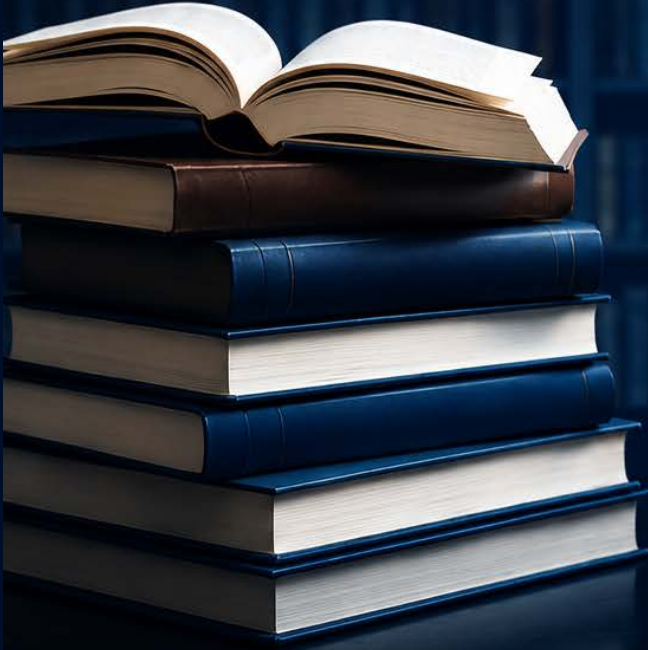


YÖNETİM BİLİŞİM SİSTEMLERİ ALANINDA GÜNCEL KONULAR VE AKADEMİK DEĞERLENDİRMELER

Editör: Doç.Dr. Senem ALTAN



yaz
yayınları

Yönetim Bilişim Sistemleri Alanında Güncel Konular ve Akademik Değerlendirmeler

Editör

Doç.Dr. Senem ALTAN

yaz
yayınları

2026

**Yönetim Bilişim Sistemleri Alanında
Güncel Konular ve Akademik
Değerlendirmeler**

Editör: Doç.Dr. Senem ALTAN

© YAZ Yayınları

Bu kitabın her türlü yayın hakkı Yaz Yayınları'na aittir, tüm hakları saklıdır. Kitabın tamamı ya da bir kısmı 5846 sayılı Kanun'un hükümlerine göre, kitabı yayınlayan firmanın önceden izni alınmaksızın elektronik, mekanik, fotokopi ya da herhangi bir kayıt sistemiyle çoğaltılamaz, yayımlanamaz, depolanamaz.

E_ISBN 978-625-5450-70-8

Ekim 2026 – Afyonkarahisar

Dizgi/Mizanpaj: YAZ Yayınları

Kapak Tasarım: YAZ Yayınları

YAZ Yayınları. Yayıncı Sertifika No: 73086

M.İhtisas OSB Mah. 4A Cad. No:3/3

İscehisar/AFYONKARAHİSAR

www.yazyayinlari.com

yazyayinlari@gmail.com

İÇİNDEKİLER

**Siber Güvenlik ve Yönetim Bilişim Sistemlerinde Veri
Mahremiyeti: KVKK Bağlamında Bir Değerlendirme ..1**
Mansur BEŞTAŞ, Abdurrezzak ÇELİK

**Yönetim Bilişim Sistemlerinde Dijital Sürdürülebilirlik:
Kavramsal Temeller, Akıllı Bilgi Sistemleri ve
Sürdürülebilir Değer Yaratımı.....33**
Furkan ATLAN

**Embodiment as Commons: The Political Economy of
Open-Source AI Bodies.....55**
İsmail Erim GÜLAÇTI

"Bu kitapta yer alan bölümlerde kullanılan kaynakların, görüşlerin, bulguların, sonuçların, tablo, şekil, resim ve her türlü içeriğin sorumluluğu yazar veya yazarlarına ait olup ulusal ve uluslararası telif haklarına konu olabilecek mali ve hukuki sorumluluk da yazarlara aittir."

SİBER GÜVENLİK VE YÖNETİM BİLİŞİM SİSTEMLERİNDE VERİ MAHREMİYETİ: KVKK BAĞLAMINDA BİR DEĞERLENDİRME

Mansur BEŞTAŞ¹

Abdurrezzak ÇELİK²

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin işletme işlevleriyle bütünleşmesi, yönetim bilişim sistemlerini (YBS) çağdaş kuruluşların karar alma ve operasyon süreçlerinde merkezi bir konuma taşımıştır. Yönetim bilişim sistemleri veri toplama, işleme, saklama ve raporlama işlevlerini bir araya getirerek yöneticilere zamanında ve güvenilir bilgi sağlamayı amaçlamaktadır (Laudon ve Laudon, 2011). Sistemlerin kapsamı genişledikçe işlenen verinin hacmi, çeşitliliği ve hassasiyeti de artmaktadır. Böylece siber güvenlik ve veri mahremiyeti, yalnız bilgi işlem birimlerinin değil, üst yönetimin ve bütün kurumsal işlevlerin sorumluluk alanına girmektedir.

Uzaktan ve hibrit çalışma düzenlerinin yaygınlaşması, kurumsal uygulamaların bulut altyapılarına taşınması ve üçüncü taraf hizmetlere bağımlılığın artması, bilgi güvenliği risklerini daha karmaşık hâle getirmiştir. Bulut ortamlarında yetkisiz erişim, veri kaybı, güven eksikliği, farkındalık yetersizliği ve düzenleyici belirsizlikler öne çıkan sorunlar arasındadır (Ukeje vd., 2024). Bu koşullar işletmelerin teknik altyapı yatırımlarıyla

¹ Doç. Dr., Bitlis Eren Üniversitesi, ORCID: 0000-0002-8192-2044.

² Bilim Uzmanı, ORCID: 0000-0003-1128-534X.

birlikte hukuki uyum, tedarikçi denetimi ve kurumsal yönetim kapasitelerini de geliştirmesini gerektirmektedir.

Kişisel verilerin korunması, siber güvenliğin temel hukuki boyutlarından biridir. Türkiye'de 7 Nisan 2016 tarihinde yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin işlenmesine ilişkin ilkeleri, işleme şartlarını ve veri sorumlularının yükümlülüklerini düzenlemektedir. Kanun'un 8, 9, 11, ve 13-18. maddeleri yayımından altı ay sonra, diğer hükümleri ise yayımı tarihinde yürürlüğe girmiştir. Kanun'un özel nitelikli kişisel veriler ile yurt dışına aktarımı düzenleyen 6 ve 9. maddeleri ile kabahatlere ilişkin 18. maddesi 2024 yılında değiştirilmiş, böylece ulusal sistemin Avrupa Birliği düzenlemeleriyle uyumlaştırılması yönünde önemli bir adım atılmıştır (Turan Başara, 2024; Kişisel Verileri Koruma Kurumu [KVKK], 2024a). Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ise belirli koşullarda Birlik dışında yerleşik veri sorumluları ve veri işleyenler üzerinde de etki doğurmaktadır. Her iki düzenleme, veri mahremiyetinin YBS'nin tasarımıyla işletilmesine kadar bütün yaşam döngüsünde gözetilmesini gerektirmektedir.

Çalışmanın amacı, yönetim bilişim sistemlerinde siber güvenlik ve veri mahremiyetini teknik güvenlik, hukuki uyum, insan faktörü ve kurumsal yönetimden oluşan dört bileşenli bir çerçevede incelemektir. Bu doğrultuda KVKK ile GDPR'nin işletme uygulamalarına etkileri karşılaştırılmakta, güncel siber güvenlik yaklaşımları değerlendirilmekte ve Türkiye'deki işletmelere yönelik uygulanabilir öneriler geliştirilmektedir. İnceleme, ampirik bir araştırmadan çok güncel mevzuat ile alan yazını eleştirel biçimde bir araya getiren kavramsal bir sentez niteliğindedir.

Bu kavramsal sentezde, yönetim bilişim sistemleri, siber güvenlik, veri mahremiyeti, bulut bilişim, insan faktörü ve

kurumsal bilgi güvenliği alanındaki güncel akademik çalışmalar ile KVKK, GDPR, Kişisel Verileri Koruma Kurulu kararları, Kurum rehberleri ve ilgili standartlar birlikte incelenmiştir. Kaynaklar, bölümün teknik, hukuki, insan ve yönetim boyutlarını açıklama gücü ile güncellikleri dikkate alınarak seçilmiş, mevzuata ilişkin değerlendirmelerde resmî düzenleme ve Kurum kaynakları esas alınmıştır.

Bu çalışmada veri mahremiyeti ile bilgi güvenliği birbirinin yerine kullanılan kavramlar olarak ele alınmamaktadır. Veri mahremiyeti, kişisel verilerin hangi amaçla, hangi hukuki dayanakla ve hangi sınırlar içinde işlendiğine odaklanırken bilgi güvenliği, verinin gizlilik, bütünlük ve erişilebilirliğini koruyan teknik ve idari tedbirleri kapsar. Şifreleme, kimlik ve erişim yönetimi ile ağ segmentasyonu bu nedenle mahremiyetin kendisi değil, hukuka uygun veri işleme düzenini destekleyen güvenlik araçlarıdır.

Çalışma sekiz ana başlıktan oluşmaktadır. Girişin ardından yönetim bilişim sistemlerinin kavramsal çerçevesi ve temel bileşenleri açıklanmakta, siber güvenlik kavramı ile dijitalleşme sürecinde ortaya çıkan başlıca tehditler ele alınmaktadır. Daha sonra KVKK ve GDPR karşılaştırılmakta, bulut bilişim, ERP entegrasyonu ve çalışan davranışlarından kaynaklanan mahremiyet riskleri tartışılmaktadır. Kurumsal bilgi güvenliği yönetimi standartlarının incelenmesinden sonra Türkiye'deki uygulama sorunları ve öneriler değerlendirilmekte, çalışma genel bir değerlendirmeye tamamlanmaktadır.

2. YÖNETİM BİLİŞİM SİSTEMLERİ: KAVRAMSAL ÇERÇEVE

Yönetim bilişim sistemleri, bir kuruluşun karar alma, koordinasyon, kontrol ve analiz faaliyetlerini desteklemek üzere insan, süreç, veri ve teknolojiyi bir araya getiren yapılardır

(Laudon ve Laudon, 2011). İşlem işleme sistemleri, yönetim raporlama sistemleri, karar destek sistemleri ve yönetici bilgi sistemleri farklı yönetsel düzeylerdeki bilgi ihtiyaçlarına karşılık verir. Güncel dijital dönüşüm yazını ise bilgi sistemlerinin yalnız mevcut süreçleri destekleyen araçlar olmadığını, değer önerisini, örgütsel kimliği ve iş modellerini dönüştürebildiğini vurgulamaktadır (Verhoef vd., 2021; Wessel vd., 2021). Çağdaş YBS yaklaşımı bu dönüşüm doğrultusunda, operasyonel verimlilik ile stratejik ve örgütsel dönüşümü aynı çerçevede değerlendirmelidir.

Kurumsal kaynak planlaması (ERP) sistemleri, finans, insan kaynakları, tedarik zinciri ve müşteri ilişkileri gibi işlevleri bütünsel bir veri tabanı üzerinde bir araya getiren başlıca YBS uygulamalarındandır (Abd Elmonem vd., 2016). Bu bütünsel veri tutarlılığını ve işlem hızını artırırken, tek bir güvenlik açığının birden fazla kurumsal işlevi etkileyebileceği bir risk yoğunlaşması yaratır. Dijital dönüşümün teknoloji kadar örgütsel aktörler, yetkinlikler ve çalışma ortamıyla ilişkili olması, ERP dönüşümlerinde güvenlik ve mahremiyetin yalnız teknik kurulum aşamasına bırakılmamasını gerektirir (Nadkarni ve Prügl, 2021).

Kurumların bulut tabanlı ERP çözümlerine yönelmesinde maliyet etkinliği, ölçeklenebilirlik ve bakım kolaylığı belirleyici olurken, veri güvenliği ve mahremiyet kaygıları geçiş kararını sınırlayabilmektedir (Chang, 2020). Güncel sistematik incelemeler, bulut kullanımında teknik zafiyetlerin yanı sıra yönetişim, güven, farkındalık ve düzenleyici uyum sorunlarının da belirleyici olduğunu ortaya koymaktadır (Ukeje vd., 2024). Hizmet sağlayıcısı ile veri sorumlusu arasındaki görevlerin sözleşmelerde açıkça belirlenmesi ve güvenlik gereksinimlerinin sistem mimarisine başlangıç aşamasında dâhil edilmesi gerekir.

YBS aracılığıyla işlenen veri çeşitliliği müşteri işlemleri, çalışan performansı, tedarikçi kayıtları ve pazarlama analitiği gibi

geniş bir alana yayılmaktadır. Dijital dönüşüm, yeni veri kaynaklarını ve bağlantılı iş modellerini kurumsal karar süreçlerine dâhil ederken veri akışlarının sınırlarını da genişletmektedir (Verhoef vd., 2021). Bu genişleme işletmeleri teknik güvenliğin yanında hukuki uyum ve veri yönetişimi sorumluluğuyla karşı karşıya bırakır. Genişleyen veri akışları karşısında veri sahipliği, veri kalitesi, erişim yetkileri ve saklama süreleri kurumsal stratejiyle bağlantılı biçimde yönetilmelidir.

Karar destek sistemleri (KDS) özelinde bakıldığında, yöneticilere sunulan analitik çıktıların güvenilirliği, temel alınan verinin bütünlüğüne doğrudan bağlıdır. Bir bilgi sisteminin siber saldırıya uğraması yalnızca veri gizliliğini değil, aynı zamanda veri bütünlüğünü de tehdit etmekte, bozulan veya değiştirilen veri üzerinden üretilen kararlar, işletmeyi ciddi operasyonel ve finansal risklere maruz bırakabilmektedir (Kott ve Linkov, 2021). Yönetim bilişim sistemlerinin güvenlik mimarisinde yalnızca gizlilik değil, bütünlük ve erişilebilirlik boyutlarının da eşit ağırlıkla ele alınması gerekmektedir.

Yönetici Destek Sistemlerinin (YDS; Executive Information Systems, EIS) üst düzey stratejik kararları desteklemek amacıyla farklı kaynaklardan konsolide ettiği veriler, genellikle kurumun en hassas bilgilerini içermektedir, bu nedenle söz konusu sistemlere yönelik erişim yetkilendirmesinin çok katmanlı biçimde tasarlanması gerekmektedir. Sistemlerin farklı kullanıcı gruplarına farklı yetki düzeyleri tanıyan rol tabanlı erişim kontrolü (RBAC) modelleriyle yapılandırılması, hem iç tehditlerin hem de dış saldırıların etkisini sınırlandıran temel bir güvenlik uygulaması olarak öne çıkmaktadır.

3. DİJİTALLEŞME SÜRECİNDE SİBER GÜVENLİK KAVRAMI

Siber güvenlik, bilgi sistemlerinin gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde yetkisiz erişim, değiştirme veya tahribata karşı korunmasını ifade eden çok boyutlu bir kavramdır. Sürekli izlenebilir ve ölçümlenebilir veri güvenliğinin sağlanması, kurumsal risk yönetimi modeliyle belirlenen risklerin yönetilmesi ve yeni tehditlerin öngörülebilmesiyle mümkün olmaktadır (Korucu, 2021). Bu bakış açısı, siber güvenliğin yalnızca teknik bir savunma mekanizması değil, aynı zamanda sürekli gözden geçirilmesi gereken dinamik bir yönetim süreci olduğunu ortaya koymaktadır.

Siber dayanıklılık kavramı, saldırı sonrasında sistemlerin operasyonel sürekliliğini koruma ve hızla toparlanma kapasitesini ifade etmekte olup, günümüzde yalnızca önleyici güvenlik önlemleriyle sınırlı kalmayan bütüncül bir yaklaşımı zorunlu kılmaktadır. Siber dayanıklılığın somut biçimde ölçülebilir hâle getirilmesi, kurumların güvenlik yatırımlarının etkinliğini değerlendirebilmesi ve kaynaklarını doğru önceliklendirebilmesi açısından kritik önem taşımaktadır (Kott ve Linkov, 2021). İşletmelerin siber olgunluk düzeylerini periyodik olarak değerlendiren metrik temelli çerçeveler benimsemesi önerilmektedir.

Yapay zekâ destekli güvenlik çözümleri, tehdit tespiti ve müdahale süreçlerinde giderek daha fazla rol üstlenmektedir. Açıklanabilir yapay zekâ yaklaşımları, tehdit avcılığında tespit sonuçlarının güvenlik analistlerince yorumlanmasını kolaylaştırabilir (Kumar vd., 2023). Bununla birlikte bu sistemler yeni kişisel veri işleme faaliyetleri doğurabileceği için veri minimizasyonu, amaçla sınırlılık, ayrımcılık riski ve insan denetimi gibi konular tasarım aşamasında ele alınmalıdır. Çalışan verilerinin yapay zekâ destekli sistemlerle işlenmesi de işverenin

yönetim yetkisi ile çalışanın temel hakları arasında ölçülü bir denge kurulmasını gerektirir (Ses ve Korkusuz, 2025). Bu nedenle yapay zekâ destekli güvenlik uygulamaları, çalışmanın dört bileşenli çerçevesinde teknik kapasite, hukuki uyum, insan denetimi ve kurumsal yönetim gereksinimlerinin kesiştiği bir uygulama alanı olarak değerlendirilmelidir.

İşletmeler açısından siber güvenlik risklerinin kaynağı yalnızca dış saldırganlarla sınırlı değildir, iç tehditler, insan hatası ve süreç eksiklikleri de önemli risk unsurları arasında yer almaktadır. Bilgi sistemlerinin denetiminde siber güvenlik risklerinin kapsamlı biçimde değerlendirilmesi, işletmelerin finansal tablo güvenilirliğinden operasyonel sürekliliğe kadar geniş bir alanı doğrudan etkilemektedir (Öztürk, 2018). Bu bağlamda iç denetim fonksiyonunun bilgi teknolojileri risklerini kapsayacak biçimde genişletilmesi, kurumsal yönetişimin güncel bir gereksinimi olarak öne çıkmaktadır.

Siber güvenliğin yalnız teknik bir sorun olarak görülmesi, çalışan davranışlarını ve kurumsal koşulları ikincil konuma iter. Oysa güncel alan yazını, karar verme süreçleri, güvenlik kültürü, çalışma koşulları ve örgütsel yapıların hem güvenlik açıklarını hem de siber dayanıklılığı biçimlendirdiğini belirtmektedir (Khadka ve Ullah, 2025). Çalışanları yalnızca 'en zayıf halka' olarak nitelemek yerine, güvenli davranışı destekleyen süreçleri ve kullanılabilir kontrolleri geliştirmek daha işlevsel bir yaklaşımdır.

Fidye yazılımı (ransomware) saldırıları, son yıllarda işletmelerin operasyonel sürekliliğini tehdit eden en yaygın siber saldırı türlerinden biri hâline gelmiştir. Bu tür saldırılarda kurumsal veri tabanlarının şifrelenerek erişilemez hâle getirilmesi, yalnızca doğrudan finansal kayıplara değil, aynı zamanda müşteri güveninin sarsılmasına ve itibar kaybına da yol açabilmektedir. Yeni normal dünya düzeninde bilinen siber

saldırı ve veri hırsızlığı yöntemlerine, farklı bilişim platformlarında yaşanan veri güvenliği ihlallerinin eklenmesi, kurumların çok katmanlı ve dinamik bir savunma stratejisi geliştirmesini zorunlu kılmaktadır (Korucu, 2021).

Tedarik zinciri saldırılarında kurum doğrudan hedef alınmak yerine güvendiği yazılım sağlayıcısı, hizmet sunucusu veya iş ortağı üzerinden etkilenmektedir. YBS altyapısının çok sayıda üçüncü taraf bileşeni ve entegrasyonla çalışması saldırı yüzeyini genişletir. Bu risk, tedarikçilerin yalnız hizmet kalitesi bakımından değil, erişim yetkileri, veri işleme rolleri, alt yüklenicileri, olay bildirim süreçleri ve güvenlik olgunluğu bakımından da değerlendirilmesini gerektirir. Bulut ortamlarında hesap verebilirliğin sağlanması, teknik mimari ile sözleşmesel ve yönetsel kontrollerin birlikte kurulmasına bağlıdır (Zaguir vd., 2024).

4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKİ ÇERÇEVE: KVKK VE GDPR

4.1. Türkiye'de Kişisel Verilerin Korunması Kanunu

Türkiye'de kişisel verilerin korunmasını isteme hakkı Anayasa'nın 20. maddesinde güvence altına alınmıştır. Bu anayasal temel üzerine kurulan 6698 sayılı Kanun, kişisel verilerin işleme şartlarını, ilgili kişinin haklarını ve veri sorumlusunun yükümlülüklerini düzenlemektedir. Kanun'un 4. maddesindeki hukuka ve dürüstlük kurallarına uygunluk, doğruluk ve güncellik, belirli ve meşru amaç, amaçla bağlantılı ve ölçülü işleme ile gerekli süre kadar muhafaza ilkeleri YBS'deki veri yaşam döngüsünün tamamına uygulanmalıdır. Veri envanteri, erişim yetkileri, saklama süreleri ve imha süreçleri bu ilkelerle uyumlu biçimde tasarlanmalıdır.

Kanun'un 12. maddesi uyarınca veri sorumlusu, kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemek, verilerin muhafazasını sağlamak için gerekli teknik ve idari tedbirleri almakla yükümlüdür. Kişisel Verileri Koruma Kurumu'nun rehberi erişim kontrolü, kullanıcı hesabı yönetimi, şifreleme, ağ güvenliği, yedekleme, kayıtların izlenmesi ve düzenli testler gibi uygulamaları ayrıntılandırmaktadır (KVKK, 2018a). Bu yaklaşım, YBS güvenliğini tek bir ürün veya yazılıma indirgememekte, risk temelli ve süreklilik taşıyan bir yönetim süreci olarak ele almaktadır.

Kanun'un 12. maddesinin beşinci fıkrasında veri ihlalinin en kısa sürede ilgisine ve Kurula bildirilmesi öngörülmektedir. Kişisel Verileri Koruma Kurulunun 24 Ocak 2019 tarihli ve 2019/10 sayılı kararıyla “en kısa sürede” ifadesi, veri sorumlusunun ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirim yapması şeklinde yorumlanmıştır (KVKK, 2019).

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), kayıt yükümlülüğü bulunan veri sorumlularının veri işleme faaliyetlerine ilişkin bilgileri bildirdiği sicil sistemidir. Bununla birlikte kayıt yükümlülüğü bütün veri sorumluları için mutlak değildir. Kişisel Verileri Koruma Kurulunun 2018/32 sayılı kararı istisna tutulan veri sorumlusu gruplarını belirlemiş, 2023/1154 sayılı karar ise istisna kriterlerinden birini güncellemiştir (KVKK, 2018b, 2023). Kayıtlı yükümlü kuruluşların bildirimlerinde işleme amaçları, veri kategorileri, alıcı grupları, azami saklama süreleri, yurt dışına aktarım bilgileri ve alınan güvenlik tedbirleri yer alır. VERBİS bildiriminin güncel bir kişisel veri işleme envanterine dayanması, sicil kaydını biçimsel bir işlem olmaktan çıkarıp veri yönetişiminin parçası hâline getirir.

Çalışan verileri, iş ilişkisinin kurulmasından sona ermesine kadar insan kaynakları bilgi sistemleri, erişim kayıtları, performans değerlendirmeleri ve iş sağlığı süreçleri gibi çok sayıda kanaldan işlenmektedir. Özellikle yapay zekâ destekli izleme ve karar sistemleri, veri minimizasyonu, şeffaflık, ölçülülük ve insan denetimi bakımından yeni riskler doğurmaktadır (Ses ve Korkusuz, 2025). Bu risklerin sınırlandırılması için erişim yetkilerinin görevle sınırlandırılması, saklama sürelerinin belirlenmesi ve çalışanların anlaşılır biçimde aydınlatılması gerekir. Böylece yapay zekâ kullanımı yalnız teknik bir güvenlik veya verimlilik aracı olarak değil, hukuki dayanak, insan hakları üzerindeki etki ve yönetim sorumluluklarıyla birlikte ele alınmaktadır.

4.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü 25 Mayıs 2018'den itibaren uygulanmaktadır (Avrupa Parlamentosu ve Avrupa Birliği Konseyi, 2016). GDPR, yerleşim yeri ölçütüne ek olarak Birlik içindeki kişilere mal veya hizmet sunulması ya da davranışlarının izlenmesi gibi koşullarda bölge dışındaki kuruluşlara da uygulanabilir. Tüzük, veri korumasının tasarım aşamasında ve varsayılan ayarlarda gözetilmesini öngörür. Güncel gereksinim mühendisliği çalışmaları da düzenleyici veri koruma gereklerinin yazılım geliştirme yaşam döngüsünün başında tanımlanmasının önemini vurgulamaktadır (Negri-Ribalta vd., 2024).

GDPR uyumu, özellikle sınırlı hukuki ve teknik kaynağa sahip küçük ve orta ölçekli işletmeler için güç bir süreçtir. Veri işleme faaliyetlerinin ve yasal dayanakların belirlenmesi, risklerin değerlendirilmesi, ilgili kişi taleplerinin yönetilmesi, ihlal müdahale süreçlerinin kurulması ve uluslararası aktarımların izlenmesi birlikte yürütülmelidir. Sistematik alan yazını, yalnız

standart edinmenin uygulama yol haritası oluşturmak için yeterli olmayabileceğini, bilgi yönetişimi ile kurumsal mimarinin uyum programını destekleyen başlıca unsurlar arasında bulunduğunu belirtmektedir (Zaguir vd., 2024).

Kamu kurumlarının ve işletmelerin bulut hizmetlerine yönelmesi, veri koruma uyumunu hizmet sağlayıcılar ve alt işleyenler nedeniyle daha karmaşık hâle getirmektedir. Bulut benimsemesine ilişkin sistematik incelemelerde yetkisiz erişim, gizlilik kaybı, farkındalık eksikliği, güven sorunu ve düzenleyici belirsizlikler ortak riskler olarak belirlenmiştir (Ukeje vd., 2024). Bulut tedarikçisi seçimi bu çerçevede veri merkezi konumu, alt hizmet sağlayıcılar, erişim kayıtları, şifreleme, veri taşınabilirliği ve sözleşmenin sona ermesinden sonraki silme süreçlerini kapsamalıdır.

GDPR'de hesap verebilirlik, kuruluşun yalnız kurallara uymasını değil, uyumu kanıtlayabilmesini de gerektirir. İşleme kayıtları, risk değerlendirmeleri, veri koruma etki değerlendirmeleri, ihlal kayıtları ve alınan teknik ve yönetsel tedbirler bu kanıtlama işlevine hizmet eder. Düzenleyici gereksinimlerin bilgi sistemlerine aktarılmasındaki güçlükler, hukuk ve yazılım ekipleri arasında sistemli bir iş birliğini gerekli kılmaktadır (Negri-Ribalta vd., 2024).

KVKK ile GDPR ortak ilkeler taşımakla birlikte kapsam, kurumsal roller, ihlal bildirimi, yaptırımlar ve yurt dışına aktarım mekanizmaları bakımından aynı düzenlemeler değildir. KVKK'nın 9. maddesinde 2024 yılında yapılan değişikliklerle yeterlilik kararı, uygun güvenceler ve arıza aktarım halleri esasına dayanan yeni bir sistem benimsenmiş, standart sözleşmeler ile bağlayıcı şirket kuralları uygun güvence yöntemleri arasında düzenlenmiştir (KVKK, 2024a, 2024b). Uluslararası faaliyet gösteren Türk işletmeleri iki düzenlemenin kesişen ilkelerini

ortak kontrollerle yönetebilir, ancak her düzenlemenin ayrı yükümlülüklerini ayrıca değerlendirmelidir.

Tablo 1. KVKK ve GDPR'nin Temel Unsurlar Açısından Karşılaştırılması

Karşılaştırma unsuru	KVKK	GDPR
Uygulama alanı	Türkiye'deki veri işleme faaliyetleri ve Kanun'un kapsam hükümleri	AB içindeki faaliyetler ile belirli koşullarda bölge dışındaki mal veya hizmet sunumu ve izleme faaliyetleri
Temel ilkeler	Hukuka uygunluk, doğruluk ve güncellik, amaçla sınırlılık, ölçülülük ve gerekli süre kadar saklama	Hukuka uygunluk, adillik ve şeffaflık, amaçla sınırlılık, veri minimizasyonu, doğruluk, saklama sınırı, bütünlük ve hesap verebilirlik
Özel nitelikli veriler	6. madde kapsamında 2024'te güncellenen işleme şartları	9. madde kapsamında özel veri kategorileri ve istisnalar
İhlal bildirimi	Kurulun 2019/10 sayılı kararı uyarınca, ihlalin öğrenilmesinden itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirim	Risk doğuran ihlallerde mümkünse 72 saat içinde denetim makamına bildirim
Yurt dışına aktarım	Yeterlilik kararı, uygun güvenceler ve arızı hâller. 2024'te yenilenen sistem	Yeterlilik kararı, uygun güvenceler ve istisnalar
Kurumsal roller	Veri sorumlusu ve veri işleyen. VERBİS için istisnalar bulunur	Veri sorumlusu, veri işleyen ve belirli durumlarda veri koruma görevlisi
Yaptırımlar	Kanun'un 18. maddesindeki idari para cezaları; standart sözleşmenin beş iş günü içinde Kuruma bildirilmemesi hâlinde ayrıca 50.000–1.000.000 TL idari para cezası	Yüzde esaslı üst sınırlar dâhil kademeli idari para cezaları
Tasarım yaklaşımı	Tasarımdan ve varsayılan ayarlardan itibaren mahremiyet açık bir kanun hükmü olarak düzenlenmemiştir. Yaklaşım, genel ilkeler ve veri güvenliği yükümlülüğü üzerinden dolaylı biçimde desteklenir	Tasarımdan ve varsayılan ayarlardan itibaren veri koruma, GDPR'nin 25. maddesinde açık bir yükümlülük olarak düzenlenir

Not: Hukuki dayanaklar: KVKK m. 6, m. 9, m. 12 ve m. 18; Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı kararı; GDPR m. 9, m. 25, m. 33 ve m. 83. Tablo, bu düzenlemeler temel alınarak yazar tarafından sentezlenmiştir.

5. YÖNETİM BİLİŞİM SİSTEMLERİNDE VERİ MAHREMİYETİ RİSKLERİ

5.1. Bulut Bilişim ve ERP Sistemlerinde Güvenlik

Bulut bilişim işletmelere ölçeklenebilirlik, esneklik ve maliyet avantajı sağlarken, veri üzerindeki fiilî kontrolün hizmet sağlayıcılarla paylaşılması yeni güvenlik ve mahremiyet riskleri doğurur. Sistematik incelemeler, bulut ortamlarındaki risklerin yalnız teknik açıklarla sınırlı olmadığını, yönetim, güven, farkındalık ve düzenleyici uyum sorunlarını da kapsadığını belirtmektedir (Ukeje vd., 2024). Koruma düzeninde veri sınıflandırma, güçlü kimlik doğrulama, erişim kontrolü, şifreleme, kayıt izleme, yedekleme ve olay müdahalesi bütünlük biçimde kurulmalıdır.

ERP sistemlerinin bulut ortamına taşınması sürecinde veri güvenliği kaygıları, organizasyonların geçiş kararını erteleme ya da hibrit modelleri tercih etme eğilimini artıran başlıca faktörler arasında yer almaktadır. Organizasyonların bulut ERP sistemlerine geçiş kararında hem kolaylaştırıcı hem de engelleyici faktörlerin bir arada değerlendirilmesi gerekmekte, veri güvenliği ve mahremiyet kaygıları bu değerlendirmede belirleyici bir ağırlığa sahip olmaktadır (Chang, 2020). Bulut ERP tedarikçisi seçiminde sağlayıcının güvenlik sertifikasyonları ve veri merkezi konumlarının değerlendirilmesi kritik önem taşımaktadır.

Kurumsal sistemlerde veri kalitesi ile siber güvenlik arasındaki ilişki, alan yazında giderek daha fazla dikkat çeken bir konu hâline gelmiştir, düşük veri kalitesi, güvenlik açıklarının tespit edilmesini zorlaştırabilmekte ve yanlış karar alma risklerini artırabilmektedir. Bulut ERP sistemlerinde siber güvenlik ve veri kalitesinin birlikte ele alınması, organizasyonların hem operasyonel güvenilirliğini hem de mevzuat uyumluluğunu güçlendiren bütüncül bir yaklaşım olarak değerlendirilmektedir.

Bu bağlamda veri yönetişimi süreçlerinin güvenlik politikalarıyla entegre biçimde tasarlanması önerilmektedir.

Kurumsal ağların bölümlere ayrılması (segmentasyon), kişisel verilerin işlendiği ağ alanlarının diğer kurumsal kaynaklardan izole edilmesini sağlayarak olası bir ihlalin etkisini sınırlandırmaya yardımcı olmaktadır. Kişisel verilerin işlendiği ağ bölümünün ayrı biçimde yapılandırılması hâlinde, güvenlik kaynaklarının tüm ağ yerine yalnızca bu sınırlı alanın korunmasına yoğunlaştırılabileceği vurgulanmaktadır (KVKK, 2018a). Bu teknik yaklaşım, özellikle çok uluslu ya da çok şubeli işletmelerin veri güvenliği mimarisinde önceliklendirilmesi gereken bir uygulama olarak öne çıkmaktadır.

Kimlik ve erişim yönetimi (Identity and Access Management), bulut tabanlı yönetim bilişim sistemlerinde en kritik güvenlik bileşenlerinden birini oluşturmaktadır. Kaba kuvvet saldırılarına karşı parola girişi deneme sayısının sınırlandırılması, düzenli parola değişiminin sağlanması ve yönetici yetkisinin yalnızca gerekli durumlarda etkinleştirilmesi, temel ancak etkili koruma önlemleri arasında sayılmaktadır (KVKK, 2018a). Çok faktörlü kimlik doğrulama (MFA), erişim için parola gibi tek bir unsurla yetinmeyip en az iki bağımsız doğrulama unsurunun kullanılmasını sağlayarak özellikle ayrıcalıklı ve uzaktan erişimlerde hesap ele geçirme riskini azaltan tamamlayıcı bir IAM kontrolüdür. Bunlara ek olarak, kurumdan ayrılan çalışanların hesaplarının zaman kaybetmeksizin devre dışı bırakılması, yetkisiz erişim risklerinin azaltılmasında belirleyici bir uygulamadır.

Şifreleme, hem durağan hem de aktarım hâlindeki veriler için temel bir koruma katmanıdır. Bununla birlikte şifrelemenin etkinliği algoritma seçiminin yanında anahtarların üretimi, saklanması, yenilenmesi, erişim yetkileri ve imha süreçlerinin güvenliğine bağlıdır. Bulut ERP hizmetinde hangi verinin kim

tarafından şifrelendiği, anahtarların kimin denetiminde bulunduğu ve hizmet sona erdiğinde verinin nasıl silineceği sözleşmede açıklanmalıdır. Tasarımdan itibaren mahremiyet yaklaşımı, bu kararların sistem devreye alındıktan sonra değil, mimari tasarım sırasında alınmasını gerektirir (Bal vd., 2026).

Uzaktan ve hibrit çalışma, kurumsal ağın fiziksel sınırlarını belirsizleştirdiği için çevre güvenliğine dayalı geleneksel yaklaşımın etkisini azaltmıştır. Sıfır güven mimarisi, kullanıcıyı veya cihazı ağ içindeki konumuna dayanarak güvenilir saymamakta, her erişim isteğinin kimlik, cihaz durumu, bağlam ve yetki bakımından doğrulanmasını esas almaktadır (Kang vd., 2023). Bu yaklaşım tek bir ürün değil, kimlik yönetimi, en az ayrıcalık, ağ bölümlendirme, sürekli izleme ve yönetim bileşenlerinden oluşan kurumsal bir dönüşümdür. Uygulamanın başarısı teknik mimari kadar üst yönetim desteğine, yetkinliğe ve aşamalı bir olgunluk planına bağlıdır (Yeoh vd., 2023).

5.2. Çalışan Davranışı ve İçeriden Gelen Tehditler

Çalışanlar güvenlik olaylarında önemli bir rol oynamakla birlikte onları doğrudan 'en zayıf halka' olarak tanımlamak sorunu tek boyuta indirger. Güvenli olmayan davranışlar çoğu zaman arayüz tasarımı, iş yükü, eğitim niteliği, örgütsel iklim ve yönetim tercihleriyle birlikte şekillenir (Khadka ve Ullah, 2025). Siber güvenlik kültürüne ilişkin uygulamalar da politika, iletişim, eğitim, çalışan katılımı ve yönetim desteğinin birbirini tamamlayan bir düzen içinde ele alınmasını gerektirir (Alshaikh, 2020). Etik olmayan veya ihmalkâr çalışan davranışları ağ ve uygulama kötüye kullanımı, riskli internet kullanımı, güvenlik kurallarının ihlali ve yetersiz erişim kontrolü gibi kategoriler altında incelenebilir (Chu ve So, 2020). Etkili risk yönetimi, çalışan sorumluluğu ile kurumun güvenli çalışma koşulları oluşturma yükümlülüğünü birlikte ele almalıdır.

Güvenlik farkındalık programları ile yaptırım algısının farklı davranış türlerinde aynı sonucu üretmemesi, tek tip bir müdahale stratejisinin sınırlı kalabileceğini düşündürmektedir (Chu ve So, 2020). Farkındalık, bilgi ve güvenli davranış birbiriyle ilişkili olmakla birlikte aynı kavramlar değildir. Kullanıcının tehdidi tanıması, koruyucu aracı doğru kullanacağı anlamına gelmeyebilir (Zwilling vd., 2022). Kurumların eğitim programlarını davranış temelli risk analizi, uygulamalı ölçüm ve düzenli geri bildirimle desteklemesi, kaynakların daha etkili kullanılmasına katkı sağlayabilir.

Güvenlik kültürü ile istihdam ilişkisinin çalışanların güvenlik uyum davranışlarını nasıl şekillendirdiği üzerine yapılan araştırmalarda, örgütsel güvenlik kültürünün ve çalışan-işveren ilişkisinin kalitesinin, resmi politika ve prosedürlerden bağımsız olarak güvenlik uyumunu doğrudan etkilediği belirlenmiştir (D'Arcy ve Greene, 2014). Bu sonuç, güvenlik yönetiminin yalnızca kural koyucu bir yaklaşımla değil, çalışan bağlılığını ve güven ilişkisini gözetken bir örgüt kültürü inşasıyla desteklenmesi gerektiğine işaret etmektedir.

İçeriden kaynaklanan risklerin yönetiminde çalışanların güvenlik olaylarını bildirmekten çekinmesi önemli bir engeldir. Cezalandırılma korkusu, bildirim kanalının bilinmemesi veya karmaşık prosedürler olayların gecikmesine yol açabilir. Bildirim mekanizmaları kolay erişilebilir ve öğrenmeyi teşvik eden bir yapıda kurulmalıdır. İnsan faktörünü davranış, karar verme ve örgütsel kültürle birlikte ele alan çalışmalar, bireysel eğitimin ancak kurumsal süreçler ve yönetim desteğiyle tamamlandığında kalıcı sonuç üretebileceğini belirtmektedir (Khadka ve Ullah, 2025).

Sosyal mühendislik saldırıları, teknik açıklardan çok güven, acelecilik ve otorite algısı gibi insani özellikleri kullanır. Kimlik avı e-postaları, sahte destek çağrıları ve hedef odaklı

kimlik avı girişimleri bu saldırıların yaygın örnekleridir. Eğitimlerin yalnız bilgi aktarımına dayanmaması, çalışanların gerçekçi senaryolarla güvenli davranışı uygulamasına imkân vermesi gerekir. Simülasyon sonuçları çalışanları cezalandırmak için değil, riskli iş akışlarını ve ek desteğe ihtiyaç duyulan alanları belirlemek için kullanılmalıdır (Khadka ve Ullah, 2025).

6. KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİMİ: STANDARTLAR VE UYGULAMALAR

6.1. ISO/IEC 27001 ve Risk Yönetimi Çerçeveleri

ISO/IEC 27001, kurumların bilgi güvenliği yönetim sistemini kurması, uygulaması, sürdürmesi ve sürekli iyileştirmesi için risk temelli bir çerçeve sunmaktadır. Güncel ISO/IEC 27001:2022 sürümü varlıkların, tehditlerin, zafiyetlerin ve kontrollerin kuruluşun bağlamı içinde değerlendirilmesini gerektirir. Sertifikasyon, tek başına KVKK veya GDPR uyumunu kanıtlamaz. Bununla birlikte risk değerlendirmesi, sorumlulukların belirlenmesi, dokümantasyon, iç denetim ve sürekli iyileştirme süreçleri hukuki uyumu destekleyebilir. Standart ile mevzuat arasındaki ilişkinin bir eşdeğerlik değil, tamamlayıcılık ilişkisi olduğu gözetilmelidir (Zaguir vd., 2024).

COBIT 2019, kurumsal bilgi ve teknolojinin yönetişimi ile yönetimini işletme hedefleriyle ilişkilendiren güncel bir çerçeve sunmaktadır. Çekirdek modelde beş alan altında kırk yönetişim ve yönetim hedefi bulunmakta, bilgi güvenliği, bulut bilişim ve güncel teknoloji eğilimleri odak alanlarıyla ele alınabilmektedir (ISACA, 2018). COBIT 2019'un ISO/IEC 27001 ile birlikte kullanılması, güvenlik kontrollerinin kurumsal hedefler, sorumluluklar, performans göstergeleri ve güvence süreçleriyle ilişkilendirilmesine yardımcı olabilir. Bununla birlikte her iki çerçeve de somut KVKK ve GDPR

yükümlülüklerinin ayrıca değerlendirilmesi gereğini ortadan kaldırmaz.

Kurumsal risk yönetimi, bulut tabanlı sistemlerde risklerin tanımlanması, değerlendirilmesi, azaltılması ve sürekli izlenmesini kapsar. Bulut ortamındaki yapılandırmalar, kullanıcı hesapları, yazılım bileşenleri ve alt hizmet sağlayıcılar zaman içinde değişebildiğinden tek seferlik risk değerlendirmesi yeterli değildir. Risk kaydı, varlık envanteri, zafiyet yönetimi, olay kayıtları ve tedarikçi değerlendirmeleri birbirini besleyen bir izleme düzeni içinde yürütülmelidir (Ukeje vd., 2024).

Bilgi sistemlerinin denetiminde siber güvenlik risklerine yönelik bütüncül bir denetim modeli önerisi, risklerin yalnızca bilgi işlem birimi tarafından değil, iç denetim, risk yönetimi ve üst yönetim işbirliğiyle ele alınmasının önemine dikkat çekmektedir (Öztürk, 2018). Bu yaklaşım, bilgi güvenliğinin izole bir teknik fonksiyon olarak değil, kurumsal yönetişimin bütünlüğü bir parçası olarak konumlandırılması gerektiğini ortaya koymaktadır.

Olay müdahale planlaması (incident response planning), bir güvenlik ihlali gerçekleştiğinde kurumun ne hızla ve ne kadar etkin biçimde tepki verebileceğini belirleyen kritik bir hazırlık sürecidir. Bilişim sisteminin çökmesi, kötü niyetli yazılım bulaşması, hizmet dışı bırakma saldırısı ya da gizlilik ve bütünlüğü bozan ihlaller gibi istenmeyen olaylarda, delillerin toplanması ve güvenli biçimde saklanması gerekmektedir (KVKK, 2018a). Bu süreçlerin önceden tanımlanmış rol ve sorumluluklarla desteklenen bir olay müdahale planına dayandırılması, kriz anındaki karar verme hızını ve etkinliğini artırmaktadır.

Güvenlik açığı taramaları ve sızma testleri, kurumsal bilgi sistemlerinin bilinen zafiyetlere karşı ne ölçüde dayanıklı olduğunu ölçmeye yönelik proaktif değerlendirme araçlarıdır.

Güvenlik yazılımı mesajlarının, erişim kontrolü kayıtlarının ve diğer raporlama araçlarının düzenli biçimde kontrol edilmesi ile bu sistemlerden gelen uyarılar üzerine zamanında harekete geçilmesi gerektiği vurgulanmakta, düzenli zafiyet taramaları ve sızma testlerinin yapılması önerilmektedir (KVKK, 2018a). Bu değerlendirmelerin sonuçlarına göre güvenlik önceliklerinin periyodik olarak gözden geçirilmesi, kurumsal risk profilinin güncel tutulmasını sağlamaktadır.

6.2. Güvenlik Kültürü ve Farkındalık Eğitimleri

Kurumsal güvenlik kültürü, teknik kontrollerin günlük çalışma pratiklerinde karşılık bulmasını sağlayan tamamlayıcı bir unsurdur. Farkındalık eğitimleri düzenli ve role göre uyarlanmış biçimde tasarlanmalı, çalışanların güncel tehditleri tanınması ve şüpheli durumları doğru kanallardan bildirmesi sağlanmalıdır. Güvenlik kültürünün kalıcı hâle gelmesi, yönetim desteği, açık iletişim, çalışan katılımı ve uygulamaların düzenli değerlendirilmesiyle mümkündür (Alshaikh, 2020). Böylece çalışan yalnız risk kaynağı olarak değil, kurumsal dayanıklılığın etkin bir bileşeni olarak konumlandırılabilir.

Farkındalık programlarında aynı içeriğin bütün çalışanlara sunulması yerine görev, erişim düzeyi ve karşılaşılan tehditler dikkate alınmalıdır. İnsan kaynakları personeli çalışan verileri, finans birimi ödeme dolandırıcılığı, sistem yöneticileri ise ayrıcalıklı hesaplar bakımından farklı risklere maruz kalır. Farkındalık ve bilgi düzeyinin güvenli davranışla ilişkili olması, eğitim etkinliğinin yalnız katılım oranıyla ölçülemeyeceğini ortaya koymaktadır (Zwilling vd., 2022). Simülasyon sonuçları, olay bildirim süresi, tekrar eden hata örüntüleri ve güvenli davranış göstergeleri birlikte izlenmelidir.

Üniversite kütüphaneleri örneğinde yürütülen bir çalışma, kişisel verilerin korunmasına yönelik farkındalığın yalnızca özel sektör kuruluşlarıyla sınırlı olmadığını, kamu hizmeti sunan bilgi

merkezlerinin de kullanıcı verilerinin gizliliği, bütünlüğü ve kullanılabilirliğini gözeten politikalar geliştirmesi gerektiğini ortaya koymaktadır (Henkoğlu ve Uçak, 2015). Bu bulgu, veri mahremiyeti yönetiminin sektör bağımsız bir kurumsal sorumluluk alanı olarak ele alınması gerektiğini göstermektedir.

Güvenlik kültürünün üst yönetim tarafından açıkça desteklenmesi ve kaynak tahsisinde önceliklendirilmesi, farkındalık programlarının sürdürülebilirliği açısından belirleyici bir faktördür. Örgütsel güvenlik ikliminin çalışanların güvenlik uyum davranışlarına doğrudan yansıdığı gösterildiğinden (D'Arcy ve Greene, 2014), yöneticilerin güvenlik konusundaki söylem ve uygulamaları arasındaki tutarlılık, çalışanların güvenlik önlemlerini içselleştirme düzeyini doğrudan etkilemektedir.

7. TÜRKİYE'DE İŞLETMELERDE KVKK UYUMLULUĞU: UYGULAMA SORUNLARI VE ÖNERİLER

Türkiye'de özellikle küçük ve orta ölçekli işletmeler, KVKK uyumunun hukuki, teknik ve idari bileşenlerini aynı anda yönetmekte güçlük yaşayabilir. Veri işleme envanterinin hazırlanması, aydınlatma yükümlülüğü, işleme şartlarının belirlenmesi, ilgili kişi başvurularının yönetimi, saklama ve imha süreçleri ile güvenlik tedbirleri farklı uzmanlıkların birlikte çalışmasını gerektirir. GDPR uyumuna ilişkin güncel incelemeler de sınırlı kaynak, uzmanlık eksikliği ve uygulama yol haritası yetersizliğinin ortak sorunlar olduğunu belirtmektedir (Zaguir vd., 2024). Uyum programı kuruluşun ölçeğine ve risk profiline göre önceliklendirilmelidir.

KVKK uygulamasındaki güncel dönüşüm yalnız mevzuat metninin değiştirilmesiyle sınırlı değildir. 7499 sayılı Kanun ile özel nitelikli kişisel verilerin işlenmesini düzenleyen 6. madde,

yurt dışına aktarımı düzenleyen 9. madde ve kabahatlere ilişkin 18. madde değiştirilmiş, ayrıca geçiş hükmü getirilmiştir. Değişiklikler 1 Haziran 2024 tarihinde yürürlüğe girmiş, 9. maddenin değişiklikten önceki birinci fıkrasının yeni düzenlemeyle birlikte 1 Eylül 2024 tarihine kadar uygulanmasına imkân tanınmıştır (KVKK, 2024a). Bu değişiklikler işletmelerin işleme envanterlerini, hukuki dayanaklarını, sözleşmelerini ve bilgi sistemi akışlarını yeniden değerlendirmesini gerektirmiştir. Bu durum, hukuki uyum kararlarının doğrudan YBS mimarisi ve tedarikçi yönetimiyle ilişkilendirilmesi gerektiğini açıkça ortaya koymaktadır.

İşletmelerin karşılaştığı başlıca sorunlardan biri, kişisel verinin hangi sistemlerde, hangi amaçla ve ne kadar süreyle tutulduğunun eksiksiz belirlenememesidir. Veri keşfi araçları bu süreci destekleyebilir, ancak otomatik keşif sonuçları tek başına hukuki nitelendirme yapamaz. Teknik tarama, süreç sahipleriyle görüşme ve kayıtların örneklenmesi birlikte yürütülmelidir. Elde edilen envanter, VERBİS bildirimi gereken durumlarda bu bildirimin dayanağını oluşturmalı ve sistem değişiklikleriyle birlikte güncellenmelidir (Athier Olca ve Can, 2024; KVKK, 2018b, 2023).

Küçük ve orta ölçekli işletmelerin uyum maliyetlerini karşılayabilme kapasitesi, büyük ölçekli kurumlara kıyasla belirgin biçimde sınırlıdır. KOBİ'lerin KVKK uyum süreçlerinde tüm gereklilikleri aynı anda karşılamaya çalışmak yerine, risk düzeyine göre önceliklendirilmiş kademeli bir uygulama takvimi izlemesi daha gerçekçi bir strateji olarak değerlendirilmektedir. Öncelikle en yüksek hacimde ve en hassas nitelikte kişisel veri işlenen süreçlerin güvence altına alınması, sınırlı kaynakların etkin biçimde kullanılmasına katkı sağlayacaktır.

Sektörel farklılıklar, kişisel veri işleme riskinin niteliğini doğrudan etkiler. Sağlık, finans ve eğitim gibi alanlarda özel

nitelikli veriler, yoğun izleme faaliyetleri veya yüksek etkili karar süreçleri bulunabilir. Bu kuruluşlar KVKK'nın 6. maddesinde 2024 yılında yapılan değişiklikleri, sektörel düzenlemeleri ve Kişisel Verileri Koruma Kurulu kararlarını birlikte değerlendirmelidir (Turan Başara, 2024). Güvenlik tedbirleri yalnız sektör adına göre değil, işlenen verinin niteliği, hacmi, erişim çevresi ve ihlalin kişiler üzerindeki olası etkisine göre belirlenmelidir.

Tedarikçi ve iş ortağı yönetimi, KVKK uyumunun kritik bir boyutudur. Kişisel veri işleyen üçüncü taraflarla yapılan sözleşmelerde tarafların rolleri, işleme amacı, güvenlik tedbirleri, alt yükleniciler, olay bildirimini, denetim hakkı, saklama süresi ve hizmet sonunda silme veya iade şartları açıklanmalıdır. Yurt dışındaki hizmet sağlayıcılara veri aktarılıyorsa KVKK'nın güncel 9. maddesindeki aktarım mekanizmaları ayrıca incelenmelidir. Standart sözleşme kullanılması, veri akış haritasında veri aktaran ile veri alıcısının, aktarım ülkelerinin, veri kategorilerinin, erişim yetkilerinin ve alt işleyenlerin açık biçimde tanımlanmasını gerektirir. Sözleşmedeki güvenlik, saklama, silme ve olay bildirim hükümleri de YBS yapılandırmaları ve denetim kayıtlarıyla uygulanabilir hâle getirilmelidir. İmzalanan standart sözleşmenin beş iş günü içinde Kuruma bildirilmesi gerekir. Bildirim fiziki olarak, kayıtlı elektronik posta (KEP) üzerinden veya Kurul tarafından kullanıma sunulan Standart Sözleşme Bildirim Modülü aracılığıyla gerçekleştirilebilir (KVKK, 2024b, 2024c). Bu bildirim yükümlülüğünün yerine getirilmemesi, Kanun'un 18. maddesi uyarınca veri sorumlusu veya veri işleyen hakkında 50.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezasına yol açabilir (KVKK, 2024a).

Uygulamayı somutlaştırmak amacıyla temsili bir KOBİ senaryosu düşünülebilir. Çalışan ve müşteri kayıtlarını yurt dışındaki bir bulut hizmetinde tutan çevrimiçi perakende

işletmesi, ilk aşamada insan kaynakları, satış, erişim kaydı ve müşteri iletişimi verilerinin akışını envantere işlemelidir. İşleme şartları ve saklama süreleri belirlendikten sonra veri aktaran ile veri alıcısının rolleri, aktarım ülkesi, alt işleyenler ve erişim yetkileri veri akış haritasında gösterilmelidir. Uygun aktarım mekanizması seçilirken standart sözleşme gerekiyorsa beş iş günlük bildirim takvimi sorumlu birime atanmalı ve bildirim için fiziki yol, KEP veya Standart Sözleşme Bildirim Modülü kullanılmalı, teknik tarafta çok faktörlü kimlik doğrulama, rol tabanlı erişim, şifreleme, olay kayıtları ve hizmet sonundaki silme süreci yapılandırılmalıdır. Bu senaryo, Tablo 2'deki aşamaların hukuk, bilgi işlem, satın alma ve süreç sahiplerinin ortak çalışmasıyla uygulanabileceğini görünür kılmaktadır. Bu temsili senaryo, alan yazını ve güncel mevzuattan hareketle bu bölüm kapsamında oluşturulan uygulama örneğidir ve çalışmanın kavramsal çerçevesini işletme düzeyindeki somut adımlarla ilişkilendirmeyi amaçlamaktadır.

Yapılan değerlendirmeler doğrultusunda işletmelerin KVKK uyumunu tek seferlik bir belge hazırlama projesi olarak değil, sürekli izlenen bir yönetim süreci olarak ele alması gerekir. Veri koruma sorumlulukları hukuk ve bilgi işlem birimleriyle sınırlandırılmamalı, insan kaynakları, satın alma, pazarlama, iç denetim ve üst yönetimi kapsayan bir yapı kurulmalıdır. Uygulama takvimi veri hacmi, hassasiyet, erişim çevresi ve ilgili kişiler üzerindeki olası etki esas alınarak önceliklendirilmelidir. ISO/IEC 27001 gibi standartlar risk yönetimi ve sürekli iyileştirme bakımından destekleyici araçlar olarak kullanılmalı, ancak mevzuata uyumun yerine geçtiği varsayılmamalıdır. Çalışan eğitimleri de güncel tehdit senaryolarına ve görev bazlı risklere göre düzenli olarak yenilenmelidir.

Tablo 2. İşletmeler İçin KVKK Uyum Yol Haritası

Aşama	Temel işlem	Sorumlu birimler	YBS'ye teknik yansımaları	Üretilmesi gereken kayıt
1. Veri keşfi	Sistemlerdeki kişisel verilerin ve veri akışlarının belirlenmesi	Bilgi işlem ve süreç sahipleri	Veri keşfi, sınıflandırma ve akış haritası	Kişisel veri işleme envanteri
2. Hukuki değerlendirme	Amaç, işleme şartı, saklama süresi ve aktarım dayanağının belirlenmesi	Hukuk ve süreç sahipleri	İşleme kuralları ile saklama sürelerinin sisteme tanımlanması	Hukuki dayanak ve saklama kaydı
3. Risk analizi	Veri ve sistem risklerinin ölçülerek önceliklendirilmesi	Bilgi güvenliği ve risk yönetimi	Erişim, şifreleme, yedekleme ve kayıt kontrolleri	Risk değerlendirme ve kontrol planı
4. Tedarikçi kontrolü	Veri işleyenlerin, alt işleyenlerin ve yurt dışı aktarımların incelenmesi	Satın alma, hukuk ve bilgi işlem	Aktarım noktaları, roller ve yetkilerin sistemde belgelenmesi	Sözleşme, aktarım ve tedarikçi denetim kaydı
5. Olay yönetimi	İhlal tespiti, müdahale, bildirim ve delil saklama süreçlerinin kurulması	Olay müdahale ekibi ve hukuk	Log, uyarı, erişim kesme ve bildirim mekanizmaları	Olay ve ihlal kayıtları
6. İzleme ve iyileştirme	Envanterin, kontrollerin ve eğitimlerin periyodik olarak güncellenmesi	İç denetim ve üst yönetim	Sürekli izleme ve performans göstergeleri	Periyodik uyum ve iyileştirme raporu

Not: Tablo, bu bölümde incelenen KVKK yükümlülükleri, bilgi güvenliği kontrolleri ve kurumsal yönetim ilkelerinin uygulamaya aktarılması amacıyla yazar tarafından oluşturulan özgün bir sentezdir.

8. SONUÇ

Çalışma, yönetim bilişim sistemlerinde siber güvenlik ve veri mahremiyetinin birbirinden ayrı yönetilemeyeceğini açıklayan kavramsal bir çerçeve sunmuştur. Bulut bilişim, ERP, yapay zekâ ve üçüncü taraf entegrasyonları işletmelere hız ve ölçek kazandırırken kişisel verinin daha geniş ve değişken bir ekosistemde işlenmesine yol açmaktadır. YBS güvenliği bu açıdan yalnız sistemlerin saldırılara karşı korunmasıyla sınırlı değildir. Verinin hangi amaçla işlendiğinin, kimlerce erişilebildiğinin, nerede saklandığının, ne zaman silineceğinin ve ihlal hâlinde nasıl müdahale edileceğinin de yönetilmesini kapsar.

Yapılan değerlendirmeler, etkili YBS güvenliğinin dört bileşenin birlikte işletilmesine bağlı olduğunu göstermiştir. Bunlar teknik güvenlik, hukuki uyum, insan faktörü ve kurumsal yönetişimdir. Şifreleme, erişim kontrolü ve izleme gibi teknik önlemler hukuki dayanak, şeffaflık ve veri minimizasyonu ilkeleriyle desteklenmelidir. Çalışanların güvenli davranışı ise kullanılabilir kontroller, görev bazlı eğitim, açık bildirim kanalları ve yönetim desteğiyle güçlendirilmelidir. Risklerin sahipliği ve denetimi üst yönetim düzeyinde tanımlanmadığında bu unsurların kalıcı bir sisteme dönüşmesi güçleşir.

KVKK ile GDPR arasındaki ortak ilkeler, işletmelere bazı kontrolleri bütünsel biçimde kurma imkânı verir. Bununla birlikte iki düzenlemenin kapsamı, veri ihlali bildirimleri, kurumsal roller, yaptırımlar ve yurt dışına aktarım mekanizmaları aynı değildir. Özellikle KVKK'nın 2024 değişiklikleri sonrasında özel nitelikli verilerin işleme şartları, uluslararası veri akışları ve standart sözleşmelere ilişkin bildirim ile yaptırım hükümleri güncel kurallara göre yeniden değerlendirilmelidir. ISO/IEC 27001:2022 bu süreçte risk yönetimi, kayıt ve sürekli iyileştirme disiplini kazandırabilir, ancak tek başına hukuki uyumun kanıtı sayılamaz.

Çalışmanın sınırları, benimsenen kavramsal sentez yaklaşımından kaynaklanmaktadır. Değerlendirmeler ampirik işletme verilerine dayanmamakta ve önerilen uygulama adımları farklı sektörlerde doğrudan sınanmamaktadır. Sağlık, finans, eğitim ve elektronik ticaret gibi alanların veri türleri, düzenleyici yükümlülükleri ve risk düzeyleri farklı olduğundan öneriler bütün işletmelere aynı biçimde genellenemez. Sunulan çerçeve, kuruluşun ölçeği, sektörü, veri işleme amaçları ve risk profili dikkate alınarak uyarlanmalıdır.

Gelecek araştırmalarda Türkiye'deki işletmelerin KVKK uyum olgunluğu sektör ve ölçek temelinde ampirik olarak

karşılaştırılabilir. Yapay zekâ destekli çalışan izleme ve karar sistemlerinin hukuki ve örgütsel etkileri, sıfır güven mimarisinin KOBİ'lerde uygulanabilirliği ve 2024 sonrası yurt dışına aktarım mekanizmalarının kurumsal bilgi sistemlerine etkisi de araştırılmaya açıktır. Bu çalışmalar, teknik güvenlik ile veri koruma hukukunu aynı analitik çerçevede ele aldığı anda hem alan yazına hem de uygulamaya daha güçlü katkı sunacaktır.

KAYNAKÇA

- 6698 sayılı Kişisel Verilerin Korunması Kanunu. (2016, 7 Nisan). *Resmî Gazete* (Sayı: 29677).
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>
- Athier Olca, E., & Can, Ö. (2024). KVKK kavramlarının modellenmesi için ontoloji tabanlı bir yaklaşım. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi*, 26(76), 173–191. <https://doi.org/10.21205/deufmd.2024267620>
- Avrupa Parlamentosu ve Avrupa Birliği Konseyi. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. https://publications.europa.eu/resource/cellar/3e485e15-11bd-11e6-ba9a-01aa75ed71a1.0006.03/DOC_1 Erişim tarihi: 02.09.2026
- Bal, S., Canayaz, E., & Kabataş Soyer, Z. B. (2026). Taşınabilir tıbbi cihazların mühendislik tasarımında tasarıma dayalı gizlilik yaklaşımı: KVKK ve GDPR perspektifinde veri güvenliği. *Bilişim Teknolojileri Dergisi*, 19(2), 105–112. <https://doi.org/10.17671/gazibtd.1788711>
- Chang, Y. (2020). What drives organizations to switch to cloud ERP systems? The impacts of enablers and inhibitors. *Journal of Enterprise Information Management*, 33(3), 600–626. <https://doi.org/10.1108/JEIM-06-2019-0148>
- Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior

- perspective. *Sustainability*, 12(8), 3163.
<https://doi.org/10.3390/su12083163>
- D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474–489.
<https://doi.org/10.1108/IMCS-08-2013-0057>
- Abd Elmonem, M. A., Nasr, E. S., & Geith, M. H. (2016). Benefits and challenges of cloud ERP systems: A systematic literature review. *Future Computing and Informatics Journal*, 1(1–2), 1–9.
<https://doi.org/10.1016/j.fcij.2017.03.003>
- Henkoğlu, T., & Uçak, N. Ö. (2015). Üniversite kütüphanelerinde kişisel verilerin korunması. *Bilgi Dünyası*, 16(1), 45–74.
<https://doi.org/10.15612/BD.2015.472>
- ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. ISACA.
<https://www.isaca.org/store2/product/CB19FIM>
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, 25(12), 1595.
<https://doi.org/10.3390/e25121595>
- Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24. <https://doi.org/10.1007/s10207-025-01032-0>
- Kişisel Verileri Koruma Kurumu. (2018a). *Kişisel veri güvenliği rehberi (Teknik ve idari tedbirler)*. Erişim Tarihi: 30.08.2026.
https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

- Kişisel Verileri Koruma Kurumu. (2018b). *Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulacak veri sorumlularına ilişkin 2 Nisan 2018 tarihli ve 2018/32 sayılı karar*. Erişim Tarihi: 25.08.2026. <https://www.kvkk.gov.tr/Icerik/4233/2018-32>
- Kişisel Verileri Koruma Kurumu. (2019). Kişisel veri ihlali bildirim usul ve esaslarına ilişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı kararına ilişkin duyuru. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>
- Kişisel Verileri Koruma Kurumu. (2023). *Veri Sorumluları Siciline kayıt yükümlülüğüne ilişkin istisna kriterinde değişiklik yapılması hakkında 6 Temmuz 2023 tarihli ve 2023/1154 sayılı karar*. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/7647/2023-1154>
- Kişisel Verileri Koruma Kurumu. (2024a). *6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yapılan değişiklikler hakkında kamuoyu duyurusu*. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/7834/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununda-Yapilan-Degisiklikler-Hakkinda-Kamuoyu-Duyurusu>
- Kişisel Verileri Koruma Kurumu. (2024b). *Kişisel verilerin yurt dışına aktarılması rehberi*. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf>
- Kişisel Verileri Koruma Kurumu. (2024c). Standart Sözleşme Bildirim Modülü hakkında kamuoyu duyurusu. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/8043/Standart-Sozlesme-Bildirim-Modulu-Hakkinda-Kamuoyu-Duyurusu>

- Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44–60. <https://izlik.org/JA33DT56SH>
- Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. *Computer*, 54(2), 80–85. <https://doi.org/10.1109/MC.2020.3038411>
- Kumar, P., Wazid, M., Singh, D. P., Singh, J., Das, A. K., Park, Y., & Rodrigues, J. J. (2023). Explainable artificial intelligence envisioned security mechanism for cyber threat hunting. *Security and Privacy*, 6(6), e312. <https://doi.org/10.1002/spy2.312>
- Laudon, K. C., & Laudon, J. P. (2011). *Yönetim bilişim sistemleri* (U. Yozgat, Çev. Ed.). Nobel Akademik Yayıncılık.
- Nadkarni, S., & Prügl, R. (2021). Digital transformation: A review, synthesis and opportunities for future research. *Management Review Quarterly*, 71, 233–341. <https://doi.org/10.1007/s11301-020-00185-7>
- Negri-Ribalta, C., Lombard-Platet, M., & Salinesi, C. (2024). Understanding the GDPR from a requirements engineering perspective: A systematic mapping study on regulatory data protection requirements. *Requirements Engineering*, 29, 523–549. <https://doi.org/10.1007/s00766-024-00423-4>
- Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Journal of Accounting and Taxation Studies*, 208-232. <https://doi.org/10.29067/muvu.340848>.
- Ses, S. M., & Korkusuz, M. R. (2025). İş ilişkisinde kişisel verilerin yapay zekâ destekli sistemler yardımıyla işlenmesi. *Ankara Sosyal Bilimler Üniversitesi Hukuk*

Fakültesi Dergisi, 6(2), 1000–1050.
<https://doi.org/10.47136/asbuhfd.1566869>

- Turan Başara, G. (2024). Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde yapılan değişiklik bağlamında özel nitelikli kişisel verilerin işlenmesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 28(4), 51–80. <https://doi.org/10.34246/ahbvuhfd.1497257>
- Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, 23(2), 1459–1475. <https://doi.org/10.1007/s10207-023-00797-6>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Jensen, T. B. (2021). Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems*, 22(1), 102–129. <https://doi.org/10.17705/1jais.00655>
- Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security*, 133, 103412. <https://doi.org/10.1016/j.cose.2023.103412>
- Zaguir, N. A., Magalhães, G. H., & Spinola, M. M. (2024). Challenges and enablers for GDPR compliance: Systematic literature review and future research

directions. *IEEE Access*, 12, 81608–81630.
<https://doi.org/10.1109/ACCESS.2024.3406724>

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97.
<https://doi.org/10.1080/08874417.2020.1712269>