Yönetim Bilimleri Dergisi/Journal of Administrative Sciences
Cilt/Volume: 24, Sayı/No: 61, ss./pp.: 1267-1293
DOI: https://doi.org/10.35408/comuybd.1781595

-ARAŞTIRMA MAKALESİ-

İNSAN KAYNAKLARINDA VERİ KORUMA VE STRATEJİK YÖNETİM: KVKK-GDPR KARŞILAŞTIRMALI BİR YAKLAŞIM

Pınar SARP HÜSEYİN[1]

Öz

Bu çalışma, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) insan kaynakları yönetimi (İK) süreçleri üzerindeki etkilerini karşılaştırmalı bir perspektifle incelemektedir. Literatür incelemesi, GDPR'a ilişkin araştırmaların Avrupa merkezli ve yoğun olduğunu; buna karşılık Türkiye bağlamında KVKK'nın İK süreçlerindeki yansımalarının daha sınırlı ölçüde ele alındığını ortaya koymaktadır. Bu boşluğu gidermek amacıyla araştırma, iki temel soruya odaklanmaktadır: (1) İnsan kaynakları departmanları, çalışan verilerinin korunmasında hangi ilkelere ve uygulamalara dikkat etmelidir? (2) KVKK ve GDPR arasındaki farklılıklar, İK süreçlerini nasıl şekillendirmektedir? Çalışma, kuramsal temelini Kurumsal Teori ve Kaynaklara Dayalı Görüş (RBV) yaklaşımlarına dayandırmaktadır. Bulgular, her iki düzenlemenin hukuka uygunluk, şeffaflık ve veri minimizasyonu gibi ortak ilkeler getirdiğini; ancak düzenleme ve uygulama yöntemleri açısından bazı farklılıklar içerdiğini göstermektedir. GDPR, çalışan verilerinin korunmasına ilişkin daha ayrıntılı düzenlemeler sunarken, KVKK da benzer temel ilkeleri benimsemekte ve uygulamada Kurul kararları ile rehberler önemli bir yönlendirici rol üstlenmektedir. İK profesyonelleri açısından öne çıkan uygulama zorlukları; hukuki bilgi eksikliği, teknik altyapı yetersizlikleri ve kurumsal farkındalık sorunlarıdır. Çalışma, veri korumanın yalnızca yasal bir uyum süreci değil, aynı zamanda örgütsel güven, etik yönetişim ve stratejik kaynak yönetimi açısından kritik bir unsur olduğunu ortaya koymakta hem akademik literatüre katkı hem de uygulamaya yönelik politika önerileri sunmaktadır.

Anahtar Kelimeler: *GDPR, KVKK, İnsan Kaynakları Yönetimi*

JEL Kodları: *K31, K33.*

Başvuru: *10.09.2025* **Kabul:** *12.05.2026*

[1] Dr. Öğr. Üyesi, T.C. İstanbul Kültür Üniversitesi, İktisadi ve İdari Bilimler Fakültesi- İşletme Bölümü, p.sarp@iku.edu.tr, İstanbul, Türkiye, ORCID No: 0000-0003-3022-5182

DATA PROTECTION AND STRATEGIC MANAGEMENT IN HUMAN RESOURCES: A COMPARATIVE APPROACH TO KVKK AND GDPR [2]

Abstract

This study examines the effects of the Turkish Personal Data Protection Law (KVKK) and the European Union's General Data Protection Regulation (GDPR) on human resource management (HRM) processes from a comparative perspective. The literature review reveals that research on GDPR is extensive and largely Europe-centered, whereas the implications of KVKK for HR processes in the Turkish context have received more limited attention. To address this gap, the study focuses on two main questions: (1) Which principles and practices should HR departments consider in protecting employee data? (2) How do the differences between KVKK and GDPR shape HR processes? The study is theoretically grounded in Institutional Theory and the Resource-Based View (RBV). The findings indicate that both regulations introduce common principles such as lawfulness, transparency, and data minimization, although they differ in terms of regulatory and implementation approaches. While GDPR provides more detailed regulations regarding the protection of employee data, KVKK also adopts similar fundamental principles, with the decisions and guidelines of the Personal Data Protection Authority playing an important guiding role in practice. The main implementation challenges faced by HR professionals include lack of legal knowledge, deficiencies in technical infrastructure, and limited organizational awareness. The study demonstrates that data protection should be considered not only as a legal compliance process, but also as a critical issue in terms of organizational trust, ethical governance, and strategic resource management, thereby contributing both to the academic literature and to practical policy recommendations.

Keywords: *GDPR, KVKK, Human Resources Management*

JEL Codes: *K31, K33.*

"Bu çalışma Araştırma ve Yayın Etiğine uygun olarak hazırlanmıştır."

[2] The Extended English Summary is located the end of the Article

1. GİRİŞ

Dijitalleşme sürecinin hız kazanmasıyla birlikte insan kaynakları yönetimi kişisel verilerin en yoğun işlendiği departmanlardan biri haline gelmiştir. Bu doğrultuda işe alım, performans değerlendirme, kariyer planlama, bordrolama, eğitim ve işten ayrılma gibi süreçlerin tamamı; kimlik, iletişim, sağlık, biyometrik ve finansal nitelikteki bilgilerin işlenmesini içermektedir. İnsan kaynakları departmanlarında işlenen verilerin çeşitliliği ve hassasiyeti, kişisel verilerin korunmasını yalnızca teknik değil, aynı zamanda etik ve hukuki bir sorumluluk haline getirmektedir (Toros, 2025).

Tataru ve Tataru'ya (2020) göre kişisel verilerin korunması, çalışanların mahremiyet hakkı ile işverenin denetim ve verimlilik beklentileri arasında dengeli bir yaklaşım kurulmasını gerektirmektedir. İnsan kaynakları süreçlerinde adayların sosyal medya hesaplarının incelenmesi, performans değerlendirme araçlarının kullanılması veya sağlık verilerinin işlenmesi gibi uygulamalar, çalışanların özel yaşamını doğrudan etkileyebilmektedir. Bu nedenle veri koruması, yalnızca çalışanların kişisel haklarının korunması açısından önemli değildir. Aynı zamanda işveren–çalışan ilişkilerinde güvenin güçlenmesine, çalışan memnuniyetinin artmasına ve etik sorumlulukların yerine getirilmesine de katkı sağlamaktadır.

KVKK, Türkiye'de kişisel verileri işleyen tüm gerçek ve tüzel kişileri kapsamaktadır; bu kapsamda Türkiye'de yerleşik veri sorumluları ile Türkiye'de veri işleyen yabancı şirketler de düzenleme kapsamındadır (KVKK, 2016, m. 2). Her iki düzenleme de şeffaflık, veri minimizasyonu, amaçla sınırlılık ve saklama süresi gibi temel veri koruma ilkelerini paylaşmakla birlikte kapsam ve uygulama açısından çeşitli farklılıklar barındırmaktadır. GDPR, unutulma hakkı (GDPR, 2016, art. 17), hesap verebilirlik ilkesi ve algoritmik karar verme süreçlerine ilişkin daha ayrıntılı düzenlemeleriyle daha kapsamlı bir veri koruma çerçevesi sunmaktadır (Article 29 Data Protection Working Party, 2017). KVKK'da ise bu hak ve ilkeler GDPR'daki kadar ayrıntılı biçimde düzenlenmemiştir. Bununla birlikte Kişisel Verileri Koruma Kurulu'nun 23.06.2020 tarihli ve 2020/481 sayılı kararıyla unutulma hakkı uygulamada kabul edilmiş ve özellikle arama motorları üzerinden yapılan aramalarda kişilerin isimlerinin indeksten çıkarılması talepleri bu kapsamda değerlendirilmiştir. Dolayısıyla KVKK, temel veri koruma ilkelerini benimsemekle birlikte uygulamada daha genel bir çerçeve sunmakta; bu durum bazı konularda farklı yorum ve uygulamaların ortaya çıkmasına neden olabilmektedir.

Literatürde GDPR üzerine yapılan çalışmaların büyük ölçüde Avrupa merkezli olduğu görülürken, KVKK'nın insan kaynakları süreçlerine etkisini Türkiye bağlamında ele alan araştırmaların daha sınırlı kaldığı dikkat çekmektedir. Mevcut çalışmaların çoğu KVKK'yı daha çok hukuki veya teknik güvenlik perspektifinden değerlendirmekte, ancak çalışan verilerinin korunmasının örgütsel ve etik boyutlarını göz ardı etmektedir. Bu nedenle, bu çalışma KVKK ve GDPR'ın insan kaynakları yönetimine etkilerini kavramsal bir çerçevede karşılaştırmalı olarak ele alarak literatürdeki bu boşluğa katkı sunmayı amaçlamaktadır.

Bu noktada çalışmanın önemi iki düzeyde ortaya çıkmaktadır. İlk olarak, KVKK ve GDPR'ın karşılaştırmalı olarak ele alınması, Türkiye'de İK uygulamalarının uluslararası standartlarla ne ölçüde örtüştüğünü anlamaya imkân vermektedir. İkinci olarak, veri koruma yalnızca hukuki uyum meselesinin ötesinde kurumsal güven, etik yönetişim ve stratejik kaynak yönetimi bağlamında da literatüre katkı sağlamaktadır. Buradan hareketle çalışma, analizini iki kuramsal yaklaşıma dayandırmaktadır: Kurumsal Teori, veri koruma uygulamalarını dışsal baskılar ve meşruiyet arayışı perspektifinden açıklarken; Kaynaklara Dayalı Görüş, bu uygulamaları örgütsel güven ve rekabet avantajı yaratan stratejik bir kaynak olarak konumlandırmaktadır. Bu bilgilerden hareketle araştırma soruları kurgulanmıştır:

RQ1: İnsan kaynakları departmanları, çalışan verilerinin korunmasında hangi temel ilkelere ve uygulamalara dikkat etmelidir?

RQ2: KVKK ve GDPR arasındaki farklılıklar, insan kaynakları süreçlerini nasıl şekillendirmektedir?

Bu iki araştırma sorusu, çalışmanın hem kuramsal hem de uygulamaya dönük katkılarını şekillendirmektedir. İlk soru, İnsan Kaynakları departmanlarının veri korumadaki temel sorumluluklarını ortaya koyarak KVKK ve GDPR'ın ortak yönlerini aydınlatmayı hedeflerken; ikinci soru, iki düzenleme arasındaki farklılıkların İK süreçlerine nasıl yansıdığını inceleyerek karşılaştırmalı bir perspektif sunmaktadır. Bu yaklaşım hem literatürdeki boşluğu doldurmakta hem de İK profesyonelleri için uygulanabilir çıkarımlar üretmektedir. Araştırma, veri korumanın yalnızca yasal bir uyum meselesi değil, aynı zamanda meşruiyet, örgütsel güven ve rekabet avantajı bağlamında stratejik bir unsur olduğunu göstermeyi amaçlamaktadır.

1.1. Kişisel Verilerin Korunması: KVKK ve GDPR Çerçevesinde Temel İlkeler

Kişisel veri; "kimliği belirli ya da belirlenmesi mümkün gerçek kişilere ait her türlü bilgi" olarak tanımlanmaktadır (Kişisel Verilerin Korunması Kanunu [KVKK], 2016). Kişisel verilerin korunması, modern hukuk sistemlerinde bireyin özel hayatın gizliliği hakkının ayrılmaz bir parçasıdır. Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi bireyin özel yaşamına saygı hakkını güvence altına alırken, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'de 6698 sayılı KVKK, bu hakkı somutlaştıran en kapsamlı yasal düzenlemeler olarak öne çıkmaktadır (EU, 2016; KVKK, 2016). Her iki düzenleme de veri işleme süreçlerinde bir dizi temel ilke belirlemiş olup, bu ilkeler insan kaynakları uygulamaları açısından da yol gösterici niteliktedir.

1.1.1. Hukuka Uygunluk ve Dürüstlük

KVKK'nın 4. maddesi ve GDPR'ın 5(1)(a) maddesi, kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesini zorunlu kılar. Bu ilke, İK uygulamalarında çalışan verilerinin yalnızca yasal dayanaklar çerçevesinde ve dürüstlük ilkesine uygun şekilde toplanmasını ifade eder (KVKK, 2016, m. 4; GDPR, 2016, art. 5(1)(a)).

1.1.2. Şeffaflık

GDPR'da şeffaflık doğrudan temel bir ilke olarak düzenlenirken, KVKK'da bu yaklaşım daha çok "aydınlatma yükümlülüğü" üzerinden uygulanmaktadır. Çalışanların, hangi verilerinin hangi amaçlarla işlendiği, ne kadar süreyle saklanacağı ve üçüncü kişilerle paylaşılıp paylaşılmayacağı konusunda bilgilendirilmesi gerekmektedir. Şeffaflık ilkesi, işveren–çalışan ilişkisinde güvenin kurulması açısından kritik bir rol üstlenmektedir. (KVKK, 2016; GDPR, 2016).

1.1.3. Doğruluk ve Güncellik

KVKK'nın 4/2-b hükmü ve GDPR'ın 5(1)(d) maddesi, verilerin doğru ve güncel tutulması gereğini vurgular. İK bağlamında, örneğin çalışanın adres veya medeni durumu gibi bilgilerin güncellenmemesi hem idari işlemlerde hem de sosyal haklarda hak kayıplarına neden olabilmektedir (KVKK, 2016, m. 4/2-b; GDPR, 2016, art. 5(1)(d)).

1.1.4. Amaçla Sınırlılık

KVKK'nın 4/2-ç hükmü ve GDPR'ın 5(1)(b) maddesi, kişisel verilerin yalnızca belirlenen ve meşru amaçlarla işlenmesi gereğini düzenlemektedir (KVKK, 2016, m. 4/2-ç; GDPR, 2016, art. 5(1)(b)). İK bağlamında, örneğin işe alım sürecinde toplanan verilerin ilerleyen dönemlerde performans değerlendirmesi amacıyla kullanılması, amaç dışına çıkılması nedeniyle hukuki sorumluluk doğurabilmektedir.

1.1.5. Veri Minimizasyonu

GDPR'ın 5(1)(c) maddesinde yer alan veri minimizasyonu ilkesi, işlenen verilerin "amacın gerektirdiği kadar" olması gerektiğini belirtir. KVKK'da da "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" şartı düzenlenmiştir (KVKK, 2016, m. 4/2-d). İK süreçlerinde bu ilke, işe alımda yalnızca işin niteliğiyle doğrudan ilgili bilgilerin talep edilmesini gerektirir (GDPR, 2016, art. 5(1)(c)).

1.1.6. Saklama Süresi

GDPR'ın 5(1)(e) maddesi ve KVKK'nın 4/2-e hükmü, kişisel verilerin yalnızca gerekli süre boyunca saklanmasını öngörür. Bu bağlamda işten ayrılan bir çalışanın özlük dosyaları yalnızca yasal sürede tutulmalı, süre sonunda imha veya anonimleştirme yoluna gidilmelidir (GDPR, 2016, art. 5(1)(e); KVKK, 2016, m. 4/2-e).

1.1.7. Gizlilik ve Güvenlik

KVKK'nın 12. maddesi ile GDPR'ın 5(1)(f) ve 32. maddeleri, veri sorumlularına kişisel verilerin gizliliğini ve güvenliğini sağlama yükümlülüğü getirmektedir (KVKK, 2016, m. 12; GDPR, 2016, art. 5(1)(f), art. 3). Bu yükümlülük, hem teknik tedbirlerin (şifreleme, erişim kısıtlamaları) hem de idari tedbirlerin (yetkilendirme, politika geliştirme) uygulanmasını zorunlu kılar.

1.1.8. Hesap Verebilirlik

GDPR'ın 5(2). maddesi, veri sorumlusuna yalnızca veri işleme ilkelerine uymakla kalmayıp, aynı zamanda bu uyumu kanıtlayabilme yükümlülüğü de getirmektedir. Bu düzenleme, "hesap verebilirlik" ilkesinin açık ve sistematik bir şekilde tanımlanmasını sağlar. KVKK'da ise hesap verebilirlik ilkesi GDPR'daki gibi doğrudan ve açık bir hüküm olarak yer almamaktadır. Bununla birlikte KVKK'nın 12. maddesinde veri sorumlusuna getirilen güvenlik yükümlülükleri ve Kişisel Verileri Koruma Kurulu'nun denetim yetkileri, dolaylı olarak hesap verebilirlik mantığını içermektedir. Dolayısıyla KVKK ve GDPR büyük ölçüde benzer temel ilkeler üzerine inşa edilmiş olsa da, GDPR şeffaflık ve hesap verebilirlik ilkelerini daha ayrıntılı ve denetim odaklı bir çerçevede düzenlemektedir. Bu yönüyle GDPR, veri sorumlularına yalnızca uyum sağlama değil, aynı zamanda bu uyumu gösterebilme yükümlülüğü de getirerek daha güçlü bir denetim mekanizması sunmaktadır.

Kuner ve arkadaşları (2020), Martin, Borah ve Palmatier (2017) ile Bondarouk ve Brewster'a (2016) göre veri koruma ilkelerinin etkili şekilde uygulanması, hem uyum risklerinin hem de örgütsel maliyetlerin azaltılmasına katkı sağlamaktadır. Gereksiz veri toplanmaması ve verilerin belirli sürelerle saklanması, depolama ve denetim maliyetlerini sınırlandırırken; doğru ve güncel verilerle yürütülen bordro, performans ve eğitim süreçleri operasyonel verimliliği desteklemektedir. Ayrıca çalışan verilerinin etik ve ölçülü biçimde kullanılması, örgüt içinde güvenin güçlenmesine ve olası uyuşmazlıkların azalmasına katkı sunmaktadır. Bunun yanında veri işleme süreçlerinin kurumsal prosedürlerle desteklenmesi, işveren markası ve kurumsal itibar açısından da önemli bir avantaj sağlamaktadır.

1.2. İnsan Kaynaklarında Veri Yönetimi

Kişisel verilerin işlenmesi, dijitalleşmenin etkisiyle çalışma hayatında giderek daha yaygın hale gelmiştir. İşverenler; işe alım, performans değerlendirme, eğitim, kariyer planlama, iş sağlığı ve güvenliği ile işyeri güvenliğinin sağlanması gibi çeşitli amaçlarla çalışanlara ve iş başvurusunda bulunan adaylara ait kişisel verilere ihtiyaç duymaktadır. Bu süreçlerde çalışanların kimlik bilgileri, iletişim bilgileri, sağlık verileri, e-posta yazışmaları, sendikal faaliyetleri ve hatta bazı durumlarda biyometrik verileri gibi çok sayıda bilgi işlenebilmekte ve belirli koşullar altında üçüncü kişilerle paylaşılabilmektedir. Bu nedenle çalışanlara ait kişisel veriler, korunması gereken en hassas veri alanlarından biri olarak değerlendirilmektedir (Manav, 2025).

Çalışma hayatında kişisel veri kullanımının bu kadar yaygın hale gelmesi, insan kaynakları süreçlerinde veri koruma ve çalışan mahremiyeti tartışmalarını daha önemli hale getirmiştir. Geden ve Bensghir (2018) ile Ogriseg'e (2017) göre çalışan verilerinin farklı türlerde işlenmesi, insan kaynaklarını kişisel verilerin korunması açısından en hassas alanlardan biri haline getirmektedir. Bu nedenle, işverenin denetim ihtiyacı ile çalışanın mahremiyet hakkı arasında dengeli bir yaklaşım kurulması önem taşımaktadır. KVKK ve GDPR'da yer alan temel ilkelerin İK

süreçlerine doğru şekilde yansıtılması hem hukuki uyumun sağlanması hem de çalışan güveninin korunması açısından önemli görülmektedir.

1.2.1. İşe Alım

Şirketlerin kişisel veri işleme faaliyetleri yalnızca mevcut çalışanlarla sınırlı değildir. İşe alım sürecinde gerçekleştirilen iş görüşmeleri sırasında da insan kaynakları departmanı, çeşitli yöntemler aracılığıyla işçi adaylarına ait kişisel verilere erişmekte ve bu verileri değerlendirmektedir. Özellikle özgeçmişler, referans araştırmaları, mülakat notları ve dijital başvuru sistemleri aracılığıyla adaylara ilişkin çok sayıda veri toplanabilmektedir. Ancak bu aşamada taraflar arasında henüz resmi bir iş sözleşmesi kurulmadığı için, işverenin işçiyi koruma yükümlülüğünün kapsamı ve adaylara ait kişisel verilerin hangi sınırlar içinde işlenebileceği önemli bir tartışma konusu haline gelmektedir (Kaya, 2022). Bu durum, işe alım süreçlerini kişisel verilerin korunması açısından önemli alanlardan biri haline getirmektedir (Gatewood, Feild ve Barrick, 2010).

1.2.2. Özlük Dosyası ve Çalışma Süreci Verileri

İnsan kaynakları yönetiminde özlük dosyaları ve çalışma süreci boyunca oluşan kayıtlar, çalışanla ilgili birçok kişisel verinin işlenmesini içermektedir. Bu kapsamda kimlik bilgileri, iş sözleşmeleri, eğitim belgeleri, sağlık raporları, bordro kayıtları, performans değerlendirmeleri, izin bilgileri ve eğitim kayıtları gibi farklı veriler insan kaynakları süreçlerinde kullanılabilmektedir. Söz konusu kayıtlar, hem çalışanla ilgili süreçlerin düzenli şekilde yürütülmesine hem de işverenin yasal yükümlülüklerini yerine getirdiğinin gösterilmesine katkı sağlamaktadır (Çelik vd., 2020; Dessler, 2020).

1.2.3. Özel Nitelikli Veriler

KVKK'nın 6. maddesi ile GDPR'ın 9. maddesi, bazı kişisel veri türlerini "özel nitelikli veri" olarak değerlendirmektedir. Sağlık bilgileri, biyometrik veriler, sendika üyeliği, dini inançlar veya kişinin geçmiş sağlık durumuna ilişkin bilgiler bu kapsamda yer alabilmektedir. Bu tür veriler, bireyin özel yaşamı ve temel hakları açısından daha hassas kabul edildiği için, işlenmeleri daha sıkı kurallara bağlanmıştır. Bu nedenle özel nitelikli verilerin işlenmesi çoğunlukla açık rıza veya belirli hukuki istisnalar kapsamında mümkün olmakta; ayrıca bu verilerin korunması için daha güçlü teknik ve idari önlemler alınması gerekmektedir (Özdemir, 2009).

1.2.4. İşten Ayrılma ve Veri Saklama Süreci

İşten ayrılma süreci, yalnızca iş sözleşmesinin sona ermesiyle sınırlı kalmamakta, aynı zamanda çalışana ait bazı kayıtların belirli sürelerle saklanmasını da kapsamaktadır. Bu süreçte özlük dosyaları, bordro kayıtları, izin bilgileri ve sosyal güvenlik belgeleri gibi veriler, işveren tarafından yasal yükümlülüklerin yerine getirilmesi ve olası hukuki durumlarda gerekli belgelerin sunulabilmesi amacıyla muhafaza edilmektedir. Bunun yanında, işten ayrılan çalışanlara ilişkin kayıtlar insan kaynakları yönetimi açısından da önem taşımaktadır. Kurumlar bu verilerden yararlanarak çalışan devir oranı, performans süreçleri ve çalışan bağlılığı gibi

konularda değerlendirmeler yapabilmekte ve gelecekteki insan kaynakları uygulamalarını şekillendirebilmektedir (Mathis vd., 2016).

1.3. Kuramsal Çerçeve

Bu çalışmanın teorik temeli, veri koruma düzenlemelerinin insan kaynakları yönetiminde yarattığı değişimi açıklamak amacıyla Kurumsal Teori ve Kaynaklara Dayalı Görüş üzerine kurulmaktadır. Meyer ve Rowan (1977) ile DiMaggio ve Powell'a (1983) göre örgütler yalnızca ekonomik nedenlerle değil, aynı zamanda toplumsal beklentilere ve yasal düzenlemelere uyum sağlamak amacıyla da hareket etmektedir. Bu açıdan bakıldığında GDPR ve KVKK'ya uyum, işletmeler için sadece yasal bir zorunluluk değil; aynı zamanda çalışanlar, müşteriler ve diğer paydaşlar nezdinde güven ve kurumsal itibar oluşturmanın önemli bir parçasıdır (Scott, 2014; Greenwood vd., 2017). Özellikle uluslararası faaliyet gösteren şirketler için veri koruma uygulamaları, kurumsal meşruiyetin önemli unsurlarından biri haline gelmiştir.

Kaynaklara Dayalı Görüş ise işletmelerin rekabet avantajını sahip oldukları stratejik kaynaklarla açıkladığını savunmaktadır (Barney, 1991). Bu çerçevede çalışan verilerinin güvenli şekilde yönetilmesi, kurumlar açısından önemli bir yetkinlik olarak değerlendirilebilir. Veri güvenliği konusunda oluşturulan kurumsal yapı ve güven kültürü, çalışan bağlılığını ve işveren markasını güçlendirebilmektedir.
Kurumsal Teori veri koruma uygulamalarını daha çok dışsal baskılar ve yasal uyum üzerinden açıklarken, Kaynaklara Dayalı Görüş bu sürecin işletmelere sağlayabileceği stratejik avantajlara odaklanmaktadır. Bu nedenle GDPR ve KVKK'nın insan kaynakları süreçlerine etkisi, hem yasal uyum hem de rekabet avantajı açısından birlikte değerlendirilebilmektedir.

1.3.1. Kişisel Verilerin Korunması ve İK Yönetimine İlişkin Çalışmalar

Kişisel verilerin korunması ve insan kaynakları yönetimi ilişkisi son yıllarda literatürde giderek daha fazla ele alınan konular arasında yer almaktadır. Özellikle dijitalleşme, uzaktan çalışma sistemleri ve elektronik insan kaynakları uygulamalarının yaygınlaşmasıyla birlikte çalışan verilerinin işlenmesi, saklanması ve korunmasına yönelik tartışmalar daha görünür hale gelmiştir. Bu kapsamda yapılan çalışmalar, veri koruma düzenlemelerinin insan kaynakları süreçleri üzerindeki etkilerini farklı boyutlarıyla incelemektedir.

Toros'un (2025) çalışması, KVKK'nın insan kaynakları departmanları üzerindeki etkilerini nitel araştırma yöntemiyle incelemektedir. Çalışmada, kişisel verilerin korunmasına yönelik düzenlemelerin insan kaynakları süreçlerini daha sistematik ve güvenlik odaklı hale getirdiği ortaya konulmuştur. Bulgular, insan kaynakları departmanlarının yalnızca işe alım ve özlük işlemleriyle sınırlı kalmadığını; çalışan verilerinin işlenmesi, saklanması, imhası ve veri güvenliği süreçlerinde de merkezi bir rol üstlendiğini göstermektedir. Ayrıca KVKK ile birlikte insan kaynakları, hukuk, bilgi işlem ve kalite yönetimi gibi departmanlar arasındaki iş birliğinin arttığı; veri güvenliği, açık rıza, veri saklama süreleri ve çalışan farkındalığı konularının örgütler açısından daha önemli hale geldiği belirtilmektedir. Çalışma sonucunda KVKK'nın

yalnızca hukuki bir uyum süreci değil, aynı zamanda insan kaynakları departmanlarını stratejik bir konuma taşıyan bir dönüşüm yarattığı ifade edilmektedir (Toros, 2025). Tataru ve Tataru'nun (2020) çalışması, insan kaynakları faaliyetleri ile kişisel verilerin korunması arasındaki güçlü ilişkiyi GDPR çerçevesinde incelemektedir. Çalışmada insan kaynakları departmanlarının işe alım sürecinden iş sözleşmesinin sona ermesine kadar çalışanlara ait çok sayıda kişisel veriyi işlediği vurgulanmaktadır. Özellikle özgeçmişler, sağlık bilgileri, bordro kayıtları, performans verileri, kamera kayıtları ve dijital davranış verileri gibi hassas bilgilerin insan kaynakları süreçlerinde yoğun biçimde kullanıldığı belirtilmektedir. Araştırma, GDPR ile birlikte işletmelerin çalışan verilerini daha dikkatli yönetmek zorunda kaldığını; veri işleme süreçlerinde şeffaflık, veri minimizasyonu, güvenlik ve hukuki uygunluk ilkelerinin daha önemli hale geldiğini ortaya koymaktadır. Ayrıca çalışmada işe alım, iş ilişkisinin devamı ve işten ayrılma sonrası süreçler ayrı aşamalar halinde değerlendirilmiş; çalışanların veri sahibi olarak sahip olduğu erişim, düzeltme, silme ve itiraz haklarına da dikkat çekilmiştir. Çalışma, kişisel verilerin korunmasının insan kaynakları yönetiminin ayrılmaz bir parçası haline geldiğini ve GDPR'ın insan kaynakları uygulamalarında önemli bir dönüşüm yarattığını ifade etmektedir (Tataru ve Tataru, 2020).

Jabrayilova'nın (2015) çalışması, insan kaynakları yönetim sistemlerinde çalışanlara ait kişisel verilerin korunması ve güvenliği konusunu ele almaktadır. Çalışmada dijital insan kaynakları sistemlerinin işe alım, bordro, performans değerlendirme, eğitim, terfi ve çalışan takibi gibi birçok süreci desteklediği; bu nedenle çalışanlara ait büyük miktarda kişisel verinin işlendiği belirtilmektedir. Araştırma, sağlık bilgileri, performans kayıtları, psikolojik test sonuçları, kimlik bilgileri ve çalışan davranışlarına ilişkin verilerin insan kaynakları sistemlerinde saklanmasının veri güvenliği ve mahremiyet risklerini artırdığına dikkat çekmektedir. Bu kapsamda ISO 27002 gibi uluslararası bilgi güvenliği standartlarının önemi vurgulanmakta; veri güvenliğinin yalnızca teknik önlemlerle değil, aynı zamanda kurumsal politikalar, denetim süreçleri ve hukuki düzenlemelerle desteklenmesi gerektiği ifade edilmektedir. Çalışma ayrıca çalışan verilerinin korunmasının örgütsel güven, çalışan hakları ve sürdürülebilirlik açısından önemli olduğunu ortaya koymaktadır.

Zhang ve arkadaşlarının (2025) çalışması, dijital çağda insan kaynakları yönetiminde veri güvenliği ve mahremiyet korumasının önemini incelemektedir. Araştırmada büyük veri, yapay zekâ ve bulut teknolojileri gibi dijital uygulamaların insan kaynakları süreçlerini dönüştürdüğü; ancak bu dönüşümün veri güvenliği ve gizlilik açısından yeni riskler ortaya çıkardığı vurgulanmaktadır. Çalışma, özellikle veri sızıntıları, zayıf erişim kontrolleri, yetersiz veri güvenliği politikaları ve çalışanların düşük veri güvenliği farkındalığı gibi sorunların işletmeler açısından önemli tehditler oluşturduğunu belirtmektedir. Bunun yanında GDPR ve Çin'deki veri koruma düzenlemeleri gibi hukuki çerçevelerin örgütler üzerinde daha güçlü uyum baskısı oluşturduğu ifade edilmektedir. Araştırma ayrıca veri sınıflandırması, risk analizi, çalışan eğitimleri, veri yedekleme sistemleri ve gizlilik artırıcı teknolojilerin kullanımının insan kaynakları süreçlerinde veri güvenliğini güçlendirebileceğini savunmaktadır. Sonuç olarak çalışma, veri güvenliği ve mahremiyet korumasının yalnızca teknik bir konu olmadığını; örgütsel itibar, çalışan güveni, yasal uyum ve

sürdürülebilir rekabet avantajı açısından da stratejik bir öneme sahip olduğunu ortaya koymaktadır.

Vargas, Budz ve Onete'nin (2021) çalışması, GDPR'ın insan kaynakları faaliyetleri üzerindeki etkisini incelemektedir. Araştırmada GDPR ile birlikte insan kaynakları departmanlarının çalışan ve aday verilerini işleme süreçlerinde daha şeffaf, kontrollü ve hesap verebilir bir yapıya yöneldiği belirtilmektedir. Çalışma, işe alım süreçlerinden çalışan performans kayıtlarına, sağlık verilerinden dijital iletişim kayıtlarına kadar çok geniş bir veri alanının insan kaynakları tarafından işlendiğini ortaya koymaktadır. Ayrıca çalışanların verilerinin hangi amaçla toplandığı, ne kadar süre saklandığı ve kimlerle paylaşılabileceği konusunda bilgilendirilmesinin GDPR'ın temel gerekliliklerinden biri olduğu vurgulanmaktadır. Araştırma, özellikle çalışan rızası, veri minimizasyonu, veri paylaşımı, çalışan izleme sistemleri ve siber güvenlik önlemleri gibi konuların insan kaynakları yönetiminde daha önemli hale geldiğini göstermektedir. Bunun yanısıra şirketlerin veri ihlali durumlarında hızlı bildirim yükümlülüğü altında olduğu ve insan kaynakları departmanlarının çalışanlarla veri işleme süreçleri konusunda sürekli iletişim içinde olması gerektiği ifade edilmektedir. Ayrıca çalışma, GDPR'ın insan kaynakları uygulamalarını yalnızca hukuki açıdan değil, aynı zamanda organizasyonel politika, çalışan güveni ve veri yönetimi kültürü açısından da önemli ölçüde dönüştürdüğünü ortaya koymaktadır.

İnciroğlu ve Öge'nin (2019) çalışması, işletmelerde kişisel verilerin korunması sürecinde insan kaynakları ve bilgi işlem departmanlarının rolünü incelemektedir. Çalışmada, insan kaynakları departmanlarının işe alım sürecinden iş sözleşmesinin sona ermesine kadar çalışanlara ait çok sayıda kişisel veriyi işlediği; bilgi işlem departmanlarının ise bu verilerin elektronik ortamda güvenli şekilde saklanması, yedeklenmesi ve dış tehditlere karşı korunmasından sorumlu olduğu belirtilmektedir. Araştırma, çalışanlara ait kimlik, iletişim, sağlık, biyometrik, finansal ve performans verilerinin işletmeler açısından yüksek hassasiyet taşıdığını vurgulamaktadır. Ayrıca işe alım süreçlerinde gereğinden fazla veri toplanmaması, açık rıza alınması, veri saklama sürelerinin belirlenmesi ve süresi dolan verilerin silinmesi gibi uygulamaların önemine dikkat çekilmektedir. Çalışmada bunun yanında çalışan izleme sistemleri, kamera uygulamaları, biyometrik giriş sistemleri ve dijital takip süreçlerinin çalışan mahremiyeti açısından dikkatli yönetilmesi gerektiği ifade edilmektedir. Araştırma, kişisel verilerin korunmasının yalnızca teknik bir güvenlik konusu olmadığını; insan kaynakları, bilgi işlem ve yönetim süreçlerinin birlikte hareket etmesini gerektiren kurumsal bir sorumluluk alanı olduğunu ortaya koymaktadır.

Tikkinen-Piri, Rohunen ve Markkula'nın (2018) çalışması, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) kişisel veri toplayan işletmeler açısından ortaya çıkardığı değişimleri ve uygulama sonuçlarını incelemektedir. Araştırmada GDPR'ın yalnızca hukuki bir düzenleme olmadığı; aynı zamanda işletmelerin veri yönetimi, organizasyon yapıları, insan kaynakları süreçleri ve teknolojik altyapıları üzerinde dönüştürücü etkiler yarattığı vurgulanmaktadır. Çalışmada GDPR ile birlikte işletmelere şeffaflık, hesap verebilirlik, veri minimizasyonu ile "tasarımdan itibaren

gizlilik" ve "varsayılan olarak gizlilik" ilkelerine uygun hareket etme yükümlülüğü getirildiği vurgulanmaktadır. Özellikle çalışan ve müşteri verilerini yoğun şekilde işleyen şirketlerin veri toplama süreçlerini yeniden yapılandırmaları, açık rıza mekanizmalarını güçlendirmeleri, veri saklama sürelerini belirlemeleri ve veri ihlallerini belirli süre içinde bildirmeleri gerekmektedir. Ayrıca düzenleme kapsamında veri koruma görevlisi (DPO) atanması, veri işleme faaliyetlerinin kayıt altına alınması, çalışan eğitimlerinin artırılması ve organizasyonel farkındalığın geliştirilmesi önemli yükümlülükler arasında gösterilmektedir. Çalışmada GDPR'ın şirketler açısından yalnızca yasal uyum sağlamaya yönelik bir zorunluluk olmadığı; aynı zamanda kurumsal güven, itibar yönetimi ve rekabet avantajı açısından stratejik bir unsur haline geldiği ifade edilmektedir. Bunun yanında veri ihlallerine ilişkin yüksek para cezaları ve yaptırımların işletmeleri daha proaktif veri koruma politikaları geliştirmeye yönlendirdiği belirtilmektedir. Sonuç olarak araştırma, GDPR'ın şirketlerin kişisel veri işleme süreçlerini teknik, yönetsel ve kültürel boyutlarda yeniden şekillendiren kapsamlı bir dönüşüm yarattığını ortaya koymaktadır.
Literatür, kişisel verilerin korunmasının insan kaynakları yönetiminin ayrılmaz bir parçası haline geldiğini göstermektedir. Özellikle GDPR ve KVKK gibi düzenlemelerle birlikte insan kaynakları departmanlarının veri güvenliği, şeffaflık, veri minimizasyonu ve çalışan mahremiyeti konularındaki sorumluluklarının arttığı görülmektedir. Bunun yanında çalışmalar, veri koruma uygulamalarının yalnızca hukuki uyum açısından değil; çalışan güveni, kurumsal itibar ve sürdürülebilir insan kaynakları yönetimi açısından da önemli sonuçlar doğurduğunu ortaya koymaktadır.

2. YÖNTEM

Bu çalışma, kavramsal ve karşılaştırmalı bir araştırma tasarımıyla yürütülmüştür. Yöntemsel olarak öncelikle ulusal (KVKK) ve uluslararası (GDPR) veri koruma düzenlemeleri ayrıntılı biçimde incelenmiş; ardından insan kaynakları yönetimine yansımaları literatür taraması yoluyla değerlendirilmiştir. Literatür taramasında, konuya ilişkin akademik yayınlar, raporlar ve düzenleyici belgelerden yararlanılmıştır. Çalışmada ayrıca, veri koruma ilkeleri (hukuka uygunluk, şeffaflık, amaçla sınırlılık, veri minimizasyonu, güvenlik vb.) karşılaştırmalı olarak ele alınmıştır.

2.1. KVKK ve GDPR'IN İK Bağlamında Karşılaştırmalı Değerlendirmesi

2.1.1. İşe Alım

İşe alım süreci, adaylara ait kişisel verilerin yoğun biçimde işlendiği insan kaynakları faaliyetlerinden biridir. Özgeçmişler, iletişim bilgileri, eğitim geçmişi ve mesleki deneyimlere ilişkin bilgiler, adayın pozisyona uygunluğunu değerlendirmek amacıyla kullanılmaktadır. Bu nedenle işe alım süreçleri hem KVKK hem de GDPR kapsamında kişisel veri işleme faaliyeti olarak değerlendirilmektedir (KVKK, 2016; GDPR, 2016).

Dijital işe alım süreçlerinin yaygınlaşmasıyla birlikte adayların sosyal medya hesaplarının incelenmesi, çevrim içi kişilik testleri ve video mülakat uygulamaları veri

koruma tartışmalarını artırmıştır. Özellikle adaylara ilişkin verilerin hangi kapsamda değerlendirileceği ve ne kadar süreyle saklanacağı konusu uygulamada her zaman net biçimde belirlenememektedir. Uncular'a (2012) göre iş ilişkisinde üçüncü kişilerden bilgi edinilmesi, psikolojik testlerin uygulanması ve aday hakkında veri toplanması süreçleri kişisel verilerin korunması bakımından dikkatle değerlendirilmesi gereken uygulamalar arasında yer almaktadır.

İşe alım sürecinde oluşturulan özgeçmiş havuzlarının korunması da veri güvenliği açısından önem taşımaktadır. Hem KVKK hem de GDPR, işverenlere aday verilerinin korunması için gerekli teknik ve idari tedbirleri alma yükümlülüğü getirmektedir. Bu kapsamda erişim yetkilerinin sınırlandırılması, şifreleme yöntemlerinin kullanılması ve gereksiz verilerin belirli süre sonunda silinmesi gibi uygulamalar ön plana çıkmaktadır (KVKK, 2016, m. 12; GDPR, 2016, art. 32).

Referans kontrolü süreçlerinde adayın bilgisi dışında üçüncü kişilerle iletişime geçilmesi, kişisel verilerin işlenmesi açısından çeşitli hukuki ve etik tartışmaları beraberinde getirebilmektedir. Bu nedenle insan kaynakları birimlerinin referans araştırmalarını adayın bilgisi dahilinde, veri koruma ilkeleri ve hukuka uygun veri işleme şartları çerçevesinde yürütmesi önem taşımaktadır (KVKK, 2016, m. 5; GDPR, 2016, art. 6).

2.1.2. Performans Yönetimi ve Gözetim

Dijital teknolojilerin çalışma hayatında yaygınlaşmasıyla birlikte performans yönetimi ve işyeri gözetimi süreçlerinde çalışanlara ait kişisel verilerin işlenmesi önemli ölçüde artmıştır. Sistem giriş–çıkış kayıtları, üretkenlik analizleri, kamera görüntüleri ve biyometrik veriler gibi birçok veri türü performans değerlendirme ve denetim süreçlerinde kullanılabilmektedir. Bu durum, çalışan mahremiyeti ile işverenin denetim ihtiyacı arasında hassas bir denge kurulmasını gerekli hale getirmektedir.

GDPR, işyerinde veri işleme faaliyetlerini daha ayrıntılı biçimde düzenlemekte ve çalışan verilerinin yalnızca belirli, meşru ve ölçülü amaçlarla işlenmesine izin vermektedir. Özellikle GDPR'ın 22. maddesi, bireylerin yalnızca otomatik işlemeye dayalı ve kendileri üzerinde hukuki veya benzer önemli etkiler doğuran kararlara tabi tutulmasına ilişkin çeşitli güvenceler öngörmekte ve belirli durumlarda insan müdahalesi talep etme hakkı tanımaktadır (GDPR, 2016, art. 22).

KVKK, işyerindeki veri işleme faaliyetlerini daha genel hükümler çerçevesinde düzenlemektedir. Kanunda performans yönetiminde kullanılan algoritmik sistemler, profil oluşturma veya otomatik karar alma süreçlerine ilişkin açık hükümler bulunmamaktadır. Bu durum, özellikle çalışanların dijital gözetim uygulamalarına karşı sahip oldukları hakların sınırları konusunda belirsizlikler yaratabilmektedir. Ayrıca işveren ile çalışan arasındaki güç dengesizliği nedeniyle açık rızanın özgür iradeye dayanıp dayanmadığı da tartışmalı konular arasında yer almaktadır (KVKK, 2016; GDPR, 2016, art. 22). Dijital gözetim uygulamalarının çalışma hayatında yaygınlaşmasıyla birlikte bu tartışmalar daha görünür hale gelmiştir. Özellikle uzaktan çalışma modellerinin artmasıyla çalışanların çevrim içi faaliyetlerinin takip

edilmesi, şirket bilgisayarlarının denetlenmesi ve dijital iletişim araçlarının izlenmesi daha sık karşılaşılan uygulamalar arasında yer almaktadır. Bu durum, işverenin yönetim hakkı ile çalışanın özel hayatının gizliliği arasındaki sınırların yeniden tartışılmasına neden olmaktadır. Avrupa İnsan Hakları Mahkemesi'nin Bărbulescu v. Romania (2017) kararında da, çalışanların dijital iletişimlerinin izlenmesinde ölçülülük ve önceden bilgilendirme ilkelerinin gözetilmesi gerektiği vurgulanmıştır (Üstün ve Günal, 2020).

2.1.3. Sağlık ve Özel Nitelikli Veriler

Çalışanlara ait sağlık bilgileri, biyometrik veriler ve sendika üyeliği gibi bilgiler hem GDPR hem de KVKK kapsamında özel nitelikli veri olarak değerlendirilmektedir. Bu tür veriler, bireyin özel yaşamı ve temel hakları açısından daha hassas kabul edildiği için daha sıkı koruma kurallarına tabi tutulmaktadır.

GDPR'ın 9. maddesi, sağlık ve biyometrik verilerin işlenmesini kural olarak yasaklamakta; ancak açık rıza, iş sağlığı ve güvenliği yükümlülükleri veya sağlık hizmetlerinin yürütülmesi gibi sınırlı durumlarda veri işlenmesine izin vermektedir (GDPR, 2016, art. 9). Ayrıca GDPR, işverenlerin bu verileri korumak için şifreleme, erişim sınırlandırması, anonimleştirme ve veri koruma etki değerlendirmesi gibi ek önlemler almasını zorunlu kılmaktadır. Sağlık verilerinin amaç dışında kullanılması veya üçüncü kişilerle paylaşılması ise ciddi veri ihlali olarak değerlendirilmektedir (GDPR, 2016, art. 32).

KVKK da sağlık verilerini özel nitelikli veri kapsamında değerlendirmekte ve benzer şekilde daha yüksek düzeyde koruma öngörmektedir. Kanunun 6. maddesine göre sağlık verileri temel olarak açık rıza ile işlenebilmekte; ancak kamu sağlığının korunması veya sağlık hizmetlerinin yürütülmesi gibi bazı istisnai durumlarda rıza aranmamaktadır (KVKK, 2016, m. 6). Bununla birlikte KVKK'nın, GDPR'ye kıyasla daha genel bir çerçeve sunduğu ve veri koruma etki değerlendirmesi gibi bazı önleyici mekanizmaları açık biçimde düzenlemediği görülmektedir.

2.1.4. İşten Ayrılma ve Veri Saklama

İş sözleşmesinin sona ermesi, işverenin çalışanlara ait kişisel verilere ilişkin yükümlülüklerini tamamen ortadan kaldırmamaktadır. Hem GDPR hem de KVKK, işten ayrılan çalışanlara ait verilerin yalnızca belirli amaçlarla ve gerekli süre boyunca saklanmasına izin vermektedir (GDPR, 2016, art. 5(1)(e); KVKK, 2016, m.12). Bu süreçte özlük dosyaları, bordro kayıtları, sosyal güvenlik belgeleri ve hukuki süreçlerle ilişkili kayıtlar belirli sürelerle muhafaza edilebilmektedir.

GDPR kapsamında işverenler, iş ilişkisinin sona ermesinden sonra çalışan verilerini yalnızca meşru menfaat veya yasal yükümlülük gibi hukuki dayanaklar çerçevesinde işleyebilmektedir. Özellikle kıdem ve ihbar tazminatı, işe iade davaları veya ücret uyuşmazlıkları gibi olası hukuki süreçler nedeniyle bazı verilerin belirli süre saklanması mümkün olmaktadır. Ancak bu verilerin yalnızca gerekli süre boyunca tutulması, sürenin sonunda silinmesi veya anonim hale getirilmesi gerekmektedir.

Ayrıca eski çalışana ait verilerin üçüncü kişilerle paylaşılmasında veri işleme şartları ve hukuka uygunluk sebeplerinin gözetilmesi önem taşımaktadır (GDPR, 2016).

KVKK'da da benzer şekilde işten ayrılma sonrası veri işleme faaliyetleri belirli hukuki sebeplere dayandırılmaktadır. Ancak GDPR'ye kıyasla KVKK'da iş ilişkisi sonrasındaki veri işleme süreçlerine ilişkin daha sınırlı ve genel düzenlemeler bulunmaktadır. Bu nedenle uygulamada veri saklama süreleri ve veri paylaşımı gibi konular büyük ölçüde Kurul kararları ve genel ilkeler çerçevesinde şekillenmektedir. Özellikle özlük dosyalarının belirli sürelerle saklanması işverenin ileride doğabilecek hukuki uyuşmazlıklarda kendisini savunabilmesi açısından önem taşımaktadır (GDPR, 2016; KVKK, 2016).

3. BULGULAR

3.1. Karşılaştırmalı Değerlendirme

3.1.1. Benzerlikler: İK Süreçlerinde Ortak Dönüşüm

GDPR ve KVKK, İK'nın veri işleme biçimlerini köklü biçimde dönüştürmüştür. Her iki düzenleme de verilerin amaçla sınırlılık, veri minimizasyonu, dürüstlük ve şeffaflık ilkeleriyle işlenmesini zorunlu kılmaktadır.

Uluslararası literatürde de benzer bir yaklaşım görülmektedir. Vargas, Budz ve Onete'ye (2021) göre GDPR, yalnızca Avrupa'daki işletmeleri değil, küresel ölçekte insan kaynakları uygulamalarını da etkilemiş ve veri koruma standartlarının daha sıkı hale gelmesine katkı sağlamıştır. Bu durum, insan kaynakları departmanlarının çalışan verilerini yönetirken yalnızca operasyonel ihtiyaçları değil; etik sorumlulukları, çalışan mahremiyetini ve hukuki yükümlülükleri de daha fazla dikkate almak zorunda kaldığını göstermektedir.

Kuner, Bygrave ve Docksey'ye (2020) göre veri koruma alanında farklı hukuk sistemleri arasında giderek daha benzer bir yaklaşımın geliştiği görülmektedir. Bu çerçevede GDPR, Avrupa Birliği düzeyinde ortak veri koruma standartları oluştururken; KVKK da benzer temel ilkeleri benimseyerek Türkiye'nin küresel veri koruma yaklaşımına uyum sağlamasına katkı sunmaktadır. Bu durum, veri koruma düzenlemelerinin yalnızca ulusal değil, aynı zamanda uluslararası düzeyde ortak bir anlayış etrafında şekillenmeye başladığını göstermektedir.

Bygrave'a (2014) göre bu yakınlaşma yalnızca veri koruma mevzuatlarının teknik açıdan benzerleşmesiyle sınırlı değildir. Aynı zamanda insan kaynakları uygulamalarında çalışan verilerinin işlenmesine ilişkin daha ortak ve evrensel standartların oluşmasına da katkı sağlamaktadır. Bu çerçevede GDPR ve KVKK'nın, insan kaynakları yönetiminde veri işleme süreçlerine ilişkin daha ortak bir yaklaşımın gelişmesini desteklediği söylenebilir.

3.1.2. Farklılıklar: GDPR'ın Katılığı-KVKK'nın Esnekliği

GDPR ve KVKK arasındaki temel farklar, özellikle çalışan haklarının korunma düzeyi ve uygulamadaki denetim mekanizmalarında ortaya çıkmaktadır. GDPR, işveren–çalışan ilişkilerindeki güç dengesizliğini dikkate alarak açık rızanın özgür iradeye dayanmasına önem vermekte; hesap verebilirlik ilkesi, unutulma hakkı ve algoritmik karar verme süreçlerine ilişkin daha ayrıntılı düzenlemeler içermektedir. Bu yaklaşım, özellikle işten ayrılma sonrası veri saklama, silme ve imha süreçlerinin daha sistematik bir çerçevede ele alınmasına katkı sağlamaktadır. KVKK ise benzer temel veri koruma ilkelerini benimsemekle birlikte daha genel bir düzenleme yapısı sunmaktadır. Bununla birlikte Kişisel Verileri Koruma Kurulu'nun 23.06.2020 tarihli ve 2020/481 sayılı kararıyla unutulma hakkı uygulamada kabul edilmiş ve arama motorları üzerinden yapılan aramalarda kişilerin isimlerinin indeksten çıkarılması talepleri bu kapsamda değerlendirilmiştir. Bu durum, KVKK'da uygulamanın önemli ölçüde Kurul kararları ve genel veri koruma ilkeleri çerçevesinde şekillendiğini göstermektedir (KVKK, 2016; GDPR, 2016).

Yaptırım mekanizmaları açısından da GDPR ve KVKK arasında çeşitli farklılıklar bulunmaktadır. GDPR, veri ihlallerine karşı yüksek idari para cezaları öngörmekte ve bazı durumlarda şirketlerin global cirosunun %4'üne veya 20 milyon avroya kadar ceza uygulanabilmesine imkân tanımaktadır (EU, 2016). Bu durum, işletmelerin veri koruma süreçlerine daha kurumsal ve sistematik biçimde yaklaşmasını teşvik etmektedir. KVKK'da da idari yaptırım mekanizmaları bulunmakla birlikte, uygulamada Kurul kararları, rehberler ve bilgilendirme faaliyetleri önemli bir rol oynamaktadır (GDPR, 2016, art. 83; KVKK, 2016, m. 18).

Kurumsal yapı açısından GDPR, bazı şirketlere Veri Koruma Görevlisi (DPO) atama zorunluluğu getirmektedir. Özellikle büyük ölçekli veya hassas veri işleyen kuruluşlarda bu kişinin bağımsız hareket etmesi ve doğrudan yönetime bağlı çalışması beklenmektedir (GDPR, 2016, art. 37–39; Voigt ve Von dem Bussche, 2017). Bu uygulama, veri koruma süreçlerinin kurum içinde daha düzenli ve denetlenebilir şekilde yürütülmesini amaçlamaktadır. KVKK'da ise benzer bir zorunlu görev bulunmamakta; veri koruma süreçleri çoğunlukla şirketlerin kendi uyum veya hukuk birimleri tarafından yürütülmektedir.

Veri işleme şartlarının düzenleniş biçiminde de GDPR ve KVKK arasında bazı farklılıklar bulunmaktadır. GDPR, kişisel verilerin hangi hukuki sebeplerle işlenebileceğini daha ayrıntılı şekilde düzenlemekte ve bu kuralların uygulanmasına ilişkin daha kapsamlı rehberler sunmaktadır. KVKK ise veri işleme şartlarını daha genel bir çerçevede ele almaktadır. Bu durum uygulamada farklı değerlendirmelerin ortaya çıkmasına neden olabilmektedir. Çekin'e (2020) göre Türkiye'de uygulamanın önemli bir kısmı Kişisel Verileri Koruma Kurulu'nun kararları ve yorumları doğrultusunda şekillenmektedir.

GDPR, kişisel verilerin korunmasının yalnızca yasal düzenlemelerle değil, aynı zamanda bağımsız denetim mekanizmalarıyla da desteklenmesini öngörmektedir. Bu kapsamda Avrupa Birliği ülkelerinde GDPR'ın uygulanmasını denetleyen bağımsız veri koruma kurumları bulunmaktadır. Fransa'daki Ulusal Bilişim ve Özgürlükler

Komisyonu (CNIL), Almanya'daki Federal Veri Koruma ve Bilgi Edinme Özgürlüğü Komiserliği (BfDI) ve İspanya'daki İspanyol Veri Koruma Ajansı (AEPD) bu kurumlara örnek gösterilebilir. Ayrıca Avrupa Veri Koruma Kurulu (EDPB), Avrupa genelinde uygulama birliğini destekleyen bir koordinasyon yapısı oluşturmaktadır. Özellikle işyeri gözetimi, çalışan verilerinin işlenmesi ve dijital takip uygulamalarına ilişkin kararlar, GDPR'ın çalışan haklarını korumaya yönelik yaklaşımını güçlendirmektedir.

Türkiye'de veri koruma alanındaki temel yetkili kurum Kişisel Verileri Koruma Kurulu'dur (KVKK, 2016, m. 21). Kurul, yayımladığı rehberler, ilke kararları ve veri ihlali kararları aracılığıyla uygulamaya yön vermekte ve veri koruma kültürünün gelişmesine katkı sağlamaktadır. Literatürde de belirtildiği üzere, Türkiye'de veri koruma uygulamalarının önemli bir kısmı Kurul kararları ve rehber dokümanlar çerçevesinde şekillenmektedir (Çekin, 2020; Gürpınar, 2017). Bu durum, KVKK uygulamasında rehberlik ve uygulama yönlendirmesinin önemli bir rol oynadığını göstermektedir. GDPR'da ise denetim süreçleri, Avrupa Birliği düzeyindeki veri koruma otoriteleri ve çok katmanlı kurumsal yapı aracılığıyla daha sistematik bir çerçevede yürütülmektedir.

3.2. Uygulama Zorlukları

KVKK ve GDPR kapsamında insan kaynakları süreçlerinde karşılaşılan en önemli sorunlardan biri, çalışan verilerinin hangi sınırlar içinde işlenebileceğinin uygulamada her zaman net biçimde belirlenememesidir. Özellikle işe alım süreçlerinde adaylardan gereğinden fazla kişisel bilgi talep edilmesi, özgeçmişlerin uzun süre sistemlerde tutulması veya referans araştırmalarının adayın bilgisi dışında yürütülmesi veri koruma açısından çeşitli tartışmaları beraberinde getirmektedir. GDPR, veri minimizasyonu ve amaçla sınırlılık ilkelerini daha ayrıntılı biçimde düzenlerken, KVKK'da bu ilkeler daha genel hükümler çerçevesinde ele alınmaktadır (GDPR, 2016; KVKK, 2016). Bu durum, insan kaynakları uygulamalarında kurumlar arasında farklı veri işleme yaklaşımlarının ortaya çıkmasına neden olabilmektedir.

Özellikle gelişen teknolojiyle birlikte işyerlerinde çalışanların elektronik sistemler aracılığıyla izlenmesi daha yaygın hale gelmiştir. Biyometrik giriş sistemleri, kamera uygulamaları, konum belirleme sistemleri ve dijital iletişim araçlarının denetlenmesi, işverenin yönetim hakkı ile çalışanın mahremiyet hakkı arasındaki dengeyi daha tartışmalı hale getirmektedir (Uncular, 2020; Üstün ve Günal, 2020). Çalışan verilerinin hukuka aykırı biçimde işlenmesi ise yalnızca etik ve yönetsel sorunlar doğurmamakta; aynı zamanda hukuki ve cezai sorumluluk risklerini de beraberinde getirmektedir. Nitekim Türk Ceza Kanunu'nun 132 ve devamı maddelerinde kişisel verilerin hukuka aykırı kaydedilmesi, paylaşılması veya ele geçirilmesine ilişkin çeşitli cezai yaptırımlar düzenlenmiştir. Bu durum, insan kaynaklarında veri yönetiminin yalnızca operasyonel bir süreç değil; aynı zamanda kurumsal risk yönetimi ve yönetişim açısından stratejik bir alan olduğunu göstermektedir (Baysal, 2023).

Bir diğer önemli sorun ise veri koruma uygulamalarının kurumların teknik ve yönetsel kapasitesine bağlı olarak farklılık göstermesidir. Veri envanteri oluşturulması, erişim

yetkilerinin sınırlandırılması, saklama sürelerinin belirlenmesi ve verilerin güvenli biçimde muhafaza edilmesi gibi süreçler her kurumda aynı düzeyde uygulanamamaktadır. Özellikle veri koruma süreçlerinin yalnızca hukuk birimlerinin sorumluluğunda görülmesi, insan kaynakları uygulamalarında çeşitli eksikliklere yol açabilmektedir. Bu nedenle veri koruma yaklaşımının yalnızca hukuki uyumla sınırlı kalmaması; insan kaynakları, bilgi işlem ve yönetsel süreçlerle birlikte ele alınması gerektiği vurgulanmaktadır (Tataru ve Tataru, 2020).

İnsan kaynakları uygulamalarında karşılaşılan önemli sorunlardan biri de çalışan verilerinin yurt dışına aktarılmasıdır. Özellikle çok uluslu şirketlerde kullanılan bulut tabanlı insan kaynakları yazılımları ve global performans yönetim sistemleri, çalışan verilerinin farklı ülkelerdeki sunucularda işlenmesine neden olabilmektedir. GDPR, yurt dışına veri aktarımını yeterlilik kararları, standart sözleşmeler ve uygun güvenceler gibi çeşitli mekanizmalar çerçevesinde ayrıntılı biçimde düzenlemektedir (GDPR, 2016, art. 44–49). KVKK'da da yurt dışına veri aktarımına ilişkin düzenlemeler bulunmakta olup, özellikle 2024 yılında yapılan değişikliklerle birlikte veri aktarım mekanizmalarının GDPR'a daha uyumlu hale getirilmeye çalışıldığı görülmektedir (KVKK, 2016, m. 9).

3.3. Kuramsal Tartışma: Uyumun Ötesinde Etik ve Yönetişim

Veri koruma tartışmaları, yalnızca yasal uyumun sağlanmasıyla sınırlı kalmayıp; etik değerler, yönetişim ilkeleri ve çalışanların kendi verileri üzerindeki söz hakkı gibi daha geniş bir çerçevede ele alınmaya başlamıştır.

Bu perspektif, Bodie'nin (2022) çalışan verilerini yalnızca mahremiyet bağlamında değil; aynı zamanda çalışanların kendi verileri üzerindeki kontrolü ve karar süreçlerine katılımı açısından değerlendirmesiyle örtüşmektedir. Bu yaklaşım, çalışanların verilerinin nasıl kullanıldığı konusunda söz sahibi olmasını da önemli görmektedir. Böylece insan kaynakları yönetimi, yalnızca yasal yükümlülükleri yerine getiren idari bir yapı olmaktan çıkmakta; çalışan hakları ile veri yönetimini birlikte değerlendiren daha stratejik bir role dönüşmektedir. Bu dönüşüm aynı zamanda örgütsel verimlilik, performans yönetimi ve güvenlik gibi kurumsal çıkarlar ile çalışanların mahremiyet, bireysel özerklik ve kendi verileri üzerindeki denetim hakkı arasında hassas bir denge kurulmasını gerekli hale getirmektedir. Kurumlar dijital sistemler aracılığıyla çalışan verilerine daha fazla ihtiyaç duyarken, çalışanlar açısından kişisel verilerin korunması yalnızca hukuki değil; aynı zamanda özgürlük, özerklik ve etik yönetişim meselesi olarak değerlendirilmektedir (Küzeci, 2010). Bununla birlikte iş ilişkisinin taraflar arasında eşit güç ilişkisine dayanmaması, çalışanların veri işleme süreçlerine verdikleri rızanın her zaman tam anlamıyla özgür iradeye dayanıp dayanmadığı tartışmasını da gündeme getirmektedir. İşçinin ekonomik ve hukuki açıdan işverene bağımlı olması, çalışan verilerinin korunmasını yalnızca hukuki değil aynı zamanda etik bir yönetişim meselesi haline getirmektedir (Deniz, 2021). Bu bağlamda çalışanların işini kaybetme korkusu, performans baskısı veya örgütsel otorite nedeniyle veri işleme uygulamalarını sorgulamadan kabul edebildiği ifade edilmektedir (Çelik, 2025).

Greenwood ve arkadaşlarına (2017) göre veri koruma uygulamaları, şirketlerin yalnızca yasal düzenlemelere uyum sağlamasıyla sınırlı değildir. Aynı zamanda çalışanlar ve diğer paydaşlarla güven ilişkisi kurulmasında da önemli bir rol oynamaktadır. Benzer şekilde Suchman (1995), kurumsal meşruiyetin yalnızca paydaş çıkarlarına değil, aynı zamanda normatif onaya dayandığını belirtmektedir. Bu çerçevede örgütlerin etik değerlere ve toplumsal normlara uyum sağlaması, meşruiyetin güçlenmesinde kritik bir unsur olarak görülmektedir.

Martin, Borah ve Palmatier'nin (2017) çalışmaları da veri gizliliğinin yalnızca çalışan güveni açısından değil, işletmelerin performansı açısından da önemli olduğunu göstermektedir. Veri korumaya önem veren şirketlerin çalışanlar ve paydaşlar nezdinde daha güvenilir algılandığı, bunun da uzun vadede kurumsal itibarı ve rekabet gücünü desteklediği ifade edilmektedir. Bu nedenle veri koruma, yalnızca hukuki bir yükümlülük değil; aynı zamanda kurumların sürdürülebilir rekabet avantajı elde etmesinde etkili olan stratejik bir unsur olarak değerlendirilmektedir. Bu çerçevede insan kaynaklarında veri yönetimi, sadece yasal uyumu sağlama süreci değil; etik değerler, güven, kurumsal itibar ve çalışan haklarını birlikte kapsayan çok boyutlu bir sorumluluk alanı haline gelmektedir.

4. TARTIŞMA

Bu çalışma, GDPR ve KVKK düzenlemelerinin insan kaynakları yönetiminde kişisel verilerin işlenmesi üzerindeki etkilerini karşılaştırmalı bir çerçevede ele almıştır. Bulgular, veri koruma uygulamalarının yalnızca hukuki bir uyum süreci olmadığını; çalışan hakları, örgütsel güven, etik yönetişim ve kurumsal sürdürülebilirlik açısından da önemli sonuçlar doğurduğunu göstermektedir. Özellikle işe alım, performans yönetimi, dijital gözetim, sağlık verilerinin işlenmesi ve işten ayrılma süreçleri gibi insan kaynakları uygulamalarında çalışan verilerinin daha şeffaf, ölçülü ve güvenli şekilde işlenmesi gerekliliği ön plana çıkmaktadır.

Çalışma kapsamında yapılan değerlendirmeler, GDPR ve KVKK'nın çalışan verilerinin korunmasına ilişkin benzer temel ilkeleri benimsediğini, ancak düzenleme ve uygulama yöntemleri açısından bazı farklılıklar içerdiğini göstermektedir. GDPR; açık rıza, hesap verebilirlik ilkesi, unutulma hakkı ve veri minimizasyonu gibi konuları daha ayrıntılı ve sistematik biçimde düzenlemektedir. Ayrıca yüksek idari para cezaları ve bağımsız denetim mekanizmaları, veri koruma süreçlerinin kurumsal yapılar içerisinde daha kapsamlı biçimde ele alınmasına katkı sağlamaktadır. KVKK da benzer veri koruma ilkelerini benimsemekte ve çalışan verilerinin korunmasına yönelik önemli güvenceler içermektedir. Bununla birlikte uygulamada Kişisel Verileri Koruma Kurulu'nun kararları ve rehberleri önemli bir yönlendirici rol üstlenmektedir. Nitekim 23.06.2020 tarihli ve 2020/481 sayılı Kurul kararıyla "unutulma hakkı" uygulamada kabul edilmiş ve arama motorlarında kişilerin isimleriyle yapılan aramalarda çıkan sonuçların indeksten çıkarılması talepleri bu kapsamda değerlendirilmiştir. Bu çerçevede GDPR daha ayrıntılı ve denetim odaklı bir düzenleme yapısı sunarken, KVKK'nın uygulama boyutunda Kurul kararları ve rehberlerle şekillenen daha esnek bir yapı ortaya koyduğu söylenebilir.

Araştırma ayrıca veri koruma süreçlerinin insan kaynakları yönetimindeki rolünün giderek daha stratejik hale geldiğini ortaya koymaktadır. Çalışan verilerinin korunması yalnızca yasal riskleri azaltmaya yönelik teknik bir süreç olarak değil; çalışan güvenini artıran, kurumsal itibarı destekleyen ve örgütsel meşruiyeti güçlendiren bir unsur olarak değerlendirilmektedir. Özellikle dijital gözetim uygulamalarının yaygınlaşması, insan kaynakları departmanlarının etik sorumluluklarını daha görünür hale getirmektedir. Bu durum, veri yönetiminin yalnızca hukuk veya bilgi işlem birimlerinin değil; insan kaynakları, kalite yönetimi ve kurumsal iletişim gibi farklı birimlerin koordinasyonunu gerektiren çok boyutlu bir yönetişim alanına dönüştüğünü göstermektedir.

Bu bulgular doğrultusunda insan kaynakları departmanlarının veri koruma süreçlerini yalnızca hukuki uyum perspektifiyle ele alması yeterli değildir. Çalışanların veri işleme süreçleri hakkında açık biçimde bilgilendirilmesi, veri minimizasyonu ilkesine dikkat edilmesi, dijital gözetim araçlarının ölçülü kullanılması ve veri güvenliği uygulamalarının kurumsal kültürün bir parçası haline getirilmesi önem taşımaktadır. Ayrıca insan kaynakları çalışanlarına yönelik düzenli eğitim programları, veri koruma farkındalığının örgüt içinde yaygınlaşmasına katkı sağlayabilir.

Bu çalışmanın bazı sınırlılıkları bulunmaktadır. Araştırma kavramsal ve karşılaştırmalı bir çerçeveye dayandığı için ampirik saha verileri kullanılmamıştır. Değerlendirmeler büyük ölçüde mevcut literatür ve yasal düzenlemeler üzerinden yapılmış, sektör bazlı uygulama farklılıkları ayrıntılı biçimde ele alınmamıştır. Bu nedenle ileride yapılacak ampirik ve sektör odaklı çalışmaların, veri koruma uygulamalarının insan kaynakları süreçlerindeki etkilerini daha somut biçimde ortaya koyacağı düşünülmektedir.

Araştırma aynı zamanda gelecekte yapılacak araştırmalar için çeşitli alanlara işaret etmektedir. Özellikle farklı sektörlerde veri koruma uygulamalarının karşılaştırmalı olarak incelenmesi, çalışanların veri koruma politikalarına ilişkin algılarının araştırılması ve çok uluslu şirketlerde birden fazla veri koruma rejiminin nasıl yönetildiğinin analiz edilmesi literatüre önemli katkılar sağlayabilir. Bunun yanında veri koruma uygulamalarının çalışan bağlılığı, örgütsel güven ve iş tatmini üzerindeki etkilerinin ampirik çalışmalarla incelenmesi de önemli bir araştırma alanı olarak görülmektedir.

SONUÇ

Bu çalışma, KVKK ve GDPR'ın insan kaynakları süreçlerinde çalışan verilerinin korunmasına yönelik benzer temel ilkeler benimsediğini, ancak düzenleme ve uygulama bakımından farklılaştığını göstermektedir. GDPR daha ayrıntılı, sistematik ve denetim odaklı bir yapı sunarken, KVKK uygulaması büyük ölçüde Kişisel Verileri Koruma Kurulu kararları ve yayımlanan rehberler doğrultusunda şekillenmektedir. Bu farklılıklar özellikle işe alım, dijital gözetim, özel nitelikli verilerin işlenmesi,

verilerin saklanması ve işten ayrılma sonrası yürütülen süreçlerde daha belirgin hâle gelmektedir.

Sonuç olarak çalışan verilerinin korunması yalnızca yasal yükümlülüklerin yerine getirilmesi olarak değerlendirilmemelidir. İnsan kaynakları departmanlarının çalışanları veri işleme süreçleri hakkında açık biçimde bilgilendirmesi, yalnızca gerekli verileri toplaması ve bu verileri güvenli şekilde saklaması önem taşımaktadır. Veri koruma süreçlerinin insan kaynakları, hukuk ve bilgi işlem birimlerinin iş birliğiyle yürütülmesi hem olası hukuki riskleri azaltmakta hem de çalışan güveni ile kurumsal itibarı desteklemektedir. Bu nedenle veri koruma, hukuki uyumun yanı sıra etik ve stratejik bir insan kaynakları sorumluluğu olarak ele alınmalıdır.

DATA PROTECTION AND STRATEGIC MANAGEMENT IN HUMAN RESOURCES: A COMPARATIVE APPROACH TO KVKK AND GDPR

1. INTRODUCTION

With the acceleration of digitalization, human resource management has become one of the organizational fields where employee data are most intensively processed. In every stage of HR practices such as recruitment, performance evaluation, training, compensation, and termination, the systematic processing of identity, contact, health, and performance data places data protection principles at the core of working life. In this context, the General Data Protection Regulation (GDPR) in the European Union and the Turkish Personal Data Protection Law (KVKK) establish fundamental principles such as lawfulness, transparency, data minimization, and storage limitation, thereby guiding organizational practices. However, significant differences exist between the two regulations in terms of rights safeguards, enforcement mechanisms, and institutional frameworks. This study aims to examine the implications of these differences for human resource processes through a conceptual and comparative perspective..

2. METHODS

This study adopts a conceptual and comparative research design rather than an empirical field analysis. First, the regulatory frameworks of the General Data Protection Regulation (GDPR) in the European Union and the Turkish Personal Data Protection Law (KVKK) were systematically examined. Then, their implications for human resource management were analyzed through an extensive review of academic literature, legal texts, and institutional reports. The study further compares core principles such as lawfulness, transparency, purpose limitation, data minimization, and accountability across the two regulations. As a theoretical lens, Institutional Theory was employed to explain the role of external pressures and legitimacy concerns, while the Resource-Based View (RBV) was used to interpret data protection as a strategic resource that strengthens organizational trust and competitive advantage.

3. RESULTS

The findings indicate that KVKK and GDPR are largely built upon similar core data protection principles, although they differ in terms of scope, rights safeguards, and implementation mechanisms. GDPR regulates the principles of transparency and accountability in a more detailed manner and provides a more systematic framework for the protection of employee data through provisions related to the right to be forgotten and algorithmic decision-making processes. KVKK, on the other hand, adopts similar fundamental principles, while the decisions and guidelines of the Personal Data Protection Authority play an important guiding role in practice. These differences become particularly visible in areas such as the retention of recruitment data, performance management, and workplace surveillance. In addition, the

evaluations conducted within the scope of the study reveal that HR professionals face three major challenges in implementing data protection practices: (1) lack of legal knowledge, (2) deficiencies in technical infrastructure and security measures, and (3) limited organizational awareness. Overall, the study concludes that GDPR and KVKK pursue similar objectives regarding the protection of employee data, while adopting different regulatory and implementation approaches.

4. DISCUSSION

The comparative analysis of GDPR and KVKK demonstrates that data protection in human resource management should not be viewed solely as a legal compliance issue but also as a matter of organizational legitimacy, employee trust, and sustainable corporate reputation. While GDPR ensures stronger employee-oriented safeguards by narrowing employers' discretion through detailed principles and strict sanctions, KVKK provides a more flexible framework that often prioritizes organizational needs and relies on interpretative practices. From a theoretical perspective, these findings align with Institutional Theory, which explains how organizations adapt to external regulatory pressures to maintain legitimacy, and the Resource-Based View (RBV), which highlights data protection as a strategic capability that can enhance employee commitment and create long-term competitive advantage.

CONCLUSION

In conclusion, the comparative analysis of GDPR and KVKK reveals that both regulations are built upon common fundamental principles such as lawfulness, transparency, and data minimization, although they differ in terms of scope and implementation mechanisms. Through its detailed provisions, accountability approach, and enforcement mechanisms, GDPR provides a more systematic framework for the protection of employee data and encourages organizations to integrate data protection into their strategic and operational structures. KVKK, on the other hand, adopts similar fundamental principles while presenting a more flexible regulatory structure shaped in practice through the decisions and guidelines of the Personal Data Protection Authority. From a human resource management perspective, this demonstrates that data protection practices should be evaluated not only within the scope of legal compliance, but also in relation to organizational culture, employee trust, and managerial processes. In the Turkish context, the effectiveness of data protection practices can be said to be largely shaped by organizational awareness, implementation capacity, and regulatory guidance.

KAYNAKÇA

Article 29 Data Protection Working Party. (2017). Opinion 2/2017 on data processing at work (s. 3-24) Erişim: 15 Ekim 2025, https://ec.europa.eu/newsroom/article29/items/610169

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. https://doi.org/10.1177/014920639101700010

Baysal, U. (2021). *İş hukukunda kişisel verilerin işlenmesi*. Kişisel Verileri Koruma Kurumu.

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Geden, A. M. ve Bensghir, T. K. (2018). Reflections from GDPR to Turkish Data Protection Act in the Context of Privacy Principles. 5th International Management Information Systems Conference, 24-26 Ekim 2018, Ankara.118-122.

Bodie, M. T. (2022). The law of employee data: Privacy, property, governance. *Indiana Law Journal*, 97(3), 707–765.

Bondarouk, T. ve Brewster, C. (2016). Conceptualising the future of HRM and technology research. *The International Journal of Human Resource Management*, 27(21), 2652–2671. https://doi.org/10.1080/09585192.2016.1232296

Çekin, M. S. (2020). *Avrupa birliği hukukuyla mukayeseli olarak 6698 sayılı kişisel verilerin korunması kanunu*. On İki Levha Yayınları.

Çelik, G. G. (2025). İşverenin İşçinin Kişisel Verilerini Koruma Yükümlülüğü. *Konya Barosu Dergisi*, (1), 31-54.

Çelik, N., Caniklioğlu, N. ve Canbolat, T. (2020). *İş hukuku dersleri*. İstanbul: Beta Yayınları.

Deniz, Ö. M. (2021). İşçilerin özel nitelikli kişisel verilerinin korunması ve bundan doğan sorumluluk. *Türkiye Adalet Akademisi Dergisi*, *12*(45), 355–378.

Dessler, G. (2020). *Human resource management*. Pearson Education.

DiMaggio, P. J. ve Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. https://doi.org/10.2307/2095101

European Court of Human Rights. (2017). *Bărbulescu v. Romania*. Strasbourg: European Court of Human Rights.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (s. 1-88) Erişim: 15 Ağustos 2025, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Gatewood, R., Feild, H. ve Barrick, M. (2010). *Human resource selection.* Cengage Learning.

Greenwood, R., Oliver, C., Lawrence, T. B. ve Meyer, R. E. (2017*). The SAGE handbook of organizational institutionalism*. SAGE.

Gürpınar, D. (2017). Kişisel verilerin korunamamasından doğan hukuki sorumluluk. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 19 (3), 679–694. https://search.trdizin.gov.tr/tr/yayin/detay/265922/kisisel-verilerin-korunamamasindan-dogan-hukuki-sorumluluk

İnciroğlu, E. K. ve Öğe, E. (2019). İnsan kaynakları ve bilgi işlem departmanlarının işletmelerde kişisel verilerin korunmasındaki rolü: Farklı sektörlerden örnek olay çalışmaları *Uluslararası Sosyal Araştırmalar Dergisi*, *65*(12), 1433-1454

Jabrayilova, Z. (2015). Problems of Protectıon of Personal Data in Human Resource Management Systems. *Problems of information society,* 6(2), 22-28. https://doi.org/10.25045/jpis.v06.i2.03

Kaya, T. (2022). İş Görüşmeleri Sürecinde Aday İşçinin Kişisel Verilerinin Korunması. *Kişisel Verileri Koruma Dergisi,* 4(2), 34-47.

Kişisel Verilerin Korunması Kanunu [KVKK], Kanun No. 6698. (2016). *Resmî Gazete*, 29677, 7 Nisan 2016.

Kuner, C., Bygrave, L. A., Docksey, C. ve Drechsler, L. (Ed.). (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.

Küzeci, E. (2010). *Kişisel verilerin korunması* (Yayımlanmamış doktora tezi). Ankara Üniversitesi.

Manav, A. E. (2015). İş ilişkisinde işçinin kişisel verilerinin korunması. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi,* 19(2), 95-136.

Mathis, R. L., Jackson, J. H., Valentine, S. ve Meglich, P. (2016). *Human resource management*. Cengage Learning.

Martin, K., Borah, A. ve Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Meyer, J. W. ve Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340–363. https://doi.org/10.1086/226550

Ogriseg, C. (2017). GDPR and personal data protection in the employment context. *Labour & Law Issues*, *3*(2), 1-24. https://doi.org/10.6092/issn.2421-2695/7573

Özdemir, H. (2009). *Elektronik haberleşme alanında kişisel verilerin özel hukuk hükümlerine göre korunması.* Seçkin Yayınları.

Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities*. SAGE.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20(3), 571–610. https://doi.org/10.5465/amr.1995.9508080331

Tataru, A. ve Tataru, A. (2020). Human resources and personal data protection: An indissoluble relationship. *Journal of Public Administration, Finance and Law*, *18*, 303-311. https://doi.org/10.2139/ssrn.5316854

Tikkinen-Piri, C., Rohunen, A. ve Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Toros, F. (2025). Kişisel veri yönetimi politikalarının İnsan Kaynakları departmanı üzerindeki etkileri: Nitel bir analiz. *Sosyal Mucit Academic Review*, *6*(1), 76–97. https://doi.org/10.54733/smar.1540596

Uncular, S. (2020). Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme. *Çalışma ve Toplum*, *3*(66), 1673-1700.

Uncular, S. (2012). *İş ilişkisinde işçinin kişisel verilerinin korunması* (Yayınlanmamış Yüksek lisans tezi). Galatasaray Üniversitesi.

Üstün, Y. ve Günal, A. (2020). İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi. *Kişisel Verileri Koruma Dergisi*, 2(2), 62-73.

Vargas, I., Budz, S. ve Onete, B. (2021). The relationship between human resources activities and the General Data Protection Regulation. Proceedings of the International Conference on Business Excellence*,* 15(1), 552–559.

Voigt, P. ve Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Cham: Springer International Publishing.

Zhang, B., Li, Z., Xie, K., Li, T. ve Huang, B. (2025). Research on data security and privacy protection in corporate human resource management in the digital era. *Journal of Frontier in Economic and Management Research, 1*(1), 402–410.

KATKI ORANI / *CONTRIBUTION RATE*	**AÇIKLAMA / *EXPLANATION***	**KATKIDA BULUNANLAR / *CONTRIBUTORS***
Fikir veya Kavram / *Idea or Notion*	Araştırma hipotezini veya fikrini oluşturmak / *Form the research hypothesis or idea*	Pınar SARP HÜSEYİN
Tasarım / *Design*	Yöntemi, ölçeği ve deseni tasarlamak / *Designing method, scale and pattern*	Pınar SARP HÜSEYİN
Veri Toplama ve İşleme / *Data Collecting and Processing*	Verileri toplamak, düzenlenmek ve raporlamak / *Collecting, organizing and reporting data*	Pınar SARP HÜSEYİN
Tartışma ve Yorum / *Discussion and Interpretation*	Bulguların değerlendirilmesinde ve sonuçlandırılmasında sorumluluk almak / *Taking responsibility in evaluating and finalizing the findings*	Pınar SARP HÜSEYİN
Literatür Taraması / *Literature Review*	Çalışma için gerekli literatürü taramak / *Review the literature required for the study*	Pınar SARP HÜSEYİN