Sosyal Mucit Academic Review

Research Article / Araştırma Makalesi

Cited/Atıf: Toros, F. (2025). Kişisel veri yönetimi politikalarının insan kaynakları departmanı üzerindeki etkileri: Nitel bir analiz. *Sosyal Mucit Academic Review, 6*(1), 76-97. doi: 10.54733/smar.1540596

*Kişisel Veri Yönetimi Politikalarının İnsan Kaynakları Departmanı Üzerindeki Etkileri: Nitel Bir Analiz**

Füsun Toros[1]

Received/ Başvuru: *29.08.2024* ***Accepted/ Kabul:*** *19.02.2025* ***Published/ Yayın:*** *26.03.2025*

Öz

Bu çalışma, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) organizasyonlar üzerindeki etkisinin İnsan Kaynakları (İK) departmanlarının bu süreçteki rolü bağlamında incelemektedir. KVKK'nın yürürlüğe girmesiyle, iş dünyasında kişisel verilerin toplanması, işlenmesi, saklanması ve imha edilmesi süreçleri daha sıkı kurallara bağlanmış, bu da İK departmanlarını veri yönetimi ve güvenliği açısından kritik bir konuma taşımıştır. Araştırma kapsamında, odak grup analizi yöntemi kullanılarak farklı departmanların KVKK süreçlerindeki görevleri değerlendirilmiştir. Bulgular, İK'nın işe alım süreçlerinden çalışan verilerinin saklanmasına, referans kontrollerinden veri imha politikalarına kadar geniş bir sorumluluk alanına sahip olduğunu göstermektedir. Ayrıca, departmanlar arası iş birliğinin artarak İK, Bilgi İşlem ve Hukuk birimlerinin veri güvenliği süreçlerinde merkezi roller üstlendiği belirlenmiştir. KVKK'nın uygulanabilirliğinin artırılması için İK'nın farkındalık eğitimleri düzenlemesi, veri koruma politikaları oluşturması ve teknik güvenlik önlemleriyle iş birliği içinde çalışması gerektiği tespit edilmiştir. Sonuç olarak, KVKK'nın iş dünyasında yalnızca bir yasal uyum süreci olmadığı, aynı zamanda İK'nın organizasyon içindeki rolünü genişleterek onu stratejik bir ortak haline getirdiği görülmektedir.

Anahtar Kelimeler: kişisel verilerin korunması, KVKK, insan kaynakları, veri güvenliği, işe alım, organizasyonel uyumluluk

* Bu çalışma kapsamında etik kurul onayı gerekmemektedir. Çalışmada kullanılan veriler 2020 yılı öncesinde toplanmıştır.

[1] Dr., Tirsan Kardan San. ve Tic. A.Ş., Türkiye, dr.fusuntoros@gmail.com, Orcid: 0000-0003-4500-1608

The Impact of Personal Data Management Policies on Human Resource Department: A Qualitative Analysis

Abstract

This study examines the impact of the Law No. 6698 on the Protection of Personal Data (KVKK) on organizations in the context of the role of Human Resources (HR) departments in this process. With the enactment of KVKK, the collection, processing, storage, and disposal of personal data in the business environment have been subjected to stricter regulations, positioning HR as a crucial player in data governance and security. Using a focus group analysis methodology, the research evaluates the roles of different departments in KVKK compliance. Findings indicate that HR has extensive responsibilities, ranging from recruitment processes and employee data management to reference checks and data retention policies. Additionally, interdepartmental collaboration has increased, with HR, IT, and Legal departments playing central roles in ensuring data security and compliance. To enhance the effectiveness of KVKK implementation, HR departments must conduct awareness training, develop data protection policies, and collaborate with technical teams to implement security measures. The study concludes that KVKK is not merely a legal compliance requirement but also a transformative framework that expands HR's role, making it a strategic partner within organizations.

Keywords: personal data protection, KVKK, human resources, data security, recruitment, organizational compliance

EXTENDED ABSTRACT

Background & Purpose: The increasing digitalization of business processes has brought the management of personal data into the spotlight, necessitating robust legal and organizational frameworks. Personal data protection is not only a legal necessity but also an ethical and strategic concern for organizations. The enactment of the Law No. 6698 on the Protection of Personal Data (KVKK) has significantly altered how organizations, particularly Human Resources (HR) departments, handle personal data. HR departments, traditionally responsible for workforce management, are now at the forefront of ensuring compliance with personal data protection laws, influencing recruitment, employee record management, and interdepartmental data governance. This study aims to analyze the impact of evolving legal regulations on personal data management in HR departments through a qualitative research approach. It investigates how HR professionals adapt to legal requirements, what challenges they encounter, and how data security practices are integrated into HR workflows. The study also examines how HR departments collaborate with Legal, IT, and Quality Management teams to implement compliance strategies effectively.

Research Method: This research adopts a qualitative methodology, utilizing the focus group analysis technique to gather insights from professionals across different departments involved in personal data management. A total of seven experts from HR, Legal, IT, Quality Management, Occupational Health & Safety, Corporate Communications, and the Personal Data Protection Registry (VERBIS) participated in the study. The focus group discussions were structured to assess: (i) The role of HR in personal data management before and after the KVKK implementation; (ii) Interdepartmental collaboration in ensuring compliance; (iii) The security measures adopted to protect employee data; (iv) The impact of KVKK on HR responsibilities, including recruitment, data retention, and employee privacy. The data analysis followed content analysis principles, identifying key themes, such as the expansion of HR's role, compliance challenges, and the necessity for increased data security measures.

Conclusion: The findings of this study underscore the transformative impact of data protection regulations on HR practices, highlighting how Human Resources (HR) has evolved from a traditional administrative unit into a key player in organizational data governance. With the implementation of personal data protection laws, particularly the Law No. 6698 on the Protection of Personal Data (KVKK), HR departments have assumed increased responsibilities in ensuring compliance, safeguarding employee data, and fostering a culture of data privacy awareness across organizations. One of the most significant outcomes of this transformation is the interdepartmental collaboration required for successful compliance. HR professionals no longer operate in isolation but work closely with Legal, IT, and Quality Management departments to integrate data security measures into HR processes. This collaboration is essential in establishing secure data processing mechanisms, determining appropriate data retention and disposal policies, and implementing risk mitigation strategies that align with legal requirements. The study also reveals that HR professionals face ongoing challenges in

balancing data security with employee privacy rights. While organizations must process and store employee data for various purposes—recruitment, performance evaluations, payroll management, and training records—this process must be transparent, lawful, and proportionate. A key concern raised by participants is the increasing complexity of data retention policies, particularly in reference checks, digital storage security, and the legal timeframes for data deletion. These challenges emphasize the need for clear corporate policies that guide HR in managing employee data responsibly.

1. GİRİŞ

Kişisel verilerin korunması, dijital çağın en önemli hukuki ve etik meselelerinden biri olarak öne çıkmaktadır. Teknolojik gelişmeler ve dijitalleşmenin hız kazanmasıyla birlikte, bireylerin kişisel bilgileri çeşitli platformlarda toplanmakta, işlenmekte ve saklanmaktadır. Bu durum, bireylerin mahremiyet haklarını tehdit ederken, aynı zamanda veri güvenliği ve insan onuruna ilişkin etik tartışmaları da gündeme getirmektedir. Özellikle iş dünyasında, çalışanların kişisel verilerinin korunması konusu büyük bir önem taşımaktadır. İşe alım süreçlerinden bordro yönetimine, performans değerlendirmelerinden iş sağlığı ve güvenliği uygulamalarına kadar geniş bir yelpazede kişisel verilerin işlenmesi, işverenler ve İnsan Kaynakları (İK) departmanları için çeşitli sorumluluklar doğurmaktadır.

Kişisel verilerin korunması konusundaki yasal çerçeve, Avrupa Birliği'nde Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gibi düzenlemelerle oluşturulmuştur. Bu düzenlemeler, işverenlerin çalışanlarına ait kişisel verileri nasıl işleyebileceğini, saklayabileceğini ve gerektiğinde silebileceğini belirlemekte; aynı zamanda bireylerin bu süreçler üzerindeki haklarını güvence altına almaktadır. KVKK'nın yürürlüğe girmesiyle birlikte Türkiye'deki şirketler, çalışan verilerinin yönetimi konusunda daha sıkı yükümlülüklere tabi olmuş, İK departmanlarının veri güvenliği süreçlerindeki rolü önemli ölçüde artmıştır.

Bu bağlamda, çalışmanın amacı, KVKK'nın iş dünyasında özellikle İK departmanları üzerindeki etkilerini analiz etmek, kişisel verilerin işlenmesi ve korunması sürecinde karşılaşılan zorlukları belirlemek ve bu süreçlerin etkin yönetimine yönelik öneriler sunmaktır. Çalışmada, kişisel verilerin korunmasının insan onuru ile ilişkisi ele alınarak, işe alım süreçlerinden iş sağlığı ve güvenliği uygulamalarına kadar çeşitli İK süreçlerinde veri yönetiminin nasıl gerçekleştirildiği incelenecektir.

Bu çalışmada, nitel araştırma yöntemi kullanılarak, kişisel verilerin korunmasıyla ilgili mevcut yasal düzenlemelerin İK süreçlerine etkisi değerlendirilmiştir. Çalışma kapsamında, farklı sektörlerden İK yöneticileriyle yapılan odak grup görüşmeleri ve belge analizi yöntemlerinden yararlanılmıştır. Odak grup görüşmelerinde, KVKK'nın uygulanmasına ilişkin zorluklar, İK departmanlarının karşılaştığı sorunlar ve veri güvenliği politikalarının iş süreçlerine entegrasyonu konularında derinlemesine bilgiler elde edilmiştir. Ayrıca, İK süreçlerinde kişisel veri işleme politikalarına ilişkin mevzuat, akademik çalışmalar ve sektör raporları incelenerek, mevcut uygulamalar ve karşılaşılan hukuki ve operasyonel sorunlar tespit edilmiştir. Çalışmada, İK yöneticileri, hukuk danışmanları ve bilgi işlem birimi yetkilileriyle yapılan görüşmelerden elde edilen veriler doğrultusunda, kişisel verilerin işlenmesi, saklanması ve imhasına ilişkin pratik çözümler önerilmektedir.

Araştırma bulguları, KVKK'nın İK departmanlarının iş süreçlerinde önemli değişikliklere yol açtığını ve veri yönetimi süreçlerini daha karmaşık hale getirdiğini göstermektedir. KVKK sonrasında şirketler, çalışanların kimlik bilgileri, sağlık verileri ve performans

değerlendirmeleri gibi hassas verileri işlerken daha dikkatli hareket etmektedir. Ancak, verilerin güvenli saklanması konusunda şirketler arasında farklı uygulamalar gözlemlenmiştir. İşe alım süreçlerinde adaylardan toplanan verilerin gerekliliği konusunda şirketlerin farkındalık düzeyinin arttığı, ancak bazı firmaların hala gereksiz veri topladığı belirlenmiştir. İK departmanlarının veri güvenliği süreçlerinde daha fazla sorumluluk üstlendiği, ancak hukuk ve bilgi işlem birimleriyle yeterli koordinasyon sağlanmadığında süreçlerde aksaklıklar yaşandığı görülmüştür. KVKK kapsamında belirlenen yükümlülüklere rağmen, çalışan verilerine yönelik ihlallerin ve siber güvenlik tehditlerinin hala önemli bir risk faktörü olduğu tespit edilmiştir.

Bu bulgular ışığında, çalışmanın önerileri arasında KVKK uyum süreçlerinin daha sistematik hale getirilmesi, çalışanlara yönelik farkındalık eğitimlerinin artırılması ve İK, hukuk ve bilgi işlem birimleri arasında daha güçlü bir iş birliği sağlanması yer almaktadır. KVKK, İK departmanlarının işleyişinde önemli değişikliklere yol açmış ve veri güvenliğini şirket politikalarının temel unsurlarından biri haline getirmiştir. Çalışanların kişisel verilerinin işlenmesi ve saklanmasına yönelik yasal çerçeve, işverenlerin yasal uyumluluğunu artırmakla birlikte, veri yönetimi süreçlerinde yeni zorluklar da yaratmaktadır. İK departmanları, kişisel veri yönetiminde yalnızca operasyonel süreçleri yürütmekle kalmayıp, aynı zamanda şirketin veri güvenliği politikalarının geliştirilmesine de katkı sunan stratejik bir rol üstlenmektedir. Bu çalışmada elde edilen bulgular, KVKK'nın uygulanmasına yönelik daha etkin politika ve stratejiler geliştirilmesi gerektiğini ortaya koymaktadır. Özellikle iş dünyasında kişisel verilerin korunmasına yönelik daha şeffaf ve sistematik yaklaşımlar benimsenerek, çalışanların mahremiyeti korunmalı ve işverenlerin yasal yükümlülükleri sürdürülebilir hale getirilmelidir.

Çalışma aynı zamanda kişisel verilerin korunmasının hem bireysel haklar hem de organizasyonel süreçler üzerindeki önemini vurgulayarak, İK departmanlarının modern yönetim anlayışı içerisindeki stratejik rolünü ortaya koymayı amaçlamaktadır. Bu kapsamda, işveren-işçi ilişkilerinde veri güvenliği uygulamaları, veri koruma süreçlerinde İK'nın rolü ve departmanlar arası iş birliği gibi konular detaylı bir şekilde incelenerek bu araştırma boşluğunun doldurulması amaçlamaktadır. Ayrıca, İK'nın kurumsal farkındalığı artırma ve çalışanları veri koruma politikaları hakkında eğitme rolünü vurgulamaktadır; bu konu mevcut literatürde büyük ölçüde göz ardı edilmiştir. Bu çalışma, İK'nın veri koruma düzenlemeleri çağında geçirdiği stratejik dönüşümü daha derinlemesine anlamaya katkıda bulunarak önemli bir boşluğu dolduracaktır.

2. KAVRAMSAL ARKA PLAN

Günümüz iş dünyasında, dijitalleşme ve teknolojik ilerlemelerle birlikte kişisel verilerin korunması konusu, bireylerin mahremiyet hakkının korunması açısından önemli bir boyut kazanmıştır. Kişisel verilerin korunması, bireyin insan onuru ve özel yaşam hakkının ayrılmaz bir parçası olup, hem hukuki hem de etik bir gereklilik olarak karşımıza çıkmaktadır.

İş hayatında işçi-işveren ilişkileri bağlamında kişisel verilerin işlenmesi ve korunması, özellikle insan kaynakları (İK) yönetiminin temel sorumluluklarından biri haline gelmiştir.

İK departmanları, çalışanların işe alım süreçlerinden başlayarak iş sözleşmelerinin yönetimi, performans değerlendirmeleri, özlük dosyalarının tutulması ve işten ayrılma süreçlerine kadar geniş bir yelpazede kişisel verilerle doğrudan temas halindedir. Bu nedenle, Kişisel Verilerin Korunması Kanunu (KVKK) gibi düzenlemeler, işverenin ve İK departmanlarının veri güvenliğini sağlama yükümlülüğünü artırmış, kişisel verilerin hukuka uygun şekilde işlenmesi ve korunması konusunda kapsamlı bir çerçeve oluşturmuştur.

2.1. Kişisel Verilerin Korunması ve İnsan Onuru

İnsan onuru, bireyin özgürlüğünü ve mahremiyetini temel alan evrensel bir kavramdır. Modern hukuk sistemlerinde, kişisel verilerin korunması, bireyin onurunu güvence altına almanın bir yolu olarak değerlendirilmekte ve özel hayatın gizliliği ile doğrudan ilişkilendirilmektedir (Dülger, 2018). Kişisel verilerin rıza olmadan işlenmesi, bireyin mahremiyet hakkını ihlal edebileceği gibi insan onurunu da zedeleyebilmektedir (Korkmaz, 2014).

Teknolojik gelişmelerle birlikte bireylere ait kişisel verilerin toplanması, depolanması ve analiz edilmesi hız kazanmıştır. Büyük veri analitiği ve yapay zekâ uygulamaları, bireylerin izni olmaksızın verilerini işleyerek mahremiyet sınırlarını zorlamaktadır (Çubukcu, 2024). Özellikle sosyal medya ve dijital platformlar, kişisel verilerin ihlali açısından büyük bir risk oluşturmaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), işverenlerin çalışanlarının elektronik haberleşmesini izlerken bireyin mahremiyet hakkına uygun hareket etmesi gerektiğini belirten kararlar almıştır (Vayena vd., 2018).

Bireylerin mahremiyetinin korunması için kişisel verilerin işlenmesi sürecinde anonimleştirme ve şeffaflık ilkeleri büyük önem taşımaktadır (Eroğlu, 2018). Ancak anonimleştirilen verilerin bile farklı veri kümeleriyle birleştirilerek kimlik tespitinin yapılabileceği belirtilmektedir. Bu nedenle, verilerin korunmasına ilişkin düzenlemeler, bireyin kimliğinin korunmasını ve verilerin etik kurallar çerçevesinde işlenmesini sağlamalıdır.

Kişisel verilerin korunması, yalnızca bireyin mahremiyetini değil, aynı zamanda insan onurunu da korumaya yöneliktir. Hukuki düzenlemelerin ve denetim mekanizmalarının güçlendirilmesi, bireylerin dijital dünyadaki haklarını güvence altına almak için kritik bir öneme sahiptir.

2.2. Kişisel Verilerin Korunması Kanunu ve İnsan Kaynakları Departmanı'nın Rolü

Kişisel verilerin korunması, kurumsal yönetim süreçlerinin en önemli bileşenlerinden biri haline gelmiş olup, İnsan Kaynakları (İK) departmanları bu süreçte kritik bir rol üstlenmektedir (İnciroğlu ve Öge, 2019). Çalışanların işe alım, performans değerlendirme, bordro işlemleri gibi süreçlerde kişisel verileri işlenmekte ve bu verilerin korunması, işverenlerin hukuki sorumlulukları arasına girmektedir (Kartal, 2018).

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), işverenlerin çalışan verilerini yalnızca belirli amaçlarla ve hukuka uygun şekilde işlemesini zorunlu kılmaktadır (Yazıcıoğlu, 2024). İK departmanları, bu süreçleri yönetirken, verilerin güvenli bir şekilde saklanmasını ve gerekli durumlarda imha edilmesini sağlamaktan sorumludur (Ersoy, 2019).

İK departmanlarının KVKK kapsamında üstlendiği temel görevler şu şekilde özetlenebilir (İnciroğlu ve Öge, 2019): (i) Çalışan verilerinin işlenmesi süreçlerini düzenlemek, (ii) Verilerin güvenliğini sağlamak ve erişimi sınırlandırmak, (iii) Çalışanlara kişisel veri farkındalık eğitimleri vermek, (iv) Veri ihlalleri durumunda hızlı müdahale mekanizmaları oluşturmak, ve (v) Yasal düzenlemelere uygun olarak verilerin belirlenen süre sonunda imha edilmesini sağlamak.

Bu süreçler, yalnızca hukuki gerekliliklerin yerine getirilmesini değil, aynı zamanda çalışanların haklarının korunmasını da sağlamaktadır. İK departmanları, kişisel verilerin korunmasında yalnızca teknik önlemler almakla kalmamalı, aynı zamanda organizasyonel güvenlik politikalarının oluşturulmasına ve çalışanların farkındalığının artırılmasına yönelik faaliyetlerde bulunmalıdır (Yazıcıoğlu, 2024).

İK departmanları, kişisel verilerin korunmasına ilişkin yasal yükümlülükleri yerine getirerek, çalışan verilerinin güvenli bir şekilde yönetilmesini sağlamakta ve organizasyon içinde güvenli bir veri yönetim sistemi oluşturulmasına katkıda bulunmaktadır.

2.3. İşe Alım Sürecinde Kişisel Verilerin İşlenmesi

İşe alım süreci, adaylardan toplanan kişisel verilerin işlenmesi açısından kritik bir aşamadır. İşverenler, adayın mesleki yeterliliklerini değerlendirmek amacıyla kimlik bilgileri, eğitim durumu, mesleki deneyimleri gibi bilgileri talep etmektedir (Arthur ve Owen, 2019). Ancak, KVKK kapsamında, etnik köken, dini inanç, medeni durum, siyasi görüş gibi özel nitelikli kişisel verilerin işlenmesi yasalar çerçevesinde sınırlandırılmıştır (Güdek, 2023).

Adaylardan alınan verilerin belirli bir süre saklanması gerekmekte olup, işe alım süreci tamamlandıktan sonra verilerin anonimleştirilmesi veya güvenli şekilde imha edilmesi zorunludur (İnciroğlu ve Öge, 2019). Ayrıca, İK departmanları, referans kontrollerinde adayın rızasını alarak, sadece belirtilen referans kişilerle iletişim kurmalı ve adayın bilgisi dışında herhangi bir veri paylaşımından kaçınmalıdır.

KVKK kapsamında işverenlerin dikkat etmesi gereken en önemli hususlardan biri, işe alım süreçlerinde veri minimizasyonu ilkesine uygun hareket etmektir. İşverenler yalnızca işe uygunluk açısından gerekli bilgileri talep etmeli ve kişisel verilerin gereksiz işlenmesinden kaçınmalıdır (Güdek, 2023).

İşe alım süreçlerinde toplanan kişisel verilerin korunması, işverenlerin hukuki sorumluluklarını yerine getirmesi açısından büyük önem taşımaktadır.

2.4. İş Sağlığı ve Güvenliği (İSG) Kapsamında Kişisel Verilerin Korunması

İş Sağlığı ve Güvenliği (İSG) süreçlerinde, çalışanların sağlık bilgileri, iş kazası kayıtları ve mesleki risk değerlendirmeleri gibi özel nitelikli kişisel verileri işlenmektedir (İnciroğlu ve Öge, 2019). KVKK kapsamında, işverenler yalnızca çalışan sağlığı ve güvenliğiyle doğrudan ilgili olan verileri işlemeli ve bu verilerin güvenli bir şekilde saklanmasını sağlamalıdır (Ersoy, 2019).

Çalışan sağlık verilerinin korunmasına yönelik önerilen önlemler şunlardır: (i) Sağlık verilerine yalnızca yetkilendirilmiş kişilerin erişmesi, (ii) Verilerin yalnızca belirli amaçlar doğrultusunda işlenmesi, (iii) Güvenlik açıklarının düzenli olarak denetlenmesi, ve (iv) Sağlık verilerinin belirli bir süre sonunda güvenli bir şekilde imha edilmesi (Güdek, 2023).

İşverenler, çalışanlarının sağlık verilerini işlerken, veri güvenliğini sağlamak ve yasal düzenlemelere tam uyum göstermek zorundadır. Özellikle, pandemi gibi olağanüstü durumlarda çalışanların sağlık verilerinin işlenmesi gerekliliği, işverenlerin daha hassas ve şeffaf bir yaklaşım benimsemesini gerektirmektedir (Yazıcıoğlu, 2024).

KVKK'nın getirdiği düzenlemeler, işverenlerin ve İK departmanlarının çalışan sağlık verilerini işleme süreçlerini daha dikkatli ve şeffaf bir şekilde yürütmesini zorunlu kılmaktadır. Bu nedenle, işyerlerinde sağlık verilerinin güvenliği için teknik ve idari önlemler alınmalı ve çalışanların veri hakları konusunda bilinçlendirilmesi sağlanmalıdır.

3. ARAŞTIRMA YÖNTEMİ

Bu çalışmada, İnsan Kaynakları (İK) departmanlarının ve diğer departmanların 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamındaki rollerini ve sorumluluklarını anlamak amacıyla nitel bir araştırma yöntemi benimsenmiştir. Araştırma yöntemi olarak odak grup görüşmesi tekniği tercih edilmiştir. Çalışmada kullanılan veriler 2020 yılı öncesinde toplandığından, bu süreçte etik kurul onayı alınmamıştır. Odak grup görüşmesi, belirli bir konu hakkında katılımcıların düşüncelerini, deneyimlerini ve bakış açılarını paylaşmalarını sağlamak için kullanılan bir veri toplama yöntemidir. Bu yöntem, karmaşık konuların daha derinlemesine anlaşılmasını sağlamak ve katılımcılar arasındaki etkileşimden doğan zengin verileri ortaya çıkarmak için uygun bir araçtır (Krueger ve Casey, 2015).

3.1. Odak Grup Analizi Yöntemi

Odak grup analizi, araştırmanın temelini oluşturan bir yöntem olarak tercih edilmiştir. Bu yöntem, katılımcılar arasındaki dinamiklerin ve karşılıklı etkileşimlerin gözlemlenmesini sağlayarak, konunun çok boyutlu bir şekilde incelenmesine olanak tanır (Morgan, 1997). Araştırma sürecinde odak grup yöntemi şu aşamalardan oluşmaktadır.

- **Katılımcıların Belirlenmesi:** Araştırmada, bir otomotiv sektöründe KVKK süreçlerini yöneten profesyoneller hedef grup olarak belirlenmiştir. Farklı departmanlardan 22

profesyonel davet edilmiş, 7 katılımcı görüşmelere katılım sağlamıştır. Katılımcılar, Bilgi Teknolojileri, İnsan Kaynakları, Hukuk, Kalite Yönetimi, Kurumsal İletişim, İş Sağlığı ve Güvenliği (İSG) ve Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) sorumlularından oluşmaktadır.

- **Görüşme Ortamının Tasarlanması:** Katılımcıların rahat bir şekilde etkileşimde bulunabilmesi için görüşme ortamı, U düzeninde tasarlanmıştır. Bu düzen, katılımcıların birbirleriyle göz teması kurarak tartışmalara aktif bir şekilde katılmalarını sağlamıştır (Stewart vd., 2014). Görüşmeler, doğal bir etkileşim ortamında gerçekleşmiştir ve katılımcıların özgürce görüşlerini paylaşmaları teşvik edilmiştir.
- **Görüşme Sorularının Hazırlanması:** Görüşme için açık uçlu ve katılımcıların konuya dair farklı yönlerden bilgi sunmasını sağlayacak sorular hazırlanmıştır. Sorular, KVKK süreçlerinde departmanların rolü, veri güvenliği önlemleri, iş birliği ve farkındalık faaliyetleri gibi konuları kapsamıştır.
- **Veri Toplama:** Görüşmeler, katılımcılardan alınan izinle ses kayıt cihazı kullanılarak kaydedilmiştir. Ayrıca moderatör tarafından önemli noktalar not edilmiştir. Ses kayıtları ve notlar, analiz sürecinde doğruluk ve detaylılık sağlamak için kullanılmıştır.
- **Veri Analizi:** Elde edilen veriler, içerik analizi yöntemi kullanılarak analiz edilmiştir. Katılımcıların ifadeleri temalar ve alt temalar doğrultusunda kategorilere ayrılmış ve bu temalar çerçevesinde sistematik bir şekilde değerlendirilmiştir (Elo ve Kyngäs, 2008). Analiz, katılımcılar arasındaki benzerlik ve farklılıkları ortaya koymanın yanı sıra bu farklılıkların nedenlerini de incelemiştir.

3.2. Katılımcılar ve Veri Toplama Süreci

Katılımcıların seçiminde amaçlı örnekleme yöntemi kullanılmıştır. Bu yöntem, belirli bir konuda derinlemesine bilgi sunabilecek bireylerin seçilmesi esasına dayanır (Patton, 2015). Katılımcılar, KVKK süreçlerine doğrudan dahil olan ve farklı departmanları temsil eden uzmanlardan oluşmaktadır. Araştırmaya katılan 7 katılımcının profilleri Tablo 1'de sunulmuştur.

Tablo 1. Katılımcı profili

Katılımcı	Cinsiyet	Yaş	Departman
P.D.	Kadın	32	Kurumsal İletişim
A.O.	Erkek	38	Bilgi Teknolojileri
T.F.	Erkek	36	İnsan Kaynakları
K.B.	Kadın	43	Kalite Yönetimi
D.L.	Kadın	48	Hukuk
F.Ş.	Erkek	41	VERBİS Sorumlusu
M.D.	Kadın	37	İş Sağlığı ve Güvenliği

3.3. Görüşme Sürecinin Düzeni

Odak grup görüşmesi, katılımcıların doğal bir şekilde etkileşimde bulunmasını sağlamak için güven verici bir ortamda gerçekleştirilmiştir. Görüşmelere bir moderatör rehberlik etmiştir. Moderatör, katılımcıları teşvik etmek ve tartışmayı yönlendirmek amacıyla açık uçlu sorular sormuş, aynı zamanda grup dinamiklerini gözlemlemiştir. Görüşmeler boyunca katılımcıların birbirlerine söz hakkı tanıması teşvik edilmiş ve moderatör, yalnızca görüşmelerin akışını sağlamak amacıyla müdahalelerde bulunmuştur. Görüşme sonunda, belirli temalar etrafında zengin bir tartışma ortamı sağlanmıştır.

Tablo 2. Odak grup soruları

Soru No	Soru	Amaç
1	Hangi departmanda görev yapıyorsunuz?	Katılımcıların görev alanlarını ve şirket içindeki rollerini anlamak.
2	Departmanınız KVKK ile ilgili süreçlerde hangi sıklıkla yer alıyor? Bu süreçlerden nelerden oluşuyor?	KVKK süreçlerine departman bazında katılımın düzeyini ve iş akışını tespit etmek.
3	KVKK kapsamında departmanınızda kişisel veriler işleniyor mu?	Departmanlarda işlenen kişisel veri türlerini ve bunların kullanımını anlamak.
4	İşlenen kişisel veriler hangi amaçla ve ne kadar süreyle saklanıyor?	Verilerin saklanma süresi ve amaçlarının departmanlar arasındaki farklılıklarını belirlemek.
5	KVKK uyumu konusunda departmanınızın rolünü nasıl tanımlarsınız?	Departmanların KVKK kapsamındaki sorumluluk ve rollerini detaylı olarak incelemek.
6	Departmanınızda kişisel veri güvenliğini sağlamak için hangi yöntem ve uygulamaları kullanıyorsunuz?	Veri güvenliği önlemlerinin departmanlar arasındaki çeşitliliğini ve etkinliğini değerlendirmek.

3.4. Veri Analizi Süreci

Verilerin analizinde içerik analizi yöntemi kullanılmıştır. İçerik analizi, verilerden anlamlı temalar ve kategoriler türetmeye odaklanan bir analiz yöntemidir (Hsieh ve Shannon, 2005). Ses kayıtları ve moderatör notları, verilerin detaylı bir şekilde analiz edilmesini sağlamak için kullanılmıştır. Analiz sürecinde şu adımlar izlenmiştir:

- **Ham Verilerin Kodlanması:** Katılımcıların görüşlerinden elde edilen ham veriler, ana temalar doğrultusunda kodlanmıştır. Örneğin, "KVKK uyumu", "veri güvenliği önlemleri" ve "departmanlar arası iş birliği" ana temalar olarak belirlenmiştir.
- **Alt Temaların Oluşturulması:** Her bir ana temanın altındaki detaylar belirlenerek alt temalar oluşturulmuştur. Örneğin, "KVKK uyumu" teması altında "eğitim ihtiyacı" ve "farkındalık faaliyetleri" gibi alt temalar yer almıştır.

- **Tematik Analiz:** Kodlama süreci tamamlandıktan sonra, veriler tematik analizle yorumlanmış ve katılımcılar arasındaki benzerlikler ve farklılıklar belirlenmiştir.
- **Teorik Bağlantıların Kurulması:** Elde edilen bulgular, literatürdeki teorik yaklaşımlarla ilişkilendirilmiş ve daha geniş bir bağlamda değerlendirilmiştir.

3.5. Güvenirlik ve Geçerlik

Araştırmanın geçerliliğini sağlamak amacıyla veri toplama ve analiz sürecinde sistematik bir yöntem izlenmiştir. Ses kayıtları ve notlar arasındaki tutarlılık dikkatle kontrol edilmiş, ayrıca katılımcıların ifadelerinin anlam kaybına uğramaması için kayıtlar ayrıntılı bir şekilde transkript edilmiştir. Verilerin analizinde kullanılan içerik analizi yöntemi, bulguların daha güvenilir bir şekilde yorumlanmasını sağlamıştır.

3.6. Araştırmanın Sınırlılıkları

Bu çalışmanın sınırlılıkları arasında, katılımcı sayısının sınırlı olması ve yalnızca bir sektöre odaklanılmış olması yer almaktadır. Bu durum, bulguların genelleştirilebilirliğini sınırlasa da çalışmanın derinlemesine bir perspektif sunma amacını etkilememiştir. Gelecekteki araştırmalar, farklı sektörlerden daha geniş örneklem gruplarıyla benzer yöntemler kullanılarak yürütülebilir.

Sonuç olarak, bu çalışma, odak grup analizi yöntemiyle KVKK süreçlerindeki departmanlar arası etkileşim ve İK'nın stratejik rolünü derinlemesine incelemiştir. Bu yöntemin sistematik ve yapılandırılmış bir şekilde uygulanması, araştırmanın amaçlarına uygun kapsamlı veriler elde edilmesini sağlamıştır.

4. BULGULAR

4.1. Odak Grup Analizi: Temel Çıkarımlar

KVKK'nın yürürlüğe girmesiyle birlikte, organizasyonların kişisel veri işleme süreçlerinde önemli değişiklikler meydana gelmiştir. Bu bağlamda, departman bazında KVKK öncesi ve sonrası süreçlerdeki farklılıklar belirlenmiştir.

- **Hukuk Departmanı:**

– **KVKK Öncesi:** Hukuki süreçler genellikle dışarıdan danışmanlık hizmetleri alınarak yürütülmekteydi. Veri ihlalleriyle ilgili olarak dış avukatlarla çalışılmakta, kişisel verilerin işlenmesine yönelik sözleşmelerde özel bir düzenleme bulunmamaktaydı.

– **KVKK Sonrası:** İK departmanının talepleri doğrultusunda, KVKK ile uyumlu sözleşmelerin hazırlanması, gizlilik taahhütnamelerinin oluşturulması ve hukuki uyumluluk süreçlerinin şirket içinde yürütülmesi sağlanmıştır.

- **Bilgi İşlem Departmanı:**
  - **KVKK Öncesi:** Personel bilgileri genellikle fiziksel ortamda tutuluyor ve dijital ortama aktarılmıyordu. Veri güvenliğine yönelik belirli bir standardizasyon bulunmamaktaydı.
  - **KVKK Sonrası:** Kişisel verilerin dijital ortamda güvenli bir şekilde saklanması, yedeklenmesi ve korunması için teknik altyapı güçlendirilmiştir. ISO 27001 gereklilikleri doğrultusunda siber güvenlik önlemleri artırılmış, KVKK yazılımları ve ERP sistemleri süreçlere entegre edilmiştir.

- **İş Sağlığı ve Güvenliği (İSG) Departmanı:**
  - **KVKK Öncesi:** İş kazaları ve sağlık verileri işyeri hekimleri tarafından yönetilmekteydi. Çalışanların sağlık bilgileri belirli bir düzen olmaksızın saklanmaktaydı.
  - **KVKK Sonrası:** İş sağlığı ve güvenliği verileri artık İK departmanına bağlı olarak işlenmekte, sağlık verilerinin korunması için KVKK kapsamında özel düzenlemeler yapılmaktadır.

- **Kurumsal İletişim Departmanı:**
  - **KVKK Öncesi:** Etkinliklerde çalışanların ve paydaşların görselleri izin alınmaksızın paylaşılabiliyordu. Fotoğraf, video ve diğer medya kayıtlarının kullanımı konusunda yasal bir düzenleme bulunmamaktaydı.
  - **KVKK Sonrası:** Tüm paydaşlardan açık rıza alınarak veri işleme süreçleri yürütülmektedir. Çalışanların veya paydaşların görselleri, yazılı izin olmadan kullanılamamakta, KVKK'ya uygun paylaşım prosedürleri belirlenmiştir.

- **Kalite Departmanı:**
  - **KVKK Öncesi:** ISO 27001 ve diğer bilgi güvenliği politikaları belirli bir yapıdadır ancak İK ile entegrasyonu sınırlıdır. Veri güvenliği süreci bağımsız şekilde yürütülmektedir.
  - **KVKK Sonrası:** Bilgi güvenliği yönetim sistemleri KVKK'nın bir parçası olarak ele alınmaktadır. Veri güvenliğini sağlamak için risk analizleri ve denetimler İK departmanı ile ortak yürütülmektedir.

- **İnsan Kaynakları (İK) Departmanı:**
  - **KVKK Öncesi:** Çalışanların özlük bilgileri fiziksel olarak arşivlenmekteydi. İşe alım süreçlerinde adaylardan alınan verilerin saklanması ve paylaşımı konusunda belirli bir düzenleme bulunmamaktaydı.
  - **KVKK Sonrası:** Çalışanların tüm kişisel verileri, işe alım sürecinden işten çıkışına kadar titizlikle korunmaktadır. Referans kontrolleri ve çalışan bilgilerinin üçüncü şahıslarla paylaşımı ancak açık rıza alınarak gerçekleştirilmektedir.

- **VERBİS Sorumluluğu:**
  - **KVKK Öncesi:** Organizasyonlarda VERBİS kaydı ve kişisel veri işleme envanteri tutulmamaktaydı.
  - **KVKK Sonrası:** VERBİS kaydı zorunlu hale gelmiş, kişisel verilerin kayıt altına alınması ve güncellenmesi süreçleri İK ile koordineli bir şekilde yürütülmeye başlanmıştır.

Bu değişimler, organizasyonların KVKK ile birlikte veri güvenliği, gizlilik ve hukuki sorumluluklar konusunda daha bilinçli ve sistematik bir yapı oluşturmasına katkı sağlamıştır. Özellikle insan kaynakları departmanı, tüm departmanlar arasındaki kişisel veri yönetiminde merkezi bir rol üstlenerek sürecin hukuki uyumluluğunu sağlamaktadır.

Tablo 3. Departmanların KVKK süreçlerindeki rolleri ve uygulamaları

Departman	KVKK Öncesi Süreçler	KVKK Sonrası Süreçler	KVKK Sürecindeki Rolü	Kişisel Veri Güvenliği Önlemleri
Hukuk	Dış hizmet alımı ile sözleşme ve danışmanlık süreçleri yürütülüyordu.	İçeride yürütülen yasal süreçler, gizlilik taahhütnameleri ve sözleşmeler düzenleniyor.	Yasal uyum, sözleşme hazırlama, gizlilik süreçlerinin takibi.	Hukuki güvence sağlanması, gizlilik taahhütnameleri ve KVKK uyumlu sözleşmelerin hazırlanması.
Bilgi İşlem	Veriler dijital ortamda saklanmıyordu, teknik altyapı eksikti.	Kişisel veriler dijital ortamda şifrelenerek saklanıyor, ISO 27001 standartları uygulanıyor.	Veri güvenliği sağlamak, sistemlerin KVKK uyumluluğunu kontrol etmek.	Veri şifreleme, yedekleme, siber güvenlik yazılımları kullanımı.
İSG	İş sağlığı verileri işyeri hekimi tarafından tutuluyordu.	İK'ya bağlı olarak işleniyor ve güvenlik önlemleri artırıldı.	Çalışanların sağlık verilerini KVKK'ya uygun şekilde saklamak.	Yetkili kişiler dışında erişim kısıtlaması.
Kurumsal İletişim	İç ve dış paydaşlarla yapılan iletişimde veri koruma önceliklendirilmezdi.	Etkinlikler sırasında veri sahiplerinden açık rıza alınması zorunlu hale geldi.	Paydaşlarla iletişim süreçlerinde KVKK'ya uyumu sağlamak.	Veri paylaşımı için açık rıza prosedürlerinin uygulanması.
Kalite	KVKK uyumu bağımsız olarak ISO 27001 ve kalite süreçleri ile ilerliyordu.	İK ile koordineli bir şekilde KVKK uyumlu denetimler yürütülmeye başlandı.	Veri güvenliği risk analizlerini yönetmek.	Bilgi güvenliği denetimleri, veri saklama protokollerinin uygulanması.
İK	Özlük dosyalarının yönetimi ve temel kayıt işlemleri yürütülüyordu.	İşe alım süreçlerinden başlayarak çalışan verilerinin saklanması, işlenmesi ve imhasından sorumlu hale gelindi.	KVKK sürecinin yönetiminde merkezi rol oynama, veri imha prosedürlerini uygulama.	Kişisel verileri güvenli sistemlerde saklama, yalnızca yetkililere erişim izni verme.
VERBİS Sorumlusu	Organizasyonda yer almayan bir rol.	KVKK kapsamında organizasyon yapısına dahil edildi ve veri envanter yönetimi başladı.	VERBİS bildirimlerini yapmak ve güncellemeleri takip etmek.	KVKK'ya uygun olarak kişisel verilerin kayıt altına alınması ve güncellenmesi.

4.2. Odak Grup Görüşmelerinin Analizi ve Yöntemsel Yaklaşım

Odak grup görüşmeleri, belirli bir konu hakkında derinlemesine bilgi edinmek, katılımcılar arasında etkileşimi teşvik etmek ve farklı bakış açılarını ortaya çıkarmak amacıyla kullanılan nitel bir araştırma yöntemidir (Krueger ve Casey, 2015). Bu çalışmada, insan kaynakları (İK) yönetimi bağlamında Kişisel Verilerin Korunması Kanunu (KVKK) uygulamalarının işletmelerdeki yansımalarını anlamak amacıyla odak grup yöntemi tercih edilmiştir. Katılımcılar, KVKK süreçlerini farklı açılardan değerlendiren çeşitli departmanlardan uzmanlardan oluşmaktadır.

Odak grup görüşmesi sürecinde, katılımcıların etkileşimleri**,** ortaya çıkan ana temalar**,** departmanlar arasındaki farklılıklar ve benzerlikler analiz edilmiştir. Bu bağlamda, aşağıdaki üç temel analiz düzeyi belirlenmiştir: (i) Departmanların KVKK süreçlerindeki rolleri ve işlevleri; (ii) Kişisel veri yönetimi ve saklama süreçlerine dair departman bazlı uygulamalar ve (iii) KVKK uyumu için alınan güvenlik önlemlerinin sistematik analizi.

4.2.1. Departmanlar Arası İş Birliği ve Sorumluluk Paylaşımı

Odak grup analizinde departmanlar arası KVKK uyumu konusunda artan iş birliği açıkça görülmektedir. İnsan Kaynakları, Hukuk, Bilgi İşlem ve Kalite departmanları merkezi roller üstlenirken**,** İSG, Kurumsal İletişim ve VERBİS sorumlusu gibi departmanlar destekleyici ancak kritik görevler üstlenmiştir**.** Özellikle İK departmanı, kişisel verilerin korunması ve imhası konusunda ana koordinasyon merkezi olarak konumlanmıştır.

4.2.2. Departmanların KVKK Süreçlerindeki Rollerinin Karşılaştırmalı Analizi

Odak grup verileri, departmanların KVKK uyum sürecinde farklı sorumluluklar üstlendiğini göstermektedir. Analiz sonuçları şu şekildedir:

- **Hukuk Departmanı:** KVKK öncesinde daha çok dış kaynaklı hukuki danışmanlık hizmetlerine bağımlıyken**,** KVKK sonrası iç süreçlerde hukuki sözleşmelerin hazırlanması, gizlilik taahhütnamelerinin oluşturulması ve yasal uyumun sağlanması açısından daha aktif bir rol üstlenmiştir.
- **Bilgi İşlem Departmanı:** Kişisel verilerin dijital ortamda saklanması ve güvenliği için altyapı oluşturulmuştur. ISO 27001 bilgi güvenliği yönetimi çerçevesinde KVKK uyumlu sistemlerin entegre edilmesi sağlanmıştır.
- **İş Sağlığı ve Güvenliği (İSG) Departmanı:** Sağlık verilerinin işlenmesi ve korunması konusunda İK'ya bağlı olarak çalışmaktadır. Sağlık kayıtlarının saklanma süreleri KVKK ile yeniden düzenlenmiştir.
- **Kurumsal İletişim Departmanı:** Eskiden paydaşlarla yapılan iletişim süreçlerinde KVKK uyumuna dikkat edilmezken**,** şimdi her türlü etkinlik ve görsel paylaşımda açık rıza alınması zorunlu hale gelmiştir.

- **Kalite Departmanı:** Bilgi güvenliği standartlarıyla KVKK süreçlerinin entegrasyonu sağlanmıştır. Denetim ve risk analizleri İK ile eşgüdümlü yürütülmektedir.
- **İK Departmanı:** Çalışan verileri konusunda KVKK'nın en fazla etki ettiği departman olarak öne çıkmaktadır. İşe alım, performans değerlendirme, özlük bilgileri yönetimi ve veri imha süreçleri KVKK'ya uygun olarak yeniden yapılandırılmıştır.
- **VERBİS Sorumlusu:** Daha önce organizasyon içinde tanımlanmayan bir pozisyonken, KVKK ile birlikte kişisel veri kayıtlarının yasal takibi açısından merkezi bir rol üstlenmiştir.

Bu karşılaştırma, departmanların KVKK öncesi ve sonrası süreçlerde nasıl bir dönüşüm yaşadığını göstermektedir. Özellikle İK, Bilgi İşlem ve Hukuk birimlerinin süreçlerin merkezinde olduğu ve diğer birimlerle sıkı iş birliği içinde çalıştığı tespit edilmiştir.

Tablo 4. KVKK uyumu için alınan güvenlik önlemleri

Departman	Uygulanan Güvenlik Önlemleri
Hukuk	Sözleşmelerde yasal güvenlik önlemleri, gizlilik taahhütnameleri.
Bilgi İşlem	Veri şifreleme, yedekleme, siber güvenlik yazılımları.
İSG	Sağlık verilerine sadece yetkili kişilerin erişimi.
Kurumsal İletişim	Veri paylaşımı için açık rıza prosedürlerinin uygulanması.
Kalite	Bilgi güvenliği denetimleri, veri saklama protokolleri.
İK	Çalışan verilerinin güvenli sistemlerde saklanması, erişim kontrolü.
VERBİS Sorumlusu	Kişisel verilerin KVKK'ya uygun olarak kayıt altına alınması ve güncellenmesi.

4.2.3. Kişisel Verilerin İşlenmesi ve Saklanma Süreçleri Üzerine Değerlendirme

Odak grup verileri, KVKK öncesinde birçok departmanın kişisel veri saklama süreleri konusunda belirli bir standarda sahip olmadığını**,** ancak KVKK ile bu süreçlerin belirli yasal çerçevelere oturtulduğunu göstermektedir.

- Hukuk Departmanı, sözleşmeler ve taahhütnameleri 10 yıl saklamakla yükümlüdür.
- Bilgi İşlem Departmanı, kişisel verilerin 5 yıl süreyle dijital ortamda güvenli şekilde tutulmasını sağlamaktadır.
- İSG Departmanı, sağlık verilerini 10 yıl boyunca saklamaktadır.
- Kurumsal İletişim Departmanı**,** etkinlik verilerini 2 yıl boyunca arşivlemektedir.
- İK Departmanı, çalışan özlük bilgilerini işten ayrıldıktan sonra bile 10 yıl boyunca saklamaktadır.
- VERBİS Sorumlusu, kişisel veri kayıtlarını 5 yıl süreyle korumaktadır.

Bu bulgular, departmanların veri saklama sürelerinin operasyonel gereklilikler ve yasal düzenlemeler doğrultusunda değiştiğini ve bu süreçlerin artık daha kontrollü yürütüldüğünü göstermektedir.

Tablo 5. KVKK süreçlerinde departmanların kişisel verileri işleme amaçları ve saklama süreleri

Departman	İşlenen Kişisel Veriler	İşleme Amacı	Saklama Süresi
Hukuk	Çalışan sözleşmeleri, gizlilik taahhütnameleri	Yasal süreçlerin yürütülmesi, sözleşmelerin güvence altına alınması.	Yasal süreçlere bağlı olarak 10 yıl
Bilgi İşlem	Dijital veri kayıtları, sistem erişim logları	Verilerin güvenli saklanması, sistem bütünlüğünün korunması.	5 yıl
İSG	İş kazası raporları, sağlık verileri	İş sağlığı ve güvenliği politikalarının uygulanması.	10 yıl
Kurumsal İletişim	Fotoğraf, video kayıtları, etkinlik katılımcı listeleri	İç ve dış paydaşlarla iletişim süreçlerinin yönetilmesi.	2 yıl
Kalite	Veri güvenliği denetim raporları	KVKK uyumunun sağlanması ve denetim süreçlerinin yürütülmesi.	Süre belirtilmemiş
İK	Çalışan özlük bilgileri, eğitim, performans ve disiplin kayıtları	Çalışan verilerinin yasal çerçevede saklanması ve kullanılması.	Çalışan işten ayrıldıktan sonra 10 yıl
VERBİS Sorumlusu	VERBİS kayıtları ve raporları	Kişisel verilerin kayıt altına alınması ve yasal uyumun sağlanması.	5 yıl

4.2.4. KVKK Uyumu İçin Alınan Güvenlik Önlemlerinin Analizi

KVKK uyumu bağlamında departmanların aldığı güvenlik önlemleri**,** odak grup analizinde üç ana tema altında toplanmıştır:

- **Tema 1. Hukuki Önlemler:** Sözleşmelerin yeniden düzenlenmesi, gizlilik taahhütnameleri, veri koruma politikalarının oluşturulması.
- **Tema 2. Teknik Önlemler:** Bilgi İşlem departmanı tarafından yürütülen veri şifreleme, sistem erişim kontrolleri, siber güvenlik yazılımları ve yedekleme gibi uygulamalar.
- **Tema 3. Yönetsel Önlemler:** İK tarafından yürütülen eğitim ve farkındalık çalışmaları, veri sorumluları için denetim mekanizmalarının oluşturulması.

Özellikle İK ve Bilgi İşlem departmanlarının güvenlik politikaları konusunda merkezi bir rol oynadığı ve diğer departmanlarla koordinasyon içinde olduğu tespit edilmiştir.

Odak grup analizinden elde edilen veriler doğrultusunda aşağıdaki çıkarımlar yapılabilir:

- Departmanlar arası iş birliği zorunluluğu artmıştır. KVKK uyum sürecinde İK, Bilgi İşlem ve Hukuk birimleri en kritik rolleri üstlenmiştir.
- Veri saklama ve imha süreçleri yasal çerçeveye oturtulmuştur. Eskiden belirli standartlara sahip olmayan süreçler, artık KVKK kapsamında yasal gerekliliklere göre yürütülmektedir.
- Dijitalleşme ve siber güvenlik önlemleri öncelik kazanmıştır. Bilgi İşlem departmanı, siber güvenlik yazılımlarının entegrasyonu ve veri güvenliği süreçlerini yönetme noktasında temel aktör haline gelmiştir.
- Eğitim ve farkındalık artırılmalıdır. KVKK'nın uygulanabilirliğini artırmak için çalışanların farkındalığını yükseltmeye yönelik eğitimlerin düzenli olarak yapılması gerekmektedir.

Odak grup analizine dayalı olarak yapılan bu değerlendirme, KVKK'nın organizasyonlarda önemli bir dönüşüm yarattığını ve departmanlar arasındaki sorumluluk paylaşımının netleştiğini göstermektedir. Özellikle İK'nın veri yönetimi ve hukuki süreçlerde merkezi bir rol üstlendiği, Bilgi İşlem'in teknik güvenliği sağladığı ve Hukuk biriminin yasal süreçleri denetlediği açıkça görülmüştür. KVKK'nın etkin şekilde uygulanabilmesi için departmanlar arası koordinasyonun güçlendirilmesi, güvenlik önlemlerinin sürekli güncellenmesi ve çalışanların farkındalığının artırılması gerekmektedir.

4.3. Odak Grup Analizi Bağlamında İnsan Kaynakları (İK) Departmanının Rolü ve Değerlendirilmesi

Odak grup analizinde elde edilen veriler, İnsan Kaynakları (İK) departmanının KVKK süreçlerinde en kritik rolü üstlenen birimlerden biri olduğunu ortaya koymaktadır. KVKK öncesinde İK departmanları, çalışanların özlük bilgileri, işe alım süreçleri ve bordrolama gibi temel işlevlere odaklanırken, KVKK sonrasında veri güvenliği, kişisel veri işleme politikalarının oluşturulması, saklama ve imha süreçlerinin yönetimi gibi yeni sorumluluklarla genişleyen bir görev tanımıyla karşı karşıya kalmıştır.

Odak grup görüşmelerinde, İK'nın KVKK sürecinde merkezi koordinasyon rolü üstlendiği belirlenmiştir. Özellikle çalışan verilerinin toplanması, işlenmesi, saklanması ve imha edilmesi süreçleri doğrudan İK departmanının kontrolünde yürütülmektedir. Departmanların verdiği yanıtlar ışığında, İK'nın KVKK bağlamında üstlendiği temel roller aşağıdaki başlıklar altında analiz edilmiştir.

4.3.1. Çalışan Verilerinin Yönetimi ve KVKK Uyumluluğu

İşe alım süreçlerinde kişisel veri toplama ve işleme: İK, adayların kişisel bilgilerini işe alım sürecinde toplamakta ve bu bilgileri belirli bir süre saklamaktadır. KVKK öncesinde, aday bilgileri uzun yıllar boyunca tutulabilirken, KVKK sonrası belirli bir saklama süresi belirlenerek kişisel verilerin gereksiz tutulması önlenmiştir**.** Çalışan verilerinin korunması: İK, çalışanların açık rızasını alarak kişisel verilerini işleme zorunluluğu getiren birimler arasında yer almaktadır. Çalışanların özlük bilgileri, sağlık kayıtları ve performans verileri gibi birçok özel nitelikli kişisel verinin yasal çerçevede işlenmesi, saklanması ve gerektiğinde imha edilmesi süreçlerini yönetmektedir**.** Referans kontrolleri ve üçüncü taraf paylaşımı: Önceden çalışanların bilgileri, işten ayrıldıktan sonra başka şirketlerle paylaşılabiliyorken, KVKK kapsamında çalışanların açık rızası olmadan üçüncü taraflarla veri paylaşımı yasaklanmıştır.

4.3.2. Kişisel Veri Saklama ve İmha Politikalarının Yürütülmesi

İK, çalışan verilerinin saklama süreleri ve imha süreçlerinin yönetilmesinden sorumludur**.** Örneğin, bir çalışanın işten ayrılması durumunda, özlük dosyaları 10 yıl süreyle saklanmakta ve belirlenen sürenin sonunda KVKK'ya uygun bir şekilde imha edilmektedir. İK, çalışan verilerinin anonimleştirilmesi konusunda da önemli bir rol üstlenmektedir. Örneğin,

çalışanların eğitim geçmişi veya performans değerlendirmeleri anonim hale getirilerek organizasyonel analizlerde kullanılmaktadır.

4.3.3. Departmanlar Arası Koordinasyon ve Eğitim Faaliyetleri

KVKK farkındalık eğitimleri: İK departmanı, çalışanların KVKK uyumu konusunda bilinçlenmesi için eğitim ve farkındalık programları düzenlemektedir. KVKK öncesinde bu tür eğitimler yaygın değilken, KVKK sonrası özellikle işe giriş oryantasyonu süreçlerinde KVKK farkındalık eğitimlerinin zorunlu hale getirildiği görülmektedir**.** Departman içi iş birliği: İK, özellikle Hukuk ve Bilgi İşlem departmanlarıyla sıkı iş birliği içinde çalışarak çalışan verilerinin yasal ve teknik güvenlik açısından korunmasını sağlamaktadır.

4.3.4. Çalışan Sağlığı ve Güvenliği Verilerinin Yönetimi

İK, İş Sağlığı ve Güvenliği (İSG) departmanıyla birlikte çalışarak çalışanların sağlık bilgilerini yasal çerçevede saklamak ve yalnızca yetkililerin erişimine açmakla yükümlüdür**.** Pandemi süreci gibi olağanüstü durumlarda çalışanların aşı durumu, PCR test sonuçları gibi sağlık verileri KVKK kapsamında korunmakta ve işveren tarafından belirlenen süreler boyunca saklanmaktadır.

5. TARTIŞMA ve SONUÇ

Bu çalışma, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) organizasyonlar üzerindeki etkilerini ve özellikle İnsan Kaynakları (İK) departmanının bu süreçteki rolünü incelemektedir. Araştırma sonucunda, KVKK'nın yalnızca hukuki ve teknik bir düzenleme olmanın ötesinde, İK'nın görev tanımını ve organizasyon içindeki konumunu dönüştüren önemli bir faktör olduğu görülmüştür. Benzer şekilde, Savaş vd. (2020) iş süreçlerinin dijitalleşmesi ve çalışanlarla ilgili verilerin elektronik ortamda tutulması, KVKK'nın İK departmanı için önem kazanmasına neden olmuştur. İK, artık yalnızca çalışan ilişkilerini yöneten bir departman değil, aynı zamanda veri güvenliğini sağlayan ve yasal uyumu yöneten stratejik bir birim olarak konumlanmıştır.

İK departmanının KVKK kapsamındaki rolü, çalışan verilerinin yönetimi, veri güvenliğinin sağlanması, işe alım süreçlerinin düzenlenmesi, departmanlar arası iş birliğinin sağlanması ve çalışanlara yönelik farkındalık çalışmalarının yürütülmesi gibi pek çok alanda genişlemiştir. KVKK öncesinde, İK'nın veri yönetimiyle ilgili süreçleri daha serbest bir şekilde yürütülürken, KVKK sonrası süreçlerin belirli standartlar çerçevesinde yürütülmesi zorunlu hale gelmiştir. Çalışan verilerinin toplanması, saklanması ve imha edilmesi süreçlerinin yasal uyumluluk çerçevesinde yürütülmesi gerekliliği, İK'nın görev tanımını büyük ölçüde değiştirmiştir. Bu sonucun temel sebebi olarak, İnciroğlu ve Öge (2019) çalışan verilerinin elektronik ortamda tutulması ve işlenmesinde, fiziksel güvenlik önlemleri kadar teknik güvenlik önlemlerinin de alınması gerekliliğini göstermiştir.

KVKK'nın işe alım süreçlerine etkisi, adaylardan toplanan verilerin yalnızca belirli amaçlar doğrultusunda kullanılmasını ve gereksiz veri toplanmasının önlenmesini zorunlu hale getirmiştir. Özellikle referans kontrolleri, adayın açık rızası olmadan yapılamaz hale gelmiş, adaylardan toplanan verilerin süresiz saklanması yerine belirli süreler içinde imha edilmesi gerekliliği ortaya çıkmıştır. Bu durum, İK'nın işe alım süreçlerini daha dikkatli yönetmesini gerektirmiştir.

Çalışan verilerinin güvenliği ve saklanma süreleri konusunda İK departmanı, kişisel verilerin yalnızca belirlenen süre boyunca saklanmasını ve süre sonunda güvenli bir şekilde imha edilmesini sağlamakla yükümlüdür. Bu süreçte, organizasyon içinde veri güvenliği politikalarının oluşturulması ve uygulanması, İK'nın koordinasyonuyla yürütülmektedir. Özellikle Bilgi İşlem ve Hukuk departmanları ile yapılan iş birliği, veri güvenliği süreçlerinin etkin yönetilmesi açısından kritik bir öneme sahiptir.

KVKK ile birlikte departmanlar arası iş birliği daha önemli hale gelmiş, İK departmanı Bilgi İşlem, Hukuk ve Kalite departmanlarıyla yakın bir şekilde çalışmak zorunda kalmıştır. Hukuk departmanı ile sözleşmelerin hazırlanması, Bilgi İşlem departmanının veri güvenliğini sağlaması ve Kalite departmanının ISO 27001 gibi bilgi güvenliği standartlarına uyum sağlaması gibi süreçlerde İK departmanı koordinatör bir rol üstlenmiştir. KVKK sürecinde, yalnızca yasal gerekliliklerin yerine getirilmesi değil, organizasyon içindeki iş birliği ve uyum mekanizmalarının da güçlendirilmesi gerekmektedir.

Çalışanlara yönelik farkındalık ve eğitim çalışmaları da İK'nın KVKK kapsamında üstlendiği önemli görevlerden biri olmuştur. Çalışanların veri güvenliği konusunda bilinçlendirilmesi, olası ihlallerin önlenmesi açısından büyük bir önem taşımaktadır. Bu nedenle, İK departmanlarının düzenli eğitim programları yürütmesi ve veri güvenliği kültürünü oluşturması gerekmektedir.

Araştırma sonuçları, KVKK'nın yalnızca bir yasal düzenleme olmanın ötesinde, İK'nın organizasyon içindeki rolünü dönüştüren bir süreç olduğunu ortaya koymaktadır. İK departmanları, artık yalnızca personel yönetimiyle sınırlı kalmayıp, veri güvenliği, uyumluluk ve stratejik yönetim süreçlerine doğrudan katkı sağlamaktadır.

KVKK ile birlikte İK departmanları, kişisel verilerin korunması konusunda organizasyonun merkezinde yer alan bir birim haline gelmiştir. Çalışan verilerinin işlenmesi, saklanması ve imha edilmesi süreçlerinin yasal çerçevede yürütülmesi, İK'nın hem iş yükünü artırmış hem de organizasyon içindeki rolünü güçlendirmiştir. Bu bağlamda, İK'nın yasal uyumu sağlamak, çalışan farkındalığını artırmak ve veri güvenliği politikalarını oluşturmak gibi kritik görevleri bulunmaktadır.

KVKK'nın organizasyonel yapılar üzerindeki etkisi değerlendirildiğinde, İK'nın yalnızca bir operasyonel birim olmaktan çıkıp, organizasyonun veri yönetimi stratejisini belirleyen, çalışan farkındalığını artıran ve yasal uyumu sağlayan bir birim haline geldiği görülmektedir. Bu süreç,

İK'nın organizasyon içinde daha fazla sorumluluk almasını ve diğer departmanlarla daha fazla iş birliği yapmasını gerektirmiştir. KVKK'nın etkili bir şekilde uygulanabilmesi için İK departmanlarının süreci doğru yönetmesi, çalışanlara rehberlik etmesi ve organizasyon içinde veri güvenliği kültürünü oluşturması gerekmektedir.

Sonuç olarak, KVKK süreci, İK departmanlarını organizasyon içinde daha stratejik bir konuma taşımış ve veri güvenliği yönetiminde kilit bir aktör haline getirmiştir. İK'nın, çalışanların verilerini koruma sorumluluğunun yanı sıra, organizasyonun genel KVKK uyumluluğunu sağlamada da kritik bir rolü olduğu ortaya çıkmıştır. Bu süreç, İK'nın daha bilinçli, güvenlik odaklı ve veri yönetimi konusunda daha sorumlu bir yapıya dönüşmesini sağlamıştır.

Kaynakça

Arthur, K. N. A., & Owen, R. (2019). A micro-ethnographic study of big data-based innovation in the financial services sector: Governance, ethics and organisational practices. *Journal of Business Ethics, 160*, 363-375. https://doi.org/10.1007/s10551-019-04203-x

Çubukcu, Z. (2024). Dijital çağda kişisel verilerin korunmasında veri koruma otoritelerinin rolü. *Toplum Ekonomi ve Yönetim Dergisi, 5*(3), 454-469. https://doi.org/10.58702/teyd.1485163

Dülger, M. V. (2018). İnsan hakları ve temel hak ve özgürlükler bağlamında kişisel verilerin korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 5*(1), 71-144.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107-115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Eroğlu, Ş. (2018). Dijital yaşamda mahremiyet (gizlilik) kavramı ve kişisel veriler: Hacettepe Üniversitesi bilgi ve belge yönetimi bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 35*(2), 130-153. https://doi.org/10.32600/huefd.439007

Ersoy, E. C. (2019). Examining Turkish law on data protection. *Computer Fraud & Security, 2019*(9), 9-11. https://doi.org/10.1016/s1361-3723(19)30095-8

Güdek, B. (2023). Kamu sektöründe etik yönetime ilişkin politikaların uygulanması: KVKK ve veri etiği. *Politik Ekonomik Kuram, 7*(2), 237-251. https://doi.org/10.30586/pek.1325605

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288. https://doi.org/10.1177/1049732305276687

İnciroğlu, E. K., & Öge, E. (2019). İnsan kaynakları ve bilgi işlem departmanlarının işletmelerde kişisel verilerin korunmasındaki rolü: Farklı sektörlerden örnek olay çalışmaları. *Journal of International Social Research, 12*(65), 1433-1454. https://doi.org/10.17719/jisr.2019.3552

Kartal, M. T. (2018). Kişisel verilerin korunması: türk bankacılık sektörü üzerine kavramsal bir değerlendirme. *Uluslararası Ekonomi ve Yenilik Dergisi, 4*(1), 1-18. https://doi.org/10.20979/ueyd.347548

Korkmaz, A. (2014). İnsan hakları bağlamında özel hayatın gizliliği ve korunması. *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi, 2014*(3), 99-103. https://doi.org/10.18493/kmusekad.97442

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research*. Sage Publications.

Morgan, D. L. (1997). *Focus groups as qualitative research*. SAGE Publications. https://doi.org/10.4135/9781412984287

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage Publications.

Savaş, R. N., Zaim, A. H., & Aydın, M. A. (2020). KVKK ve GDPR kapsamında firmaların mevcut durum analizi üzerine bir inceleme. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 19*(38), 208-223.

Stewart, D. W., Shamdasani, P. N., & Rook, D. W. (2014). *Focus groups: Theory and practice*. Sage Publications.

Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. *PLOS Medicine, 15*(11), e1002689. https://doi.org/10.1371/journal.pmed.1002689

Yazıcıoğlu, M. B. (2024). ISO 27001, KVKK, and GDPR: A comparison of information security and data protection standards. *Journal of Engineering and Technology, 5*(1), 11-21.

Katkı Oranı Beyanı: Yazar çalışmayı tek başına gerçekleştirmiştir.
Destek ve Teşekkür Beyanı: Çalışmada herhangi bir kurum ya da kuruluştan destek alınmamıştır.
Çatışma Beyanı: Yazar herhangi bir çıkar çatışması olmadığını deklare etmektedir.

Bu çalışmada "Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi" kapsamında uyulması belirtilen kurallara uyulmuştur.

Bu makale benzerlik tespit yazılımlarıyla taranmıştır.