddo.gov.tr/projeler/e-yazisma/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2023f). e-Yazışma teknik rehberi v2.0. https://cbddo.gov.tr/SharedFolderServer/CMSFiles/EYP.pdf adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Çakmak, T.; Özel, N. (2013). Dijital varlık yönetimi ve bilgi hizmetleri. http://www.openaccess.hacettepe.edu.tr:8080/xmlui/bitstream/handle/11655/11752/Dijital_Varl%C4%B1k_Y%C3%B6netimi_ve_Bilgi_Hizmetleri_Tolga_Nevzat.pdf?sequence=1 adresinden 01 Mayıs 2023 tarihinde alınmıştır.

Çelik, V.; Ergun, T.; Turan, E.; Saldık, S.; Balkaya, M.M.; Seyirt, M. (2017). Elektronik Yazışma Projesi Güvenlik Katmanları ve Uygulama Geliştirme Esnasında Dikkat

Edilmesi Gereken Hususlar. Özdemirci, F.; Akdoğan, Z. (Ed.) *Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar* içinde (ss. 103-120). BİL-MEM.

Çevre ve Orman Bakanlığı (2009). *Yönetim Bilgi Sistemi ve Bakanlığımızda Uygulamaları.* Çevre ve Orman Bakanlığı.

Çiçek, N. (2015). *Kurumsal bilgi ve belge yönetimi: Kurumsal İletişim, Belge Türleri, e-Yazışma, Elektronik Belge Yönetimi, Dosyalama İşlemleri*. Marmara Belediyeler Birliği.

Data Governance Institute (2023). Definitions of data governance. https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/ adresinden 02 Mart 2023 tarihinde alınmıştır.

DAMA International (2017). *DAMA-DMBOK Data Management Body of Knowledge. Technics Publications* (2nd ed.). Technics Publications.

DAMA International (2023). Data management framework or dama wheel. https://www.dama.org/cpages/dmbok-2-wheel-images adresinden 10 Ocak 2023 tarihinde alınmıştır.

Darbishire, H. (2010) Proactive transparency : The future of the right to information? https://openknowledge.worldbank.org/handle/10986/25031 adresinden 24 Kasım 2022 tarihinde alınmıştır.

Dataversity (2023). What is the data management body of knowledge (DMBoK)? https://www.dataversity.net/what-is-the-data-management-body-of-knowledge-dmbok/adresinden 10 Ocak 2023 tarihinde alınmıştır.

Davenport, T. H., ve Prusak, L. (1998). *Working Knowledge : How Organizations Manage What They Know*. Harvard Business School Press.

Değer, M.K. (2021). Kartografik ve Fotografik Materyallerin Arşivsel Değeri. *Hazine-i Evrak Arşiv ve Tarih Araştırmaları Dergisi*, *3*(3), 27-42.

Demir, E. (2021). Veri Yönetimi. *Dijital Dönüşüm ve Bilişim Sistemleri (*s.87-98) içinde. Efe Akademi.

Defize, D.R. (2020). *Developing a maturity model for AI-augmented data management* [Yüksek Lisans Tezi]. Twente Üniversitesi.

Devlet Teşkilatı Merkezi Kayıt Sistemi (2023). https://detsis.gov.tr/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Devlet Arşivleri Başkanlığı (2019). Devlet Arşivleri Başkanlığının 2020-2024 dönemi stratejik planı. https://www.devletarsivleri.gov.tr/Sayfalar/Haberler/Duyuru.aspx?ID=4166

Devlet Arşivleri Başkanlığı (2023a). Devlet Arşivleri Başkanlığı 2022 yılı faaliyet raporu. https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=1030&h=92BE7C48C7C181481EF5CBDAC2DE662069CD6CC7C5F209D9811C5B34F36A3E72

Devlet Arşivleri Başkanlığı (2023b). Standart dosya planı. https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=4&h=4ED7C6FC0901076942FD7973AF6CD3F7BC5DC84B001433968BE9919D6C54E66B adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi (2018). T.C. Resmi Gazete, Tarih: 16 Temmuz 2018, Sayı: 30480. https://mevzuat.gov.tr/MevzuatMetin/19.5.11.pdf

Devlet Arşiv Hizmetleri Hakkında Yönetmelik (2019). T.C. Resmi Gazete, Tarih: 18 Ekim 2019, Sayı: 30922. https://www.mevzuat.gov.tr/mevzuat? MevzuatNo= 33899&MevzuatTur=7& MevzuatTertip=5

Devlet Sırrı Kanun Tasarısı (2008). https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss287 adresinden 03 Ekim 2023 tarihinde alınmıştır.

Diamond, S. (1995). *Records management; polieies, practiees, techniques*. *Amacom*.

Diri, M. ve Gülçiçek, M. (2012). Türkiye'de kamu hizmetinin görülmesinde kullanılmakta olan gizlilik derecesi tanımları: uygulamadaki sorunlar ve çözüm önerileri. *Maliye Dergisi*, *162*(2), 26-56.

DOD 5015.2-STD (2007) Electronic records management software applications design criteria standard. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/501502std.pdf adresinden 10 Ocak 2023 tarihinde alınmıştır.

Doğan, K. ve Arslantekin, S. (2016). Büyük veri: Önemi, yapısı ve günümüzdeki durum. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 56*(1), 15-36. https://doi.org/10.1501/Dtcfder_0000001461

Dublin Core (2023a). Dublin core metadata element set. https://www.dublincore.org/specifications/dublin-core/dces/ adresinden 10 Ocak 2023 tarihinde alınmıştır.

Dublin Core (2023b). About DCMI. https://www.dublincore.org/about/ adresinden 10 Ocak 2023 tarihinde alınmıştır.

Duranti, L. (2001). The impact of digital technology on archival science. *Archival science*, *1*, 39-55.

Düzce Üniversitesi (2022). Big data nedir. https://duzce.edu.tr/akademik/fakulte/if/yonetim-bilisim-sistemleri/f8d9/buyuk-veri-big-data-nedir adresinden 04 Aralık 2022 tarihinde alınmıştır.

Ehie, I. ve Madsen, M. (2005). Identifying critical issues in enterprise resource planning (ERP) implementation. *Computers in Industry, 56,* 545-557. https://doi.org/10.1016/j.compind.2005.02.006

EDM Council (2023). The data management capability assessment model (DCAM). https://www.edmcouncil.org adresinden 15 Ocak 2023 tarihinde alınmıştır.

Eken, M. (1994). Kamu yönetiminde gizlilik geleneği ve açıklık ihtiyacı. *Amme İdaresi Dergisi*, *27*(2), 25-54.

Ekici, S. (2021). *Ulusal bilim ve teknoloji politikalarında bilgi yönetimine yaklaşım: Türkiye için bir strateji ve eylem planı model önerisi* [Doktora Tezi]. Hacettepe Üniversitesi.

Ekiz, D. (2020). *Bilimsel araştırma yöntemleri (6. bs)*. Ankara: Anı Yayıncılık.

Elektronik İmza Kanunu (2004). T.C. Resmi Gazete, Tarih: 23 Ocak 2004, Sayı: 25355. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5

Elektronik Haberleşme Kanunu (2008). T.C. Resmi Gazete, Tarih: 10 Kasım 2008, Sayı: 27050. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf

Eroğlu, Ş. (2017). *Türkiye'de kamu verilerinin açık devlet uygulamaları ve belge yönetimi çerçevesinde değerlendirilmesi: Bir model önerisi* [Doktora Tezi]. Hacettepe Üniversitesi.

Eroğlu, Ş. (2018a). Dijital yaşamda mahremiyet (gizlilik) kavramı ve kişisel veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 35*(2), 130-153. https://doi.org/10.32600/huefd.439007

Eroğlu, Ş. (2018b). *Açık Devlet ve Açık Devlet Verisi*. Hiperlink.

Eroğlu, Ş. ve Çakmak, T. (2020a). Personal data perceptions and privacy in Turkish academic libraries: An evaluation for administrations. *The Journal of Academic Librarianship, 46*(6), 102251. https://doi.org/10.1016/j.acalib.2020.102251

Eroğlu, Ş. ve Çakmak, T. (2020b). Information as an organizational asset: assessment of a public organization's capabilities in Turkey. *Information Development, 36*(1), 58-77. https://doi.org/10.1177/0266666918811004.

Fox, J. (2007). The uncertain relationship between transparency and accountability.*Development in practice, 17*(4-5), 663-671. https://doi.org/10.1080/09614520701469955

Franks, P. C. (2013). *Records and information management*. American Library Association.

Frické, M. H. (2018). Data-information-knowledge-wisdom (DIKW) pyramid, framework, continuum. *Encyclopedia of Big Data,* 1–4. https://doi.org/10.1007/978-3-319-32001-4_331-1

de Figueiredo, G. B., Moreira, J. L. R., de Faria Cordeiro, K., ve Campos, M. L. M. (2019). Aligning DMBOK and open government with the FAIR data principles. *Advances in conceptual modeling: ER 2019 workshops FAIR, MREBA, EmpER, MoBiD, OntoCom, and ER doctoral symposium papers* içinde (s. 13-22). Springer International Publishing. https://doi.org/10.1007/978-3-030-34146-6_2

Gartner (2023). Master data management (MDM). https://www.gartner.com/en/information-technology/glossary/master-data-management-mdm adresinden 24 Ocak 2023 tarihinde alınmıştır.

Geiger, C. P. Ve Von Lucke, J. (2012). Open government and (linked)(open)(government)(data).*JeDEM-eJournal of eDemocracy and open Government*, *4*(2), 265-278. https://doi.org/10.29379/jedem.v4i2.143

Gemalmaz, M. S. ve Gemalmaz, H. B. (2004). *Ulusalüstü insan hakları standartları ışığında Türkiye'de bilgi edinme düşünce-ifade ve iletişim mevzuatı*: *Düşünce suçuna karşı girişim*. Yazıhane Yayınları.

Genç, Ş. (2019). *Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-Devlet yapısının incelenesi* [Yüksek Lisans Tezi]. İstanbul Okan Üniversitesi.

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022). T.C. Resmi Gazete, Tarih: 26 Nisan 2022, Sayı: 31821 https://www.tccb.gov.tr/resmiyazisma/gizlilik-yonetmeligi/

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu (2023). https://www.tccb.gov.tr/resmiyazisma/gizlilik-kilavuzu/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Gordon, K. (2022). *Principles of data management: Facilitating information sharing* (3. Baskı). BCS, The Chartered Institute for IT.

Gray, J. (1996). Data management: Past, present, and future. *IEEE Computer, 29*(10), 38-46. https://doi.org/10.48550/arXiv.cs/0701156

Gökalp, E. ve Demirörs, O. (2016, Mayıs, 210-224). Towards a process capability assessment model for government domain. *Communications in Computer and Information Scienc*e içinde. 16th International Conference, Dublin, Ireland. https://doi.org/10.1007/978-3-319-38980-6_16

Guha, T. K. (2008). Dublin Core: The standard for networking libraries. http://eprints.rclis.org/12164/1/dcweb.pdf adresinden 24 Ocak 2023 tarihinde alınmıştır.

Güvenlik Soruşturması ve Arşiv Araştırması Kanunu (2021). T.C. Resmi Gazete, Tarih: 17 Nisan 2021, Sayı: 31457. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7315&MevzuatTur=1&MevzuatTertip=5

Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik (2022). T.C. Resmi Gazete, Tarih: 03 Haziran 2022, Sayı: 3185. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5649&MevzuatTur=21&MevzuatTertip=5

Hare, K.; McLeod, J. (1997). *Developing a records management programme*. Aslib.

Haselden, K. Ve Wolter, R. (2021). Profisee trust your data. https://profisee.com/masterdata- management-what-why-how-who adresinden 04 Aralık 2022 tarihinde alınmıştır.

HEYS (2023). Hizmet envanteri yönetim sistemi. https://envanter.kaysis.gov.tr/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Inmon, W. H., Strauss, D. ve Neushloss, G. (2008). *DW 2.0: The architecture for the next generation of data warehousing*. Elsevier. https://doi.org/10.1016/B978-0-12-374319-0.X0001-2

Inmon, W. ve Linstedh, D. (2015). Data architecture: A primer for the data scientist: Big data, data warehouse and data vault. Morgan Kaufmann.

ISCAP (2023). Interagency security classification appeals panel. https://www.archives.gov/declassification/iscap adresinden 10 Eylül 2023 tarihinde alınmıştır.

ISCAP Tüzüğü, Kuralları ve Temyiz Prosedürleri (2012). https://www.federalregister.gov/documents/2012/07/09/2012-16655/the-interagency-security-classification-appeals-panel-iscap-bylaws-rules-and-appeal-procedures#sectno-reference-2003.11

ISO 8000 (2022). Data quality. https://www.iso.org/obp/ui/#iso:std:iso:8000:-1:ed-1:v1:en

ISO 8000-6. (2016). Data quality management: Process reference model. https://www.iso.org/obp/ui/#iso:std:iso:8000:-61:ed-1:v1:en

ISO/IEC TR 10032 (2003). Information technology - Reference model of data management. https://www.iso.org/standard/38607.html

ISO/IEC 19583-1 (2019). Information technology-Concepts and usage of metadata-Part 1: Metadata concepts. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:19583:-1:ed-1:v1:en

ISO/IEC 19583-21 (2022). Information technology - Concepts and usage of metadata Part 21: 11179-3 Data model in SQL. https://www.iso.org/obp/ui/#iso:std:iso- iec:tr:19583:-21:ed-1:v1:en

ISO/IEC 19583-22 (2018). Information technology - Concepts and usage of metadata Part 22: Registering and mapping development processes using ISO/IEC 19763. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:19583:-22:ed-1:v1:en

ISO/IEC 19583-23 (2020). Information technology - Concepts and usage of metadata Part 23: Data element exchange (DEX) for a subset of ISO/IEC 11179-3. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:19583:-23:ed-1:v1:en

ISO/IEC 19763-1 (2015). Information technology - Metamodel framework for interoperability (MFI) - Part 1: Framework. https://www.iso.org/obp/ui/#iso:std:iso- iec:19763:-1:ed-2:v1:en

ISO/IEC 27001 (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

ISO/IEC 27002 (2022). Information security, cybersecurity and privacy protection - Information security controls. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

ISO/IEC 27014 (2020). Information security, cybersecurity and privacy protection - Governance of information security https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27014:ed-2:v1:en

ISO 55001 (2014). Asset management - Management systems - Requirements. https://www.iso.org/obp/ui/#iso:std:iso:55001:ed-1:v1:en

ISO 15489-1 (2016). Information and documentation - Records management - Part 1: Concepts and principles. https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en

ISO/IEC 19773 (2011). Information technology - Metadata Registries (MDR) modules.
https://www.iso.org/obp/ui/#iso:std:iso-iec:19773:ed-1:v1:en

ISO 16175-1 (2020). Information and documentation - Processes and functional requirements for software for managing records - Part 1: Functional r equirements and associated guidance for any applications that manage digital records.
https://www.iso.org/obp/ui/#iso:std:74294:en

ISO/TS 16175-2 (2020). Information and documentation - Processes and functional requirements for software for managing records - Part 2: Guidance for selecting, designing, implementing and maintaining software for managing records. https://www.iso.org/obp/ui/#iso:std:74293:en

ISO 23081-1 (2017). Information and documentation - Records management processes - Metadata for records - Part 1: Principles.
https://www.iso.org/obp/ui/#iso:std:iso:23081:-1:ed-2:v1:en

ISO 23081-2 (2021). Information and documentation - Metadata for managing records - Part 2: Conceptual and implementation issues.
https://www.iso.org/obp/ui/#iso:std:iso:23081:-2:ed-2:v1:en

ISO/TR 23081-3 (2011). Information and documentation - Managing metadata for records -Part 3: Self-assessment method.
https://www.iso.org/obp/ui/#iso:std:57121 :en

ISO/IEC 29100 (2011). Information technology - Security techniques - Privacy framework.
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:29100:ed-1:v1:en

ISO/IEC 29101 (2018). Information technology - Security techniques - Privacy architecture framework.
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:29101:ed-2:v1:en

ISO 30300 (2020). Information and documentation - Records management - Core concepts and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso:30300:ed-2:v1:en

ISO 30301 (2019). Information and documentation - Management systems for records - Requirements. https://www.iso.org/obp/ui/#iso:std:iso:30301:ed-2:v1:en

ISO 30302 (2022). Information and documentation - Management systems for records - Guidelines for implementation. https://www.iso.org/obp/ui/#iso:std:iso:30302:ed-2:v1:en

ISOO (2022). Information security oversight office annual report to the president. https://www.archives.gov/files/isoo/reports/isoo-2022-annual-report-to-the-president.pdf

ISOO (2023a). History of the Information Security Oversight Office (ISOO). https://www.archives.gov/isoo/about/history.html adresinden 24 Eylül 2023 tarihinde alınmıştır.

ISOO (2023b). Information Security Oversight Office. https://www.archives.gov/isoo adresinden 24 Eylül 2023 tarihinde alınmıştır.

ISOO (2023c). Mandatory declassification review (MDR). https://www.archives.gov/isoo/training/mdr adresinden 24 Eylül 2023 tarihinde alınmıştır.

İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik (2006). T.C. Resmi Gazete, Tarih: 12 Temmuz 2006, Sayı: 26226. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=200610654&MevzuatTur=21&MevzuatTertip=5

İnceoğlu, S. ve Şentürk, B. (2014). Dijital çağda arşivci: Sahip olması gereken temel yetkinlikler ve roller. *Bilgi Dünyası*, *15*(2), 353-374. https://doi.org/10.15612/BD.2014.437

Jaseena, K. U. Ve David, J. M. (2014). Issues, challenges, and solutions: Big data mining. *CS & IT-CSCP*, *4*(13), 131-140. https://doi.org/10.5121/csit.2014.41311

Jeffery, K. (2014). Data is the New Oil. https://indico.cern.ch/event/313634/attachments/600436/826361/Jeffery_Data_is_the_new_Oil.pdf adresinden 29 Kasım 2022 tarihinde alınmıştır.

Jenkins, T.; Köhler, W.; Shackleton, J. (2005). *Enterpise content management methods: What you need to know?* Open Text Coorporation.

Kamu İç Denetim Genel Tebliği (2013). T.C. Resmi Gazete, Tarih: 19 Nisan 2013, Sayı: 28623. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=18302&MevzuatTur=9&MevzuatTertip=5

Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu Veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik (2010). T.C. Resmi Gazete, Tarih: 23.10.2010,Sayı: 27738. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=14387&MevzuatTur=7&MevzuatTertip=5

Kamu Malî Yönetimi ve Kontrol Kanunu (2003). T.C. Resmi Gazete, Tarih: 24 Aralık 2003, Sayı: 25326. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5018&MevzuatTur=1&MevzuatTertip=5

Kandur, H. (2006). *Elektronik belge yönetimi sistem kriterleri referans modeli (v. 2.0)*. Devlet Arşivleri Genel Müdürlüğü.

Kaptan, S. (1995). *Bilimsel araştırma teknikleri ve istatistik yöntemleri*. Bilim Yayıncılık

Karaman, Z. T. ve Atak, Ş. (1996). Kamu yönetiminde gizlilik faktörünün çevre korumacı politikalara etkisi. *Türk İdare Dergisi, Yıl*, *68*, 111-129.

Karasar, N. (2015). *Bilimsel araştırma yöntemi: Kavramlar ilkeler teknikler* (28. bs.). Nobel Yayın.

Kaya, C. (2011). Avrupa Birliği veri koruma direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *Journal of Istanbul University Law Faculty, 69*(1-2), 317-334.

Kaya Bensghir, T.; Topcan, F. (2010). *e-İmza: Türkiye'de kamu kurumlarında uygulanması*. Türkiye ve Orta Doğu Amme İdaresi Enstitüsü (TODAİE).

Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2011). T.C. Resmi Gazete, Tarih: 25.08.2011, Sayı: 28036. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=15224&MevzuatTur=7&MevzuatTertip=5

Kim, D. ve Solomon, M.G. (2019). *Bilgi sistemleri güvenliğinin temelleri* (3. Baskı). (Ö. Can, Çev. Ed.). Nobel (Orijinal Eserin Basım Tarihi, 2019, 3. Baskı).

Kim, G. T. (2019). A Study on the system of confidential record management of the USA. *The Korean Journal of Archival Studies,* (59), 159–206. https://doi.org/10.20923/KJAS.2019.59.159

King, T. ve Schwarzenbach, J. (2020). *Managing data quality: A practical guide*. BCS Publishing.

Kişisel Verilerin Korunması Kanunu (2016). T.C. Resmi Gazete, Tarih: 07 Nisan 2016, Sayı: 29677. https://mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Kitchin, R. (2014). *The data revolution: Big data, open data, data ınfrastructures and their consequences*. Sage.

KMS (2023). Kamu Mevzuat Sistemi. https://kms.kaysis.gov.tr/ adresinden 04 Mayıs 2023 tarihinde alınmıştır.

Krishnan, K. (2013). *Data warehousing ın the age of big data*. Morgan Kaufmann.

Koç Üniversitesi (2022). Veri Sınıflandırma Prosedürü. https://my.ku.edu.tr/wp-content/uploads/2022/03/Veri-Siniflandirma-Proseduru-1.pdf adresinden 29 Kasım 2022 tarihinde alınmıştır.

Kosar, K. R. (2011). *Classified information policy and executive order 13526*. DIANE Publishing.

Köroğlu, S.A. (2015). *Literatür taraması üzerine notlar ve bir tarama tekniği. GİDB Dergi*, (01) 61-69.

Külcü, Ö. (2007). Belge yönetiminin değişen yüzü: standartlaşma çalışmaları ve uluslararası uygulamalar. *Bilgi Dünyası, 8*(2), 230-279. https://doi.org/10.15612/BD.2007.341

Külcü, Ö. (2010). Belge yönetiminde yeni fırsatlar: Dijitalleştirme ve içerik yönetimi uygulamaları*. Bilgi Dünyası, 11*(2), 290-331. https://doi.org/10.15612/BD.2010.239

Külcü, Ö., Çakmak, T. ve Özel, N. (2015). *Kamusal bilgi ve elektronik belge yönetimi: organizasyonlar ve üniversitelere yönelik koşulların analizi*. Türk Kütüphaneciler Derneği.

Külcü, Ö. (2018). *Kurumsal bilgi sistemleri ve belge yönetimi: Organizasyonlarda bilgi ve belge yönetiminin temel ilkeleri*. Hiperlink.

Lee, K. R. (2010). The Historical understanding of the US secret records management. *The Korean Journal of Archival Studies*, (23), 257-297. https://doi.org/10.20923/KJAS.2010.23.257

Luftman, J., Derksen, B., Dwivedi, R., Santana, M., Zadeh, H. S. ve Rigoni, E. (2015). Influential IT management trends: an international study. *Journal of Information Technology*, *30*(3), 293-305. https://doi.org/10.1057/jit.2015.1

MacKenzie, G. (1999). A new world ahead: international challenges for information management. *Information Management*, *33*(2), 24.

McGilvray, D. (2021). *Executing data quality projects: Ten steps to quality data and trusted information (TM)*. Academic Press.

Mesquita, V., Faria, J., Gonçalves, D. ve Varajão, J. (2013, Haziran, 1291-1301). Motivations for the adption of ERP and CRM systems: a comparative analysis. 10th International Conference on Information Systems and Technology Management, São Paulo, Brezilya.

Milli Savunma Bakanlığı (2023). Savunma sanayii güvenliği yönergesi. https://www.msb.gov.tr/TeknikHizmetler/icerik/savunma-sanayii-guvenligi-mevzuati-yonergeler adresinden 01 Mayıs 2023 tarihinde alınmıştır.

NAA (2023). Information management standard for Australian Government. https://www.naa.gov.au/information-management/standards/information-management- standard-australian-government adresinden 24 Nisan 2023 tarihinde alınmıştır.

NDC (2023). the National Declassification Center. https://www.archives.gov/declassification/ndc/about-ndc adresinden 24 Eylül 2023 tarihinde alınmıştır.

NFPA 75 (2020). Standard for the fire protection of information technology equipment. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=75 adresinden 24 Nisan 2023 tarihinde alınmıştır.

NFPA 232 (2022). Standard for the protection of records. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and standards/detail?code= 232 adresinden 24 Nisan 2023 tarihinde alınmıştır.

NFPA 909 (2021). Code for the protection of cultural resource properties - Museums, libraries, and places of worship. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=909 adresinden 24 Nisan 2023 tarihinde alınmıştır.

O'Callaghan, R. Ve Smits, M. (2005). A strategy development proscess for enterprise content management. https://aisel.aisnet.org/ecis2005/148/ adresinden 24 Nisan 2023 tarihinde alınmıştır.

Odabaş, H. (2008). Elektronik belge düzenleme yaklaşımları ve Türkiye'de e-devlet uygulamalarında elektronik belge yönetimi. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 12*(2), 121-142.

Odabaş, H. (2009). *E-Devlet sürecinde elektronik belge yönetimi*. Hiperlink Yayınları.

OECD (2021). Guidelines governing the protection of privacy and transborder flows of personal data. https://legalinstruments.ecd.org/en/instruments/OECD-LEGAL-0188

OECD (2022). OECD work on privacy. https://www.oecd.org/sti/ieconomy/privacy.htm adresinden 12 Aralık 2022 tarihinde alınmıştır.

Oracle (2023). Veri yönetimi nedir? https://www.oracle.com/tr/database/what-is-data-management/ adresinden 15 Ocak 2023 tarihinde alınmıştır.

Özdemirci, F. (1999). Organizasyonlarda belge yönetimi ve toplam kalite. *Türk Kütüphaneciliği, 13*(2), 101-111.

Özdemirci, F. (2003). İlk uluslararası belge yönetim standardı: ülkemiz açısından bir değerlendirme. *Türk Kütüphaneciliği*, *17*(3), 225-246.

Özdemirci, F. ve Torunlar, M. (2015). *Bilgi Çağında Arşivsel Bilgi Analizi: Bilgi-İktidar-İdeoloji-Devlet*. Ankara Üniversitesi Basımevi.

Özdemirci, F. (2019). Kurumlar için EBYS ve e-arşiv sistemi idari yapılanma ve yönetim süreci: Bileşenler ve entegrasyonlar. B. Yalçınkaya, M.A. Ünal, B. Yılmaz, F. Özdemirci (Ed.), *Bilgi yönetimi ve bilgi güvenliği: ebelge-earşiv-edevlet-bulut bilişim-büyük veri-yapay zeka* (s. 3-9) içinde. Ankara Üniversitesi BİL-BEM.

Öztürk, H. (2021). Arşivler ve Yapay Zekâ. *Bilgi Yönetimi, 4*(2), 283-300. https://doi.org/10.33721/by.987197

Pala, İ.B. (2021). *Kurumsal büyük veri analitiği yetenekleri ve performans ilişkisi: Türkiye için bir araştırma* [Yüksek Lisans Tezi]. İstanbul Teknik Üniversitesi.

Pande, M. (2020). Difference between ISO 8000 & 9001. https://certificateplace.com/difference-between-iso-8000-9001/ adresinden 01 Mayıs 2023 tarihinde alınmıştır.

Penn, I. A., Mordel, A. ve Pennix, G. (1994). *Record management hand-book*. Kelvin Smith: Gower.

PIDB (2023). The Public Interest Declassification Board. https://www.archives.gov/declassification/pidb adresinden 10 Ekim 2023 tarihinde alınmıştır.

PIDB Yönetmeliği (2020). https://www.archives.gov/declassification/pidb/by-laws.html

Proença, D., ve Borbinha, J. (2018, Ekim, 81-93). Maturity models for data and information management: A state of the art. *Digital Libraries for Open Knowledge* içinde*. 22nd International Conference on Theory and Practice of Digital Libraries, Porto, Portugal.*

Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2006). T.C. Resmi Gazete, Tarih: 20 Haziran 2006, Sayı: 26204. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=10429&MevzuatTur=7&MevzuatTertip=5

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2020). T.C. Resmi Gazete, Tarih: 10 Haziran 2020, Sayı: 31151. https://www.mevzuat.gov.tr/ mevzuatmetin/21.5.2646.pdf

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu (2020). https://www.tccb.gov.tr/resmiyazisma/kilavuz/ adresinden 25 Kasım 2022 tarihinde alınmıştır.

Röglinger, M., Pöppelbuß, J. ve Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal, 18*(2), 328–346. https://doi.org/10.1108/14637151211225225

Rukancı, F., Anameriç, H., & Başar, A. (2021). *Arşiv ve arşivcilik: Kuram, strateji ve uygulamalar*. Türkiye Cumhuriyeti Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Yayınları (12).

Sak, R., Sak, İ. T. Ş., Şendil, Ç. Ö. ve Nas, E. (2021). Bir araştırma yöntemi olarak doküman analizi. *Kocaeli Üniversitesi Eğitim Dergisi, 4*(1), 227-256. https://doi.org/10.33400/kuje.843306

Savunma Sanayii Güvenliği Kanunu (2004). T.C. Resmi Gazete, Tarih: 03 Temmuz 2004, Sayı: 25511. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5202&MevzuatTur=1&MevzuatTertip=5

Sebetci, Ö., Günay, M. B. ve Sebetci, E. (2018). İş süreç yönetimi (BPM) ve iş akış yönetimi (WFM) kavramlarına yaklaşım. *AJIT-e: Academic Journal of Information Technology*, *9*(33), 115-126. https://doi.org/10.5824/1309-1581.2018.3.007.x

Şenay, B. A. ve Güneş, A. (2021) Antik Çağ'da Kütüphane Mimarileri: Efes Celcus, Pergamon (Bergama), İskenderiye ve Ninova Örnekleri. *Bilgi ve Belge Araştırmaları,* (15), 95-107. https://doi.org/10.26650/bba.2021.15.05

Sevinç, İ. ve Özata, M. (2011). *Türk kamu yönetiminde bilgi sistemleri ve e-dönüşüm*. Eğitim Yayınevi.

Sinanç, D. (2014). *Cep telefonu kullanıcı davranışlarını modelleme* [Yüksek Lisans Tezi]. Gazi Üniversitesi.

Shen, S. (2019). Master data management: An essential part of data strategy. https://towardsdatascience.com/master-data-management-an-essential-part-of-data- strategy-db12411a05b2 adresinden 15 Ocak 2023 tarihinde alınmıştır.

Sreemathy, J., Nisha, S.; RM, G. P. (2020, Mart, 1444-1448). Data integration in ETL using TALEND. *2020 6th international conference on advanced computing and communication systems (ICACCS)* , Coimbatore, India.

Stephens, D.O. ve Wallace, R.C. (2003). *Electronic records retention: New strategies for data life cycle management.* ARMA International.

Strengholt, P. (2020). *Data Management at Scale*. O'Reilly Media, Inc.

Talend (2023). What is data governance and why do you need it? https://www.talend.com/resources/what-is-data-governance/ adresinden 15 Ocak 2023 tarihinde alınmıştır.

TechTarget (2023). Data quality.https://www.techtarget.com/searchdatamanagement/definition/data-quality 24 Ocak 2023 tarihinde adresinden alınmıştır.

Torunlar, M. ve Özdemirci, F. (2019). *Bilginin bilgiyle savaşı: Belge ve bilgi yönetimi vizyonuyla*. Ankara Üniversitesi.

TSE K 523 (2016). *Bilgi varlıklarının gizlilik derecelerine göre sınıflandırılması kriteri*. Ankara: TSE.

TS 13298 (2015). *Elektronik belge ve arşiv yönetim sistemi standardı*. Ankara: TSE.

Turban, E., Leidner, D., McLean, E. ve Wetherbe, J. (2008). *ınformatıon technology for management.* John Wiley & Sons.

Türk Ceza Kanunu (2004). T.C. Resmi Gazete, Tarih: 12 Ekim 2004, Sayı: 25611. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5

Türk Ticaret Kanunu (2011). T.C. Resmi Gazete, Tarih: 14 Şubat 2011, Sayı: 27846. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6102&MevzuatTur=1&MevzuatTertip=5

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2017). KamuNet ağına bağlanma ve KamuNet ağının denetimine ilişkin usul ve esaslar hakkında tebliğ. T.C. Resmi Gazete, Tarih: 21 Haziran 2017, Sayı: 30103. https://resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm

Ulaştırma ve Altyapı Bakanlığı (2021). 2021 yılı faaliyet raporu. https://www.uab.gov.tr/duyurular/ulastirma-ve-altyapi-bakanligi-2021-yili-faaliyet-raporu-yayinlanmistir

Ulaştırma ve Altyapı Bakanlığı (2023a). KamuNet. https://hgm.uab.gov.tr/kamu-net adresinden 03 Ocak 2023 tarihinde alınmıştır.

Ulaştırma ve Altyapı Bakanlığı (2023b). Kamu entegre veri merkezi projesi. https://hgm.uab.gov.tr/kamu-entegre-veri-merkezi-projesi?PageSpeed=noscript adresinden 03 Eylül 2023 tarihinde alınmıştır.

Ulaştırma ve Altyapı Bakanlığı (2023c). 2022 yılı faaliyet raporu. https://www.uab.gov.tr/duyurular/2022-yili-ulastirma-ve-altyapi-bakanligi-faaliyet-raporu-yayinlanmistir

Ulusal Veri Sözlüğü Projesi (2019). https://cbddo.gov.tr./projeler/ulusalverisozlugu adresinden 29 Kasım 2022 tarihinde alınmıştır.

Ulusal Veri Sözlüğü Yazılımı Kullanım Kılavuzu (2020). https://cbddo.gov.tr./projeler/ulusalverisozlugu/dokumanlar adresinden 29 Kasım 2022 tarihinde alınmıştır.

Ünver, M. (2018). *Elektronik belge yönetim sistemi geliştirilmesi ve küçük boyutlu dosyalardan oluşan büyük verinin depolanması için dağıtık dosya sistemi tasarımı* [Doktora Tezi]. Kırıkkale Üniversitesi.

Yıldız, A. (2022). Büyük veri'nin v'leri ve veri analitiği. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (51), 377-394. https://doi.org/10.30794/pausbed.1117208

Yılmaz, Y. ve Üstündağ, M. T. (2015). Kayıtlı elektronik posta (KEP) hizmetinin kamu kuruluşlarına ait elektronik belge yönetimi sistemlerinde kullanılması. *Bilgi Dünyası*, *16*(2), 204-221. https://doi.org/10.15612/BD.2015.488

Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S. Ve Hsiao, K. F. (2018, Temmuz, 1-5). Ensuring privacy and security in e-health records. *2018 International conference on computer, information and telecommunication systems (CITS),* Alsace, Colmar, France. https://doi.org/10.1109/CITS.2018.8440164

Wallace, D. A. (2001). Electronic records management defined by court case and policy. *Information Management*, *35*(1), 4-14.

Wallis, I. (2021). *Data strategy: From definition to execution*. BCS Publishing.

Wang, Y., Teperek, M., Andrews, H., Lavanchy, P.M., Ilamparuthi, S., Turkyılmaz-van der Velden, Y., Plomp, E. (2020). *Data Management Concept Note For General Public***.** https://doi.org/10.5281/zenodo.3819204

Watson, R. T. (2007). *Information systems*. The Global Text Project.

Weber, K., Otto, B. ve Österle, H. (2009). One size does not fit all-a contingency approach to data governance. *Journal of Data and Information Quality (JDIQ)*, *1*(1), 1-27. https://doi.org/10.1145/1515693.1515696

Wilkoff, N., Walker, J., Root, N. ve Dalton, J. (2001). *What's next for content management?* Cambridge: Forrester Research Inc.

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ ve BELGE YÖNETİMİ ANABİLİM DALI BAŞKANLIĞINA

Tarih:29/04/2024

Tez Başlığı: Elektronik Belge Yönetim Sistemlerinde Bilgi Güvenliği Yönetimi
Tez Başlığı (Almanca/Fransızca)*:…….

Yukarıda başlığı verilen tezimin a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 209 sayfalık kısmına ilişkin, 29/04/2024 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 6'dır.

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 tezimin 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.

Ahmet KAYMAK

Öğrenci Bilgileri		
	Ad-Soyad	Ahmet Kaymak
	Öğrenci No	
	Enstitü Anabilim Dalı	Bilgi ve Belge Yönetimi
	Programı	Bilgi ve Belge Yönetimi

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 Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları İkinci bölüm madde (4)/3'te de belirtildiği üzere: Kaynakça hariç, Alıntılar hariç/dahil, 5 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit match size to 5 words) filtreleme yapılmalıdır.

TO HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INFORMATION MANAGEMENT

Date:04/29/2024

Thesis Title (In English): Information Security Management in Electronic Document

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 04/29/2024 for the total of 209 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 6 %.

Filtering options applied**:

1. ☒ Approval and Decleration 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.

Kindly submitted for the necessary actions.

Ahmet Kaymak

Student Information		
	Name-Surname	Ahmet Kaymak
	Student Number	
	Department	Information Management
	Programme	Information Management

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 refence, quotation excluded/included, Match size up to 5 words excluded.

EK 2. ETİK KOMİSYON İZNİ

T.C.
HACETTEPE ÜNİVERSİTESİ
Rektörlük

Sayı : 35853172/ 433 - 2350

02 Ağustos 2016

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi: 30.06.2016 tarih ve 3408 sayılı yazınız.

Enstitünüz Bilgi ve Belge Yönetimi Anabilim Dalı yüksek lisans programı öğrencilerinden **Ahmet KAYMAK'ın Prof. Dr. Özgür KÜLCÜ** danışmanlığında hazırladığı **"Elektronik Belge Yönetim Sistemlerinde Bilgi Güvenliği Yönetimi"** başlıklı tez çalışması, Üniversitemiz Senatosu Etik Komisyonunun **26 Temmuz 2016** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. Rahime M. NOHUTCU
Rektör a.
Rektör Yardımcısı

Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
Telefon: 0 (312) 305 3001 - 3002 • Faks: 0 (312) 311 9992
E-posta: yazimd@hacettepe.edu.tr • www.hacettepe.edu.tr

Ayrıntılı Bilgi için:
Yazı İşleri Müdürlüğü
0 (312) 305 1008

Hata 16