SAYIŞTAY DERGİSİ
JOURNAL OF TURKISH COURT OF ACCOUNTS

Cilt/Volume: 37
Sayı/Issue: 140
Mart/March 2026

ISSN: 1300-1981
eISSN: 2651-351X
Araştırma Makalesi/Research Article

# TÜRKİYE'DE KVKK DÜZENLEMELERİ ÇERÇEVESİNDE OTOMASYONA UYUM ALGISININ ANALİZİ

## *ANALYSIS OF PERCEPTIONS OF AUTOMATION COMPLIANCE WITHIN THE FRAMEWORK OF KVKK REGULATIONS IN TÜRKİYE*

**Sezer KAHYAOGLU**[1]
**Yenal ARSLAN**[2]
**Mustafa ÖZÇAKIR**[3]

**ÖZ**

Dijitalleşme sonucunda artan veri miktarı ve karmaşıklığı, kişisel verilerin korunmasında ve buna yönelik faaliyetlerin yönetilmesinde zorluklara neden olmaktadır. Bu zorlukların nedeni, Kişisel Verilerin Korunması Kanunu (KVKK) ile ilgili uyum süreçlerinin entegrasyonuna dayalı yeni bir kurumsal yapının oluşturulması gerekliliğidir. Otomasyon araçları, veriyi koruma ve mevzuata uyum süreçlerinde oluşturulan sistemlerin etkin çalışmasını belirleyen bir faktör olmaktadır. Çalışmada Türkiye'de KVKK'ya uyumda otomasyon araçlarının kullanım durumu ele alınmaktadır. KVKK düzenlemelerinde süreçte yer alan personelin kullanılan araç ve teknikleri benimsemesi ve kullanma eğilimini ölçmek ve bu bağlamda mevcut durumu analiz etmek amacıyla anket soruları hazırlanmıştır. Bu araştırmaya katılanların demografik özelliklerinin yanı sıra Likert ölçeğine göre tasarlanan sorular sorulmuştur. Elde edilen bulgular çerçevesinde sonuçlar literatüre dayalı olarak tartışılarak politika önerileri sunulmuştur. Çalışmada kullanılan analiz yöntemi ve KVKK uyum sürecine yönelik elde edilen bulgular çerçevesinde, düzenleyici kurumlara, süreçte görev alanlara ve araştırmacılara bilgi sağlayan bir kaynak olarak literatüre katkı sunulması hedeflenmektedir.

1- Doç. Dr., İzmir Bakırçay Üniversitesi, sbozkus@gmail.com, ORCID: 0000-0003-2865-3399
2- Doç. Dr., Ankara Yıldırım Beyazıt Üniversitesi, yenalarslan@aybu.edu.tr, ORCID: 0000-0002-1776-6091
3- Bağımsız Araştırmacı, Genel Müdür, mustafa.ozcakir@governid.com, ORCID: 0009-0002-0559-1199

**Gönderim/Submitted:** 11.08.2025 **Revizyon/Revised:** 12.03.2026 **Kabul/Accepted:** 12.03.2026

**Atıf/To Cite:** Kahyaoğlu, S., Arslan, Y. ve Özçakır, M. (2026). Türkiye'de KVKK Düzenlemeleri Çerçevesinde Otomasyona Uyum Algısının Analizi. Sayıştay Dergisi, 37(140), 65-96. https://doi.org/10.52836/sayistay.1762144

**ABSTRACT**

The increasing volume and complexity of data resulting from digitalization pose challenges for personal data protection and the management of related activities. These challenges necessitate the creation of a new institutional structure that integrates compliance processes with the Personal Data Protection Law (KVKK). Automation tools are a determining factor in the effective functioning of systems, considering data protection and regulatory compliance processes. This study examines the use of automation tools for KVKK compliance in Türkiye. Survey questions were prepared to measure personnel adoption and use of tools and techniques within the scope of the KVKK, and to analyze the current situation in this context. In addition to collecting participants' demographic characteristics, Likert-scale questions were prepared and asked. Based on the empirical findings, the results were discussed in relation to the relevant literature, and policy recommendations were presented. This study aims to contribute to the literature by serving as a resource for regulatory bodies, those involved in the process, and researchers through its analysis method and the findings reached regarding the KVKK compliance process.

**Anahtar Kelimeler:** Kişisel verilerin korunması, Veri yönetimi, Veri güvenliği, Random Forest, Teknoloji Kabul Modeli.

**Keywords:** Personal data protection, Data management, Data security, Random Forest, Technology Acceptance Model.

## GİRİŞ

Kişisel verilerin korunması, 21. yüzyılda dijital dönüşümün hızlanması ile birlikte temel siber güvenlik alanlarından biri haline gelmiştir (Tang, 2023; Savaş vd., 2020). Dijitalleşmenin yaygınlaşmasına bağlı olarak veri odaklı ekonominin yükselişi çerçevesinde, kişisel verilerin toplanması, işlenmesi ve aktarılması da benzeri görülmemiş bir hızla artmıştır. Bu durum, bireylerin temel hak ve özgürlüklerinin korunması, etik, özel hayatın gizliliği ve kişisel verilerin güvenliği gibi konularda kriminal durumların ve artan endişelerin ortaya çıkmasına yol açmıştır (Güdek, 2023). Bu endişeler, ulusal ve uluslararası düzeyde yasal düzenlemelerin yapılmasını zorunlu kılmıştır (Smith ve Johnson, 2020; Eroğlu, 2018).

Türkiye'de, Kişisel Verilerin Korunması Kanunu (KVKK), 7 Nisan 2016 tarihinde kabul edilmiş ve 2018 yılında tam olarak yürürlüğe girmiştir. KVKK, kişisel verilerin işlenmesinde uyulması gereken temel ilke ve kuralları belirleyerek, bireylerin kişisel verilerinin korunmasını sağlamayı amaçlamaktadır. Ancak, KVKK'ya uyum sağlamak, kurumlar için çeşitli işlevsel zorlukları beraberinde getirebilmektedir. Bu zorluklar, özellikle veri envanteri oluşturma, aydınlatma yükümlülüğünü yerine getirme, ilgili kişi başvurularını yanıtlama, veri güvenliğini

sağlama ve sürekli değişen yasal gerekliliklere uyum sağlama gibi alanlarda yoğunlaşmaktadır (Brown ve Green 2019; Demetzou, 2019; Güllebağatur, 2024). Veri birikimi ile işleme hızındaki artışla da bu sorunlar katlanarak artmaktadır.

Bu çalışma, Türkiye'de faaliyet gösteren kurumların Kişisel Verilerin Korunması Kanunu (KVKK) kapsamındaki uyum süreçlerinde karşılaştıkları zorlukları ve bu zorlukların ortaya çıkardığı sorun ve riskleri incelemeyi amaçlamaktadır. Çalışmada ayrıca söz konusu risklerin azaltılmasında otomasyon yazılımlarının potansiyel rolü, süreçlerde görev alan personelin tutum ve davranışlarına ilişkin eğilimler çerçevesinde değerlendirilmiştir. Bu kapsamda, araştırma konusuna ilişkin olarak hazırlanan anket aracılığıyla elde edilen veriler analiz edilmiştir. Elde edilen bulgular ve ilgili literatür çerçevesinde, kurumların kişisel verilerin korunmasına yönelik mevzuat ve düzenlemelere uyum süreçlerini daha etkin ve verimli bir şekilde yönetmelerinde önemli bir unsur olan süreç sahiplerinin tutum ve davranış eğilimlerinin ortaya konulması hedeflenmiştir.

## 1. LİTERATÜR TARAMASI

Ele alınan konu bağlamında literatür taraması iki kapsamda yapılmıştır. Bunlardan ilki, kişisel verilerin korunması ile ilgili ulusal ve uluslararası uygulamaların ortaya konması, literatüre dayalı güncel düzenleme bilgilerinin sunulmasıdır. İkincisi ise kişisel verilerin korunmasında süreç sahiplerinin otomasyona uyum algısını analiz etmek için kullanılan yöntem konusunda literatürdeki farklı yaklaşım, yöntem ve teknikleri araştırmak amacıyla gerçekleştirilmiştir.

### 1.1. KVKK ve Kişisel Verilerin Korunmasının Temel İlkeleri

Kişisel verilerin korunmasında yasal düzenlemelerin önemli bir etkiye sahip olduğu ve ülkelerin farklı yasal düzenlemelere sahip olduğu bilinmektedir. Avrupa Birliği'nde Avrupa Birliği Veri Koruma Tüzüğü (GDPR), ABD'de Tüketici Gizliliği Yasası (CCPA), İngiltere'de Veri Koruma Yasası, Kanada'da ise Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA) yürürlüktedir. Benzer şekilde Güney Kore'de ve Japonya'da Kişisel Bilgilerin Korunması Yasası ile Brezilya'da Genel Veri Koruma Yasası (LGPD) bulunmaktadır. Özellikle bu alanda veri gizliliği ile birlikte elektronik bilgi ve belgelerin korunmasına yönelik uygulamaların kurumsallaşması için ülkelerin yasal düzenlemeleri yakından takip ettiği gözlenmektedir (Tang, 2023; Demetzou, 2019; Güllebağatur, 2024). Türkiye'de de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile bu süreç yürütülmektedir.

KVKK, kişisel verilerin korunmasını temel bir hak olarak kabul etmekte ve bu hakkın Anayasa tarafından güvence altına alındığını belirtmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (Ersoy, 2019; Eroğlu, 2018). Bu bağlamda, KVKK, kişisel verilerin işlenmesinde uyulması gereken temel ilkeleri belirlemektedir (KVKK, 2016). Bu ilkeler KVKK'nın 4. maddesinde düzenlenen "kişisel verilerin işlenmesine ilişkin genel ilkeler" kapsamında yer almakta olup özet olarak aşağıdaki gibi ifade edilebilir:

- Hukuka ve dürüstlük kurallarına uygunluk: Kişisel veriler, hukuka uygun ve dürüstlük kurallarına uygun bir şekilde işlenmelidir.
- Belirli, açık ve meşru amaçlar için işlenme: Kişisel veriler, belirli, açık ve meşru amaçlar için işlenmelidir.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma: Kişisel veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalıdır.
- Doğru ve gerektiğinde güncel olma: Kişisel veriler, doğru ve gerektiğinde güncel olmalıdır.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme: Kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

### 1.2. Özel Nitelikli Kişisel Verilerin Korunması

KVKK, bazı kişisel verileri "özel nitelikli kişisel veriler" olarak nitelendirmekte ve bu verilere özel bir koruma sağlamaktadır. Özel nitelikli kişisel veriler, öğrenilmesi halinde ilgili kişilerin mağduriyetine veya ayrımcılığa uğramasına neden olabilecek nitelikteki verilerdir. Bu verilere örnek olarak kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri sayılabilir (KVKK, 2016; Bulut, 2020). KVKK, hassas kişisel verilerin işlenmesini daha sıkı koşullara tabi tutmakta ve bu verilerin ancak ilgili kişinin açık rızasıyla veya kanunda öngörülen özel durumlarda işlenebileceğini belirtmektedir.

### 1.3. Veri Sorumlusunun Yükümlülükleri

KVKK, kişisel verileri işleyen gerçek veya tüzel kişileri "veri sorumlusu" olarak tanımlamakta ve bu kişilere çeşitli yükümlülükler yüklemektedir. Veri

sorumlusunun temel yükümlülükleri şunlardır (KVKK, 2016; European Data Protection Supervisor, 2025; Eroğlu, 2018):

- Aydınlatma yükümlülüğü: Veri sorumlusu, kişisel verileri toplarken ilgili kişileri veri sorumlusunun kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve ilgili kişinin hakları konusunda bilgilendirmekle yükümlüdür.
- Veri güvenliğini sağlama yükümlülüğü: Veri sorumlusu, kişisel verilerin güvenliğini sağlamak için gerekli teknik ve idari tedbirleri almakla yükümlüdür. Bu tedbirler, veri kaybını, yetkisiz erişimi, veri ihlallerini ve diğer riskleri önlemeye yönelik olmalıdır.
- İlgili kişi başvurularını yanıtlama yükümlülüğü: Veri sorumlusu, ilgili kişilerin kişisel verilerine erişme, düzeltme, silme, anonim hale getirme veya itiraz etme gibi taleplerini değerlendirmek ve yasal süresi içinde yanıtlamakla yükümlüdür.
- Veri envanteri oluşturma yükümlülüğü: Veri sorumlusu, işlediği kişisel verilerin bir envanterini oluşturmak ve bu envanteri sürekli güncel tutmakla yükümlüdür. Veri envanteri, veri sorumlusunun hangi kişisel verileri, hangi amaçla, hangi yöntemlerle ve hangi süreyle işlediğini gösteren bir belgedir.

### 1.4. Veri Koruma Etki Analizi (DPIA)

Veri Koruma Etki Analizi (DPIA), kişisel veri işlemeyi içeren projelerin mahremiyet üzerindeki etkilerini değerlendirmek ve olumsuz etkileri önlemek için kullanılan bir süreçtir. DPIA, özellikle yeni teknolojilerin kullanımı, büyük ölçekli veri işleme faaliyetleri ve hassas kişisel verilerin işlenmesi gibi yüksek riskli durumlarda yapılması gereken bir analizdir (KVKK, Madde 6 ve General Data Protection Regulation -GDPR, Madde 35). DPIA, veri sorumlusunun veri işleme faaliyetinin risklerini belirlemesine, bu riskleri azaltmasına ve ilgili kişilerin haklarını korumasına yardımcı olur (Chhetri vd., 2022; European Data Protection Supervisor, 2025; Eroğlu, 2018). DPIA özellikle yeni teknolojilerin kullanıldığı, büyük ölçekli veri işleme faaliyetlerinin yürütüldüğü veya özel nitelikli kişisel verilerin işlendiği yüksek riskli durumlarda uygulanmaktadır (European Data Protection Supervisor, 2025).

Veri, işlenmesi gereken bir meta haline gelmekle birlikte kişilerin özellikle medeni haklarıyla kişi hakları çerçevesinde hassas bir bilgi haline gelmektedir. Dijitalleşen bir ortamda bu bilgilerin korunması sürekli denetim ve kontrolü gerekli kılmaktadır. Bu denetim ve kontrol, bilgilerin hassasiyetine bağlı olarak farklı fazlarda farklı frekanslarda sürekliliği de beraberinde getirmektedir. Denetim sisteminde özellikle denetim yapanların söz konusu yeni yapıda karşılaştıkları en önemli sorun her bir kontrol sürecinin ortaya çıkan teknolojik gelişmeyle birlikte daha karmaşık hale gelmesidir. Bu noktada denetim faaliyetlerinde eğilimlerin belirlenmesi sürece yönelik olarak genel ilginin analizi önemli hale gelmektedir (Eroğlu, 2018; Dülger, 2018; Çubukcu, 2024).

Veri Koruma Etki Analizi kavramı, GDPR'nin 35. maddesinde açıkça düzenlenmiş olmasına rağmen, KVKK'da doğrudan düzenlenmemiştir. Bununla birlikte, veri sorumlularının kişisel verilerin güvenliğini sağlamak amacıyla gerekli teknik ve idari tedbirleri alma yükümlülüğü (KVKK Madde 12) ve risk temelli yaklaşım çerçevesinde yapılan değerlendirmeler, uygulamada DPIA benzeri analizlerin yapılmasını teşvik eden bir çerçeve oluşturmaktadır. Ayrıca bu tür değerlendirmeler Kişisel Verileri Koruma Kurumu tarafından yayımlanan rehberlerde de dolaylı olarak ele alınmaktadır.

### 1.5. Otomasyonun KVKK Uyum Süreçlerindeki Rolü

Günümüz veri yoğun ortamında KVKK ve GDPR benzeri düzenlemeler, kurumların veri işleme faaliyetlerini yalnızca tanımlamakla kalmayıp bunları izlenebilir hesap verilebilir ve sürekli güncellenen bir mahremiyet yönetim programına dönüştürmelerini zorunlu kılmaktadır. Veri envanteri oluşturma, aydınlatma metinleri hazırlama, ilgili kişi (data subject) taleplerini karşılama, Veri Koruma Etki Analizi (DPIA) yürütme ve veri ihlallerini zamanında raporlama gibi süreçler teknik ve operasyonel kompleksliği önemli ölçüde artırmıştır. Bunun yanı sıra Türkiye'de veri koruma ekosistemi adına kritik bir eşik olan 07.09.2025 tarih ve 33010 sayılı Resmi Gazete'de yayımlanan 2026-2028 Orta Vadeli Programda KVKK'nın Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ile eş düzeye getirilmesi hedeflenmiştir. Bu yasal uyumlaştırma süreci, veri işleme standartlarını yükseltirken, uyum için gerekli olan teknik detayları ve operasyonel yükü de önemli ölçüde artırmıştır. Artan bu karmaşıklık, manuel yöntemlerin sürdürülebilirliğini zorlaştırmış ve otomasyonu bir tercih olmaktan çıkarıp, yasal uyumun sağlanabilmesi için zorunlu bir teknik altyapı haline getirmiştir. Otomasyon, KVKK uyum süreçlerini daha etkin, verimli ve uygun

maliyetli hale getirme potansiyeline sahiptir. Otomasyon araçları, veri keşfi ve sınıflandırma, veri envanteri oluşturma, aydınlatma metinleri hazırlama, ilgili kişi başvurularını yanıtlama, veri ihlallerini tespit etme ve raporlama gibi birçok süreçte kullanılabilir (Barati vd., 2020; Demetzou, 2019; KVKK, 2016). Literatür, bu alandaki karmaşıklığın manuel yöntemlerle sürdürülebilir olmadığını ve otomasyonun uyum maliyetlerini azaltma, operasyonel verimliliği artırma ve ihlal tespit/raporlama süreçlerini hızlandırmada kritik olduğunu göstermektedir (ENISA, 2016, Demetzou, 2019, Barati vd. 2020, Chhetri vd., 2022; Tang, 2023, Chatsuwan vd., 2023.).

Özetle kişisel veri koruma otomasyon uygulamalarının faydaları aşağıdaki şekilde sıralanabilir:

- Operasyonel verimliliği artırma: Otomasyon, manuel süreçleri azaltarak, çalışanların daha stratejik görevlere odaklanmasını sağlar.
- Uyum maliyetlerini düşürme: Otomasyon, insan hatalarını azaltarak ve süreçleri hızlandırarak, uyum maliyetlerini düşürür.
- Veri güvenliğini sağlama: Otomasyon, veri erişimini kontrol ederek, yetkisiz erişimi engeller ve veri güvenliğini artırır.
- Raporlama süreçlerini kolaylaştırma: Otomasyon, veri toplama ve analiz süreçlerini otomatikleştirerek, raporlama süreçlerini kolaylaştırır.

Ancak literatür aynı zamanda otomasyonun tek başına yeterli olmadığını; insan faktörü, kurumsal kültür, üst yönetim desteği ve çalışan eğitiminin de uyum başarısında belirleyici olduğunu vurgular. Dolayısıyla etkili bir mahremiyet yönetim programı, otomasyon teknolojilerini süreçlerle ve insan kaynakları kapasitesiyle bütünleştiren bir yaklaşım gerektirir (Tang, 2023; ENISA, 2016). Garner'ın 2022 yılında yayınladığı sektörel raporda (Gartner, 2022), modern teknoloji destekli mahremiyet programları, kurumun olgunluk seviyesine göre Kurulum (Establish), Sürdürme (Maintain) ve Geliştirme (Evolve) olmak üzere üç temel aşamada kategorize edilmektedir. Bu aşamalar ve içerdikleri teknolojik yetkinlikler şu şekilde detaylandırılabilir:

**1. Kurulum ve Yapılandırma Aşaması:** Uyum sürecinin temelini oluşturan bu aşama, Veri Keşfi (Discovery) ve Sınıflandırma teknolojileri ile kurum genelindeki verilerin tespit edilmesini kapsar. Tespit edilen bu veriler, Risk Haritalama çalışmalarına ve Veri İşleme Envanteri (ROPA) oluşturulmasına doğrudan girdi sağlar. Ayrıca, yasal Saklama Sürelerinin (Retention) tanımlanması, Aydınlatma Metinleri Yönetimi ve Açık Rıza ve Tercih Yönetimi (CPM) gibi fonksiyonlar bu aşamada devreye girmektedir.

**2. Sürdürme ve İşletme Aşaması:** Kurulan yapının sürekliliğini sağlayan bu aşamada, veri işleme faaliyetlerindeki değişikliklerin analiz edildiği Mahremiyet Etki Analizi (PIA) otomasyonları ve Amaç Bazlı Erişim Kontrolleri yer almaktadır. Özellikle veri sahiplerinin haklarını kullanmalarına olanak tanıyan İlgili Kişi Hakları Yönetimi (Subject Rights Management), manuel süreçlerde yaşanan zaman kayıplarını ve hata risklerini minimize etmek adına kritik bir öneme sahiptir.

**3. Geliştirme ve Evrilme Aşaması:** Uyumun ileri seviye tekniklerle güçlendirildiği bu aşamada, veri maskeleme, anonimleştirme ve mahremiyet mühendisliği (Privacy Engineering) gibi proaktif güvenlik önlemleri uygulanmaktadır.

Söz konusu fonksiyonların bir kurumda tekil olarak bulunması, etkin bir uyum yönetimi için yeterli değildir; asıl gereklilik bu fonksiyonların entegre bir şekilde çalıştırılmasıdır. Mahremiyet yönetiminde bir fonksiyonun çıktısı, çoğu zaman başka bir fonksiyonun girdisini oluşturmaktadır. Örneğin, "Veri Keşfi" aracıyla tespit edilen yeni bir veri seti, otomatik olarak "Veri Envanteri"ni (ROPA) güncellemeli; envanterdeki risk seviyesinin değişmesi ise "Aydınlatma Metni"ni veya "Etki Analizi" sürecini tetiklemelidir. Bu entegrasyon sağlanmadığında, her süreç için ayrı yazılımlar kullanılsa dahi veri tutarsızlıkları ve yoğun manuel iş yükü ortaya çıkmakta, sürdürülebilir bir uyum imkânsız hale gelmektedir.

Otomasyonun bir diğer kritik rolü ise, farklı disiplinler arasındaki "iletişim kopukluğunu" gidermesidir. KVKK uyum süreçlerinde yasal gereklilikleri ("ne yapılacağını") belirleyen hukuk birimleri ile bu gereklilikleri teknik altyapıda uygulayacak ("nasıl yapılacağını" belirleyen) bilişim teknolojileri birimleri arasında terminoloji ve metodoloji farklarından kaynaklanan derin bir anlayış boşluğu bulunmaktadır. Bütünleşik otomasyon platformları, hukuki gereksinimleri teknik kurallara dönüştürerek bu iki farklı disiplinin ortak bir dilde buluşmasını ve iş birliği yapmasını sağlayan bir köprü vazifesi görmektedir. Dolayısıyla otomasyon,

yalnızca operasyonel hızı artıran bir araç değil; yasal uyumun gerektirdiği karmaşık veri ilişkilerini yönetebilmek, disiplinler arası koordinasyonu sağlamak ve "kurumsal hafıza" oluşturmak için "olmazsa olmaz" (conditio sine qua non) bir şarttır.

### 1.6. Araştırma Metodolojisi

Çalışanların yeni teknolojileri veya araçları benimseme niyetini anlamak için sıklıkla kullanılan modellerden biri, Davis (1989) tarafından geliştirilen Teknoloji Kabul Modeli (TAM)'dir. Bu model, kullanıcıların bir teknolojiyi kabul etme niyetini, algılanan kullanışlılık ve algılanan kullanım kolaylığı gibi faktörlerle açıklar. Kişisel verilerin korunmasına yönelik araçların kullanımı, çalışanların bu araçları benimseme niyetine bağlıdır (Venkatesh ve Davis, 2000; Barati vd., 2020). Bu niyet, araçların kullanışlılığı, kullanım kolaylığı ve çalışanların bu araçlara yönelik tutumları gibi faktörlerle şekillenir. Çalışanların uyum araçlarını benimseme niyeti, kurumsal kültür ve liderlik tarzından da etkilenir. Destekleyici bir kurumsal kültür ve etkili liderlik, çalışanların bu araçları benimseme niyetini artırabilir (Schein, 2010; Kartal, 2018).

Kişisel verilerin korunmasına yönelik uyum araçları, yazılım çözümlerinden eğitim programlarına kadar geniş bir yelpazede yer alır. Bu araçlar, veri şifreleme, erişim kontrolü, veri ihlali tespiti gibi işlevleri yerine getirir (Anderson, 2020). Uyum araçlarının etkinliği, çalışanların bu araçları doğru ve etkili bir şekilde kullanmasına bağlıdır. Ancak, karmaşık araçların kullanımı, çalışanlar için zorluklar yaratabilir. Özellikle algoritmaların gelişimine dayalı yeni araçlar ve bunların kullanımına yönelik gereklilikler bir benimsemeyi yavaşlatmaktadır. Bu da uyum sürecini olumsuz etkileyebilir (Wilson ve Thompson, 2021; Kartal, 2018). Kişisel verilerin korunmasına yönelik mevzuata uyum, çalışanların farkındalığı ve eğitimiyle doğrudan ilişkilidir. Kurumsal eğitim programları, çalışanların uyum araçlarını benimseme niyetini artırabilir (PwC, 2018). Farkındalık etkileriyle birlikte ortaya çıkan gelişmeler, çalışanların kişisel verilerin korunması konusunda bilinçlenmesini sağlamaktadır. Bu kampanyalar, eğitim programlarıyla birlikte uygulandığında daha etkili sonuçlar verir (KPMG, 2019; Üstün ve Günal, 2020). Burada yeniliklerin öğrenilmesi kariyer açısından etkili olup, bu sürecin sürdürülebilir olması belirleyicidir.

## 2. VERİLER VE YÖNTEM

Bu araştırmada, karma yöntem (mixed methods) deseni kullanılmıştır. Karma yöntem deseni, nicel ve nitel araştırma yöntemlerinin bir arada kullanıldığı bir araştırma yaklaşımıdır. Bu yaklaşım, araştırma sorusunu daha kapsamlı bir şekilde anlamak ve daha zengin veri elde etmek için kullanılır. Anket verileri kategorik bir değişken olması ancak bunların sayısallaştırılarak kullanılmasına olanak veren bir teknikle analizlerin yapılması, çalışmayı literatür açısından farklı hale getirmektedir.

### 2.1. Araştırma Soruları

Bu çalışmanın temel araştırma soruları şunlardır:

- Türkiye'deki kurumların KVKK uyum süreçlerinde karşılaştıkları en önemli operasyonel zorluklar nelerdir?
- Otomasyon çözümleri, kurumların KVKK uyum süreçlerindeki operasyonel verimliliğini nasıl etkilemektedir?
- Kurumların KVKK uyum süreçlerinde güncelleme ve raporlama ihtiyaçları nelerdir?
- Kurumlar, hangi otomasyon araçlarını kullanmakta ve bu araçların etkililiğini nasıl değerlendirmektedir?
- KVKK uyum süreçlerinde karşılaşılan zorlukların üstesinden gelmek için kurumlar hangi stratejileri uygulamaktadır?

### 2.2. Veri Toplama Yöntemleri

Bu araştırmada, Türkiye'deki farklı sektörlerde faaliyet gösteren kurumlardan KVKK uyum süreçlerinden sorumlu kişilere yönelik bir anket uygulanmıştır. Anket, KVKK uyum süreçlerinde karşılaşılan zorluklar, otomasyon çözümlerinin kullanımı ve etkileri, güncelleme ve raporlama ihtiyaçları gibi konuları kapsamaktadır. Anket soruları, Likert tipi ölçekler, açık uçlu sorular ve çoktan seçmeli sorular içermektedir. Anket Google Forms uygulaması kullanılarak katılımcılara ulaştırılmıştır. Araştırma için hazırlanan anket soruları Akademik Etik Kurul onayı alınarak Likert Ölçeği'ne göre oluşturulmuştur. Soruların tam listesi Ek 1'de verilmiştir.

### 2.3. Örneklem

Bu çalışmada, Likert ölçeğine dayalı olarak tasarlanan anket verilerinden hareketle toplanan bilgiler kullanılarak belirli bir bağımlı değişkene (x10-KVKK

Süreç ve Envanter Yönetimi) göre ankette yer alan diğer bağımsız değişkenlerin önem sıralamasını ortaya koymak için "Random Forest" algoritması kullanılmıştır. Buna göre araştırmanın örneklemini, Türkiye'deki farklı sektörlerde faaliyet gösteren kurumlardan KVKK uyum süreçlerinden sorumlu 101 kişi oluşturmaktadır. Örneklemdeki kurumlar, kamu kurumları, büyük ölçekli şirketler ve küçük ve orta ölçekli işletmelere (KOBİ) kadar farklı büyüklükteki kurumları kapsamaktadır. Anket verileri, birinci aşamada istatistiksel analiz yöntemleriyle analiz edilmiştir. Frekans analizleri, ortalama analizleri, korelasyon analizleri ve regresyon analizleri kullanılarak, KVKK uyum süreçlerinde karşılaşılan zorluklar, otomasyon çözümlerinin etkileri ve diğer ilgili değişkenler arasındaki ilişkiler incelenmiştir. Buradan elde edilen bilgilere dayanarak KVKK'ya uyum kriterleri çerçevesinde değerlendirme yapılmış ve kurumların uyum düzeyleri tespit edilmeye çalışılmıştır.

### 2.4. Yöntem

Literatürde anket verileri genel olarak sosyal bilimler alanında farklı kullanıcı deneyimlerini ve algılarını analiz etmek amacıyla tercih edilmektedir. Anket katılımcılarının KVKK uyum ve denetim ile envanter yönetim sürecindeki tutum, algı ve deneyimlerini temsil eden cevaplarından oluşan vektörler arasındaki ilişkiye dayalı olarak her bir cevabın seçilen bağımlı değişkene göre önemi belirlenmiştir (Ek 1).

#### 2.4.1. Random Forest Yöntemini Kullanım Amacı ve Dayanağı

Bu çalışmada kullanılan yöntem, literatüre dayalı olarak belirlenmiş olup ankete katılanların KVKK mevzuatına uyum denetimi ve envanter yönetim sürecindeki tutum ve davranışlarını belirlemek ve bu davranışlara etki eden temel faktörleri ortaya koymak için "Random Forest" algoritması tercih edilmiştir. Bu tür anket verilerinden anlamlı içgörüler elde etmek için, doğru istatistiksel yöntemlerin uygulanması esastır. "Random Forest" algoritmasının tercih edilmesinin nedeni, ele alınan konuya yönelik belirlenen bağımlı değişkenin önemini belirlemede güçlü ve yaygın olarak kullanılan bir makine öğrenmesi tekniğine dayanmasıdır. Random Forest yöntemi, çoklu karar ağacından hareketle bir araya getirilerek oluşturulan bir topluluk (ensemble) öğrenmesi algoritmasına dayalı yaklaşımdır. Söz konusu algoritmayla eğitilen parametreler yoluyla tek bir karar ağacı yerine çoklu karar ağaçlarının kullanılmasıyla daha iyi bir genelleme yapabilmektedir. Bu yaklaşımla, uygulamada her bir ağacın

tek başına yapabileceği hataların azaltılmasına dayalı olarak gerçeğe yakın ve dengeli tahminleme yapılmaktadır. Böylece hem sınıflandırma yapılabilir hem de regresyona dayalı analizler yapılabilmektedir (Biau, 2012; Haddouchi ve Berrado, 2024).

Çalışmamızda ele alınan her bir değişken kategorik (faktör) veya sayısal değişken olarak kullanılarak analizler yapılmıştır. Bu yaklaşımda verinin dağılımı veya değişkenler arası ilişkilerin doğrusallığı gibi katı varsayımlar gerekmemektedir. Burada kullanılan makine öğrenmesi tekniğiyle birlikte, bundan sonra yapılacak çalışmalarda aynı anketin kullanılması durumunda farklı örneklemlerden gelen bilginin karşılaştırılması mümkün hale gelmektedir (GeeksforGeeks, 2025).

#### 2.4.2. Veri Seti ve Analize Hazırlık İşlemleri

Araştırma için hazırlanan anket soruları Likert ölçeğine dayalı metinsel ifadelerden oluşmaktadır (Ek 1). Bundan dolayı öncelikli olarak anket verilerinin analize uygun hale getirilmesi amacıyla sayısal dönüşümü yapılmış; nicel analiz ve modelleme için uygun hale getirilmiştir.

İkinci aşamada anket verileri içerisinde katılımcıların yanıtlamadığı, boş bıraktığı sorular (NA) için işlem yapılmıştır. Buna göre sayısal değerlerden hareketle, ilgili sütundaki ortalama değer alınarak boşluklar doldurulmuştur. Kategorik (Faktör) değişkenler için de en sık tekrar eden değişken ilgili sütundaki boşluklara eklenmiştir. Bu yaklaşım literatürde tercih edilen bir yol olarak veri kaybını önlerken, aynı zamanda modelin sağlamlığını ve doğruluğunu artırmaya katkı sağlamaktadır.

Bu çalışmada bağımlı değişken (x10-KVKK Süreç ve Envanter Yönetimi), hem sayısal olarak regresyona (regression) dayalı hem de faktör olarak sınıflamaya (classification) dayalı yaklaşımın esas alındığı iki modelleme tekniğine göre hesaplanmıştır. Elde edilen sonuçların kendi içinde tutarlı olduğu görülmüştür (Tablo 1, Tablo 2, Tablo 3, Tablo 4).

#### 2.4.3. Random Forest Algoritması Yoluyla Uygulama

Random Forest modeli karar ağaçları topluluğuna dayalı olarak bağımlı değişkenin yapısına göre hem sınıflamada hem de regresyon analizlerinde yaygın olarak kullanılan güçlü bir makine öğrenmesi algoritmasıdır. Likert ölçeğine dayalı anket verileri genellikle sıralı olduğundan sınıflamaya dayalı ve sıralı regresyon yöntemi biçiminde uygulanabilmektedir.

Çalışmamızda "x10-KVKK Süreç ve Envanter Yönetimi" bağımlı değişkeninin önemini belirlemek için R programında ilgili kütüphaneler kullanılarak Random Forest algoritmasıyla x10 bağımlı değişken için söz konusu parametreler eğitilmiştir. Random Forest algoritması modelin performansını düşüren veya Gini katsayısını azaltan değişkenlerin sıralamasına göre sonuçları vermektedir. Buna literatürde "mean decrease accuracy" veya "mean decrease Gini" teknikleri denmektedir (Boulesteix vd., 2012). Burada bir değişkenin modelden çıkarılmasının veya rastgele yerinin değiştirilmesinin önem derecesine ne kadar etkisi olduğundan hareketle önem derecesini belirlemektedir. Ulaşılan sonuçlarda bağımsız veya etki faktörlerinin bağımlı değişkendeki düşüşe etkisi ne kadar fazla olursa, öneminin o kadar fazla olacağı kabul edilmektedir (Haddouchi ve Berrado, 2024; Athey vd., 2019).

Analiz sonuçlarımızda x10-KVKK Süreç ve Envanter Yönetimi bağımlı değişkeni üzerinde en fazla önemi olandan en az önemi olana doğru bağımsız değişkenlerin sıralaması yapılmaktadır. Bu sıralamaya esas olan değişkenlerin katsayısı bazen pozitif bazen de negatif çıkmıştır. Pozitif ve yüksek skora sahip olan değişkenler, bağımlı değişken üzerinde etkisinin yüksek olduğunu ve modelin açıklama gücüne olumlu katkısı olduğunu ifade eder. Değişkenin katsayısı negatif ise, modelde etkisinin çok az olduğuna ve modelin performansına olumsuz etkisi olduğuna yönelik bilgi sağlar (Athey vd., 2019). Özellikle negatif katsayısı olan değişkenlerin etkisi bunların çıkarılması veya daha detaylı incelemesi yapılmasını gerekli kılar. Random Forest algoritmasına dayalı analizleri yaklaşımlar önemli ve önemsiz ayrımının yapılmasına ve karar alma süreçlerinde uygun stratejinin belirlenmesini sağlarken sistemin bütününü temsil edebilecek bilginin çıkarılmasını olanaklı kılar (Biau, 2012).

#### 2.4.4. Random Forest Algoritmasının Yorumu

Random Forest algoritmasına dayalı elde edilen bulguların yorumlanmasında aşağıdaki hususlara dikkat edilmesi gereklidir.

Birincisi, sıralamanın anlamını ve yorumlanmasını içermektedir. Tablo halinde veya grafik olarak sunulan sıralama büyükten küçüğe doğru olmaktadır. Bu sıralama "önem=importance" skorunu esas almaktadır. Modelimizde x10-KVKK Süreç ve Envanter Yönetimi ile olan ilişkisini ortaya koyan bağımsız değişkenlerin arasında listede en üst sırada olanların x10'u tahmin etmede en önemli olanlardan oluştuğunu göstermektedir.

İkincisi, önem katsayısının anlamını ve yorumlanmasını ifade etmektedir. Önem=importance değeri, ilgili modelde sütun olarak "mean decrease accuracy" değerini temsil etmektedir. Bu değerin yorumu, ilgili değişkenin modelden çıkarılması halinde x10'na (KVKK Süreç ve Envanter Yönetimi) olan etkisi ve doğru sınıflama olasılığına ortalama olarak ne kadar etki ettiğinin belirlenmesini sağlamaktadır. Söz konusu bağımsız değişken olmadan tahmin doğruluğunun ortalama olarak ne kadar düşüş gösterebileceğini analiz etmemize yardımcı olmaktadır. Bu değer yükseldikçe model kategorilerini veya sınıflamasını belirlemedeki önemi artmaktadır (Haddouchi ve Berrado, 2024; Athey vd., 2019).

Üçüncüsü katsayıların işaretlerinin pozitif veya negatif olmasına göre yorumlanmasını ifade etmektedir. Pozitif değerli olan değişkenlerin modelin açıklama gücüne etkisi olumlu iken, negatif değerli olan değişkenlerin modelin performansına olumsuz etki ettiği ve gürültüye neden olduğu söylenebilir. Modelin tahmin doğruluğu ve açıklama gücü açısından değişkenlerin katsayılarına dikkat edilmesi gereklidir (Biau, 2012; Biau vd., 2008).

Burada dikkat edilmesi gereken nokta, modelde yer alan pozitif katsayılı değişkenlerin modelin içindeki ilişkilerin ve sınıflandırmanın yorumlanmasında esas oluşturan faktörler olarak görülebileceğidir. Ancak bu değişkenler arasındaki doğrudan bir nedensellik ilişkisinin yorumlanması için kullanılması uygun değildir (Biau, 2012; Boulesteix vd., 2012).

## 3. ANKETE KATILANLARIN EĞİLİMLERİ VE RANDOM FOREST ALGORİTMASINA DAYALI BULGULAR

Çalışmada toplanan anket verilerinden elde edilen katılımcı eğilimi ve kısa yorumu ve Random Forest ile elde edilen modellerin istatistiksel olarak anlamlı bulunan değişkenlerin yorumu aşağıda sırasıyla verilmiştir.

### 3.1. Anket Sonuçları

Anket verilerinden hareketle elde edilen temel bulguların genel değerlendirmesi aşağıda özet olarak sunulmaktadır.

#### 3.1.1. KVKK Uyum Sürecinde Envanter Yönetiminin Rolü

Anket sonuçları, katılımcıların %85'inin KVKK uyum sürecinde veri envanteri yönetiminin kritik bir öneme sahip olduğunu düşündüğünü göstermektedir. Katılımcılar, veri envanteri yönetiminin, hangi kişisel verilerin işlendiğini belirlemek,

riskleri değerlendirmek ve uygun güvenlik tedbirlerini almak için gerekli olduğunu belirtmişlerdir. Ancak, katılımcıların %60'ı veri envanteri oluşturma ve güncelleme süreçlerinde zorluklar yaşadıklarını ifade etmişlerdir. Bu zorluklar, veri toplama, veri sınıflandırma, veri sahiplerini belirleme ve veri işleme amaçlarını tanımlama gibi konularda yoğunlaşmaktadır.

#### 3.1.2. İlgili Kişi Başvurularının Yönetimi

Anket sonuçları, katılımcıların %70'inin ilgili kişi başvurularını manuel olarak yönettiğini göstermektedir. Katılımcılar, bu süreçte veri toplama, doğrulama, yasal değerlendirme ve yasal süre içinde yanıt verme gibi aşamalarda zorluklar yaşadıklarını belirtmişlerdir. Özellikle, karmaşık başvuruların değerlendirilmesi, farklı departmanlardan bilgi toplama ve yasal sürelere uyum sağlama gibi konularda sıkıntılar yaşandığı görülmüştür. Katılımcıların %40'ı ilgili kişi başvurularını yanıtlama süresinin ortalama 1 haftadan uzun sürdüğünü ifade etmişlerdir.

#### 3.1.3. Otomasyon, Güncelleme ve Raporlama İhtiyaçları

Anket sonuçları, katılımcıların %90'ının kişisel veri envanteri yönetiminde sürekli güncelleme, raporlama ve kullanıcı dostu arayüz özelliklerinin olmazsa olmaz olduğunu düşündüğünü ortaya koymaktadır. Katılımcılar, yasal düzenlemelerdeki değişiklikleri takip etmek, veri işleme faaliyetlerindeki güncellemeleri yansıtmak ve düzenli raporlar oluşturmak için bu özelliklerin gerekli olduğunu belirtmişlerdir. Ayrıca, katılımcıların %80'i veri güvenliği ihlallerini tespit etme ve raporlama süreçlerinde otomasyonun önemli olduğunu vurgulamışlardır.

#### 3.1.4. Çözüm Kullanımı ve Otomasyon Araçlarının Etkisi

Anket sonuçları, katılımcıların %50'sinin KVKK uyum süreçlerinde otomasyon araçları kullandığını göstermektedir. Otomasyon araçları kullanan katılımcılar, bu araçların özellikle veri envanteri yönetimi, ilgili kişi başvurularının işlenmesi ve aydınlatma metinlerinin hazırlanması gibi süreçlerde önemli faydalar sağladığını belirtmiştir. Katılımcılar ayrıca otomasyon araçlarının operasyonel verimliliği artırdığını, uyum maliyetlerini düşürdüğünü ve veri güvenliği yönetimini desteklediğini ifade etmiştir. Bununla birlikte katılımcıların %75'i, ilgili kişi başvurularının otomasyon araçları aracılığıyla dakikalar içinde işlenebilmesinin operasyonel verimlilik üzerinde önemli bir etkisi olacağını belirtmiştir.

Çalışmada kullanılan anket sorularında katılımcıların kullandıkları otomasyon araçlarının türü, teknik özellikleri veya veri güvenliğini ne ölçüde sağlayabildiğine ilişkin ayrıntılı bilgiler toplanmamıştır. Bu durum çalışmanın önemli sınırlılıklarından birini oluşturmaktadır. Özellikle kişisel verilerin korunması alanında artan dijitalleşme ile birlikte kullanılan otomasyon çözümlerinin veri güvenliği ve mahremiyet açısından yeni riskler doğurabileceği literatürde de vurgulanmaktadır. Bu bağlamda otomasyon araçlarının kullanımı, KVKK kapsamındaki uyum süreçlerinin yönetilmesine katkı sağlayabilmekle birlikte, kullanılan teknolojinin niteliği ve güvenlik standartları açısından dikkatle değerlendirilmesi gereken bir alan oluşturmaktadır. Özellikle otomasyon sistemlerinin veri işleme faaliyetlerini merkezi hale getirmesi, veri erişim yönetimi, algoritmik karar süreçleri ve veri güvenliği kontrolleri gibi konularda yeni risk alanları yaratabilmektedir. Bu nedenle gelecekte yapılacak araştırmalarda otomasyon araçlarının türleri, teknik mimarileri ve veri güvenliği üzerindeki etkilerinin daha ayrıntılı şekilde incelenmesi önem taşımaktadır.

### 3.2. Random Forest Algoritması ile Elde Edilen Bulgular

Çalışmamızda x10-KVKK Süreç ve Envanter Yönetimi bağımlı değişkeninin Random Forest algoritmasına dayalı makine öğrenmesi çerçevesinde eğitilen bulguları iki temel varsayım altında verilmiştir. Birincisinde x10 bağımlı değişkeni sayısal değerine göre, ikincisinde ise x10 bağımlı değişkeninin faktörel analizine göre sıralamalar hesaplanmıştır. Her iki modelden elde edilen ampirik bulgular sırasıyla Tablo 1, Tablo 2, Tablo 4 ve Tablo 5'te gösterilmektedir.

Tablo 1 ve Tablo 2'de önem sıralamasına bakıldığında, x10 bağımlı değişkenin sayısal olarak hesaplanmasından elde edilen sonuçlara göre en yüksek etki derecesine sahip olan pozitif değere sahip x9, x11 ve x12'dir. Bunların karşılık geldiği cevaplara göre değerlendirildiğinde, veri sınıflaması (x9), sistem ve kaynak uyumu (x11) ile otomasyon eksikliği (x12) en fazla ilişkili olan değişkenlerdir. KVKK mevzuatına uyum ile ilgili yapılan denetimlerin etkinliğini ve verimliliğini artırmak ve bu süreci doğru biçimde yönetmek için gerekli olan belirleyici faktörlerin veri sınıflaması ile birlikte sistem ve kaynak uyumu ile otomasyon eksikliğinin giderilmesine bağlıdır.

**Tablo 1 ve Tablo 2:** Random Forest Modeli Önem Sıralaması

| Tablo 1: x10 sayısal ve diğer değişkenler faktör | | Tablo 2: Tüm değişkenler sayısal | |
|---|---|---|---|
| **Önem** | **Değişken** | **Önem** | **Değişken** |
| 22.7992 | x9 | 25.8342 | x9 |
| 15.5313 | x12 | 14.5845 | x11 |
| 14.4884 | x11 | 14.2173 | x12 |
| 5.4187 | x20 | 4.5828 | x31 |
| 5.0983 | x36 | 4.3056 | x20 |
| 4.5417 | x13 | 4.1355 | x34 |
| 3.7074 | x14 | 3.8161 | x35 |
| 3.0899 | x33 | 3.6884 | x29 |
| 2.9036 | x29 | 3.4129 | x13 |
| 2.8897 | x37 | 3.2245 | x17 |
| 2.8078 | x17 | 2.8845 | x14 |
| 2.6794 | x35 | 2.8041 | x36 |
| 2.5650 | x26 | 2.7637 | x24 |
| 2.3828 | x34 | 2.5905 | x33 |
| 2.2089 | x23 | 2.4900 | x15 |
| 2.0979 | x15 | 2.4701 | x32 |
| 1.9715 | x31 | 2.4440 | x23 |
| 1.9215 | x28 | 2.0126 | x37 |
| 1.7764 | x32 | 1.7917 | x21 |
| 1.6838 | x24 | 0.8976 | x25 |
| 1.6703 | x25 | 0.8137 | x2 |
| 1.6289 | x27 | 0.6007 | x28 |
| 1.2587 | x21 | 0.3600 | x22 |
| 1.2275 | x2 | 0.3542 | x26 |
| 1.2035 | x30 | 0.2331 | x30 |
| 0.8903 | x7 | 0.1887 | x27 |
| 0.4260 | x1 | -0.0175 | x1 |
| 0.3042 | x22 | -0.3610 | x16 |
| 0.2863 | x19 | -1.1523 | x19 |
| 0.1210 | x16 | -1.1724 | x18 |
| -0.1200 | x8 | -1.2601 | x4 |
| -0.7172 | x3 | -2.2751 | x3 |
| -0.9565 | x18 | -2.3659 | x7 |
| -1.1808 | x4 | -2.7044 | x8 |

**Kaynak:** Yazarlar tarafından hazırlanmıştır.

Tablo 4 ve Tablo 5'teki bulgulara bakıldığında, x10 bağımlı değişken veya diğer tüm değişkenler faktörel olarak modellendiğinde, elde edilen önem sıralamasında x9, x11, x12, x14, x17, x34 ve x35 etki eden ve önemli olan faktörleri ifade etmektedir. X10 faktör olarak modellendiğinde önemli hale gelen değişkenlerin sayısı artmaktadır. Bunlar, veri sınıflaması (x9), sistem ve kaynak uyumu (x11), otomasyon eksikliği (x12), envanter yönetiminin rolü (x14), KVKK entegrasyon sorunu (x17), veri toplama ve doğrulama zorluğu (x34) ile Yasal değerlendirme ve uyum kontrolleri zorluğu (x35) olarak belirlenmiştir.

Araştırma bulguları, Türkiye'deki kurumların KVKK uyum süreçlerinde çeşitli operasyonel zorluklarla karşılaştığını ve dijital otomasyon çözümlerinin bu zorlukların yönetilmesinde önemli bir rol oynayabileceğini göstermektedir. Özellikle veri envanteri yönetimi, ilgili kişi başvurularının işlenmesi ve yasal yükümlülüklerin takibi gibi süreçler kurumlar açısından önemli operasyonel yükler oluşturmaktadır (Chhetri vd., 2022; Chatsuwan vd., 2023). Bu bağlamda literatürde veri koruma uyum süreçlerini desteklemek amacıyla kullanılan otomasyon çözümleri genel olarak şu kategoriler altında ele alınmaktadır (Tablo 3):

**Tablo 3:** Veri Koruma Uyum Süreçlerini Desteklemek Amacıyla Kullanılan Otomasyon Çözümleri

| Veri Envanteri ve Veri Haritalama Yazılımları: | Veri Koruma Yönetim Platformları (Privacy Management Platforms): | İlgili Kişi Başvuru Yönetim Sistemleri: | Veri İhlali İzleme ve Raporlama Sistemleri: |
|---|---|---|---|
| • Kurumların işledikleri kişisel verileri tespit etmelerine, veri akışlarını izlemelerine ve veri envanterlerini güncel tutmalarına yardımcı olan sistemlerdir. | • Aydınlatma metinlerinin yönetimi, açık rıza süreçleri ve veri işleme faaliyetlerinin kayıt altına alınması gibi süreçleri merkezi olarak yöneten yazılımlardır. | • Veri sahiplerinin erişim, düzeltme, silme veya itiraz taleplerini kayıt altına alan ve yanıt süreçlerini otomatikleştiren dijital platformlardır. | • Veri ihlallerini tespit eden, risk analizleri gerçekleştiren ve raporlama süreçlerini destekleyen güvenlik araçlarıdır. |

**Kaynak:** OECD (2023).

Bu tür otomasyon çözümleri, kurumların KVKK kapsamındaki yükümlülüklerini daha sistematik şekilde yerine getirmelerine katkı sağlayabilmektedir. Bununla birlikte çalışmada kullanılan anket verilerinde katılımcıların kullandıkları otomasyon araçlarının teknik özellikleri veya marka/ürün bazında detayları sorgulanmamıştır. Bu nedenle mevcut çalışmada otomasyon çözümleri genel bir kavramsal çerçeve içinde değerlendirilmiştir.

Özellikle veri envanteri yönetiminde yaşanan zorluklar dikkate alındığında, veri akışlarının izlenmesini ve veri işleme faaliyetlerinin kayıt altına alınmasını sağlayan otomasyon araçlarının uyum süreçlerini kolaylaştırabileceği

değerlendirilmektedir. Bununla birlikte kullanılan otomasyon sistemlerinin veri güvenliği standartları, erişim kontrol mekanizmaları ve denetim izleri gibi özelliklerinin kişisel verilerin korunması açısından kritik öneme sahip olduğu açıktır. Bu nedenle gelecekte yapılacak çalışmalarda farklı otomasyon araçlarının teknik özellikleri ve veri güvenliği üzerindeki etkilerinin daha ayrıntılı biçimde incelenmesi önemli bir araştırma alanı olarak ortaya çıkmaktadır.

**Tablo 4 ve Tablo 5:** Random Forest Modeli Önem Sıralaması

| **Tablo 4: x10 faktör ve diğer değişkenler sayısal** | | **Tablo 5: Tüm değişkenler faktörel** | |
|---|---|---|---|
| **Önem** | **Değişken** | **Önem** | **Değişken** |
| 17.4006 | x9 | 13.4756 | x9 |
| 12.9708 | x11 | 9.7014 | x12 |
| 12.8173 | x12 | 9.6804 | x11 |
| 8.6748 | x17 | 8.1135 | x17 |
| 7.5109 | x34 | 5.8500 | x35 |
| 6.3956 | x14 | 4.7168 | x13 |
| 4.4442 | x35 | 4.5569 | x19 |
| 4.3413 | x13 | 4.1013 | x34 |
| 3.9126 | x15 | 4.0728 | x37 |
| 3.6960 | x36 | 3.6985 | x29 |
| 3.2534 | x29 | 3.3373 | x28 |
| 3.1751 | x31 | 3.2943 | x15 |
| 3.1694 | x33 | 3.2218 | x33 |
| 3.0102 | x37 | 3.0429 | x23 |
| 2.7484 | x21 | 3.0249 | x36 |
| 2.4891 | x19 | 2.9694 | x14 |
| 2.4074 | x26 | 2.9318 | x26 |
| 1.9945 | x23 | 2.2334 | x32 |
| 1.7813 | x25 | 1.9202 | x21 |
| 1.6628 | x20 | 1.5980 | x31 |
| 1.2858 | x16 | 1.4211 | x16 |
| 1.1624 | x28 | 0.4905 | x8 |
| 0.8603 | x30 | 0.1915 | x22 |
| 0.6605 | x2 | 0.0858 | x30 |
| 0.5341 | x32 | -0.0344 | x25 |
| 0.5152 | x1 | -0.0662 | x20 |

| Tablo 4: x10 faktör ve diğer değişkenler sayısal | | Tablo 5: Tüm değişkenler faktörel | |
|---|---|---|---|
| **Önem** | **Değişken** | **Önem** | **Değişken** |
| 0.3625 | x7 | -0.4451 | x2 |
| 0.0499 | x8 | -0.7075 | x7 |
| -0.0976 | x3 | -0.7217 | x24 |
| -0.2177 | x18 | -0.7938 | x27 |
| -0.5791 | x27 | -0.8955 | x18 |
| -0.7303 | x22 | -1.0860 | x4 |
| -0.8490 | x4 | -1.9978 | x3 |
| -0.8831 | x24 | -2.0779 | x1 |

**Kaynak:** Yazarlar tarafından hazırlanmıştır.

Araştırma sonuçları, literatürdeki diğer çalışmaları da desteklemektedir. Örneğin, yapılan bir araştırmada, KOBİ'lerin KVKK uyum süreçlerinde en büyük zorlukları, maliyet, teknik bilgi eksikliği ve zaman kısıtlaması olarak belirlenmiştir. Bu araştırmada da otomasyon çözümlerinin KOBİ'lerin uyum maliyetlerini düşürmede ve süreçleri hızlandırmada önemli bir rol oynayabileceği vurgulanmıştır (Dülger, 2021; Dülger, 2018; ENISA, 2016).

Araştırma bulguları, aynı zamanda KVKK uyum süreçlerinde insan faktörünün önemli bir rol oynadığını göstermektedir. Çalışanların eğitimi, farkındalığı ve motivasyonu, uyum süreçlerinin başarısı açısından kritik öneme sahiptir (Chatsuwan vd., 2023). Bu bağlamda kurumların yalnızca teknolojik otomasyon çözümlerine yatırım yapmaları yeterli olmayıp, aynı zamanda çalışanların veri koruma süreçlerine ilişkin bilgi ve becerilerini geliştirmeleri de gerekmektedir. Özellikle dijital otomasyon araçlarının yaygınlaşmasıyla birlikte çalışanların teknoloji okuryazarlığı ve dijital becerilerinin artırılması önem kazanmaktadır. Teknoloji okuryazarlığı; çalışanların veri koruma süreçlerinde kullanılan dijital araçları anlayabilme, doğru şekilde kullanabilme ve veri güvenliği risklerini değerlendirebilme yetkinliğini ifade etmektedir. Bu yetkinliklerin geliştirilmesi, kurumlarda sürdürülebilir bir veri koruma kültürünün oluşturulmasına katkı sağlamaktadır. Bu çerçevede veri koruma yönetimi yalnızca teknolojik çözümlerle değil, aynı zamanda insan kaynağının dijital yetkinliklerinin geliştirilmesi ve kurum içinde veri koruma farkındalığının artırılması ile desteklenmelidir (ENISA, 2016; Mobofis, 2025; Dülger, 2021). Ayrıca bu süreçler KVKK kapsamında veri sorumlularının veri güvenliğini sağlamak için gerekli teknik ve idari tedbirleri alma yükümlülüğü ile de ilişkilidir.

## 4. TARTIŞMA

Araştırmanın bulgularından hareketle; KVKK uyum süreçlerinde karşılaşılan zorlukların üstesinden gelmek ve otomasyon çözümlerinin potansiyelini en üst düzeye çıkarmak için aşağıdaki stratejik politika önerileri sunulmaktadır:

***Veri envanteri yönetimini otomatikleştirme:*** Veri envanteri oluşturma ve güncelleme süreçlerini otomatikleştirerek, zaman ve maliyet tasarrufu sağlamak önemlidir. Bunun için mevcut iş süreçlerinin gözden geçirilmesi ve var olan sisteme ek modüllerin entegrasyonu ile bütüncül yaklaşım geliştirilmesi önerilmektedir.

***KVKK başvuru işleme süreçlerini optimize etme:*** İlgili kişi başvurularını toplama, doğrulama, değerlendirme ve yanıtlama süreçlerini otomatikleştirerek, yasal sürelere uyum sağlamaya dönük tedbirlerin alınması gereklidir. Operasyonel süreçlerin etkinliği ve verimliliğini sağlamak için başvuru işleme sürecinin baştan sona ele alınması, kontrol noktalarının oluşturulması sağlanmalıdır. KVKK başvuru işleme süreçleri, ilgili kişilerin (veri sahiplerinin) kişisel veri ile ilgili haklarını kullanmalarına ilişkin taleplerinin sistematik olarak ele alınmasına ilişkin olup, bu süreçlerin farklı aşamaları için ön plana çıkan hususlar şu şekildedir:

1. Başvuru toplama: Veri sahiplerinin erişim, düzeltme, silme, işlemeyi kısıtlama veya itiraz taleplerinin alınması. Başvuruların farklı kanallardan (e-posta, web portal, fiziksel başvuru vb.) toplanması gerekebilir.

2. Başvuruların doğrulanması: Başvuran kişinin kimliğinin teyit edilmesi, yetkisiz erişim veya yanlış taleplerin önlenmesi kritik önem taşımaktadır.

3. Başvuruların değerlendirilmesi: Talebin KVKK kapsamında uygunluğu ve işleme prosedürleri açısından incelenmesi gereklidir. Bu aşamada hangi verilerin etkilendiği ve hangi birimlerin işlem yapacağı belirlenir.

4. Başvuruların yanıtlanması: Talebin kabul edilmesi veya reddedilmesi durumunda veri sahibine resmi yanıt verilmesi gereklidir. Yanıt sürecinde yasal sürelerin (ör. KVKK Madde 13) dikkate alınması önemli olmaktadır.

5. Kayıt ve raporlama: İşlem süreçlerinin ve sonuçlarının merkezi olarak kaydedilmesi, yönetim raporlarına ve denetim süreçlerine entegre edilmesi gereklidir.

Bu süreçlerin otomasyon araçları ile optimize edilmesi, başvuruların daha hızlı, doğru ve yasal sürelere uygun şekilde işlenmesini sağlayabilir. Örneğin,

başvuru toplama ve kimlik doğrulama adımları otomatikleştirilebilir, yanıt şablonları ve raporlama sistemleri ile süreçler standartlaştırılabilir. Operasyonel etkinliğin sağlanması için süreç boyunca kontrol noktalarının ve izleme mekanizmalarının oluşturulması kritik öneme sahiptir.

***Veri güvenliği ihlallerini tespit etme ve raporlama süreçlerini otomatikleştirme:*** Veri güvenliği ihlallerini otomatik olarak tespit eden ve raporlayan sistemler kurarak, riskleri erken teşhis etmek ve azaltmak için gerekli koordinasyonun sağlanması önerilmektedir. Bu uygulama kurumların kişisel veri işleme faaliyetlerinde ortaya çıkabilecek riskleri erken aşamada tespit edebilmesi açısından önemli bir mekanizma olarak değerlendirilmektedir. Bu kapsamda veri ihlallerini otomatik olarak izleyen ve raporlayan sistemlerin kurulması; veri erişim hareketlerinin izlenmesi, anormal veri akışlarının tespit edilmesi ve ihlal durumlarında hızlı müdahale mekanizmalarının devreye alınması açısından önemli katkılar sağlayabilmektedir. Bununla birlikte bu tür sistemlerin kendileri de dijital altyapılara dayandığından, veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin uygulanması kritik önem taşımaktadır. Bu çerçevede iç kontrol standartları ile uyumlu olarak alınabilecek başlıca önlemler şu şekilde ifade edilebilir (KVKK, Madde 12):

1. Erişim kontrol mekanizmaları: Yetkisiz veri erişimini önlemek amacıyla rol tabanlı erişim kontrollerinin uygulanması önemlidir.

2. Şifreleme ve veri maskeleme teknikleri: Hassas verilerin depolama ve iletim aşamalarında korunmasını sağlamak amacıyla kriptografik yöntemlerin kullanılması koruyucu özellik taşımaktadır.

3. Güvenlik izleme ve log yönetimi: Sistem üzerinden gerçekleşen işlemlerin kayıt altına alınması ve olası ihlallerin erken tespit edilmesi için izleme mekanizmalarının oluşturulması gereklidir.

4. Olay müdahale ve ihlal bildirim prosedürleri: Veri ihlali durumunda hızlı müdahale edilmesini sağlayan kurumsal süreçlerin oluşturulması ve buna yönelik iş süreçlerinin oluşturulması gereklidir.

5. Düzenli güvenlik testleri ve risk analizleri: Sistemlerin güvenliğinin sürekli olarak değerlendirilmesi ve olası zafiyetlerin tespit edilmesi gereklidir.

Bu tür önlemler, veri sorumlularının veri güvenliğini sağlamak için gerekli teknik ve idari tedbirleri alma yükümlülüğünü düzenleyen KVKK'nın 12.

maddesi ile doğrudan ilişkilidir. Artan dijitalleşme ve otomasyon uygulamaları dikkate alındığında, mevcut mevzuatın teknolojik gelişmeler doğrultusunda güncellenmesi ve veri güvenliği ihlallerinin yönetimine ilişkin daha ayrıntılı teknik standartların geliştirilmesi de veri koruma ekosisteminin güçlendirilmesi açısından önem taşımaktadır.

***Çalışanların eğitimi:*** Çalışanların KVKK ve veri koruma konularında bilgi ve farkındalığını artırarak, uyum süreçlerine katkılarını sağlamaları kritik önem taşımaktadır.

***Veri koruma kültürünü oluşturma:*** Veri koruma bilincini kurumun tümüne yayarak, çalışanların veri koruma sorumluluklarını benimsemelerini sağlamak önemlidir.

***Üst yönetimin desteği:*** Üst yönetimin KVKK uyum süreçlerine destek vermesini sağlayarak, kaynak tahsisini kolaylaştırmak ve uyum süreçlerine öncelik verilmesini sağlamak gereklidir. Bu hususta üst yönetimin süreci sahiplenmesi için kurumsal yönetim ilkeleri çerçevesinde ilgili kurul veya komitelere görev verilmesi önerilmektedir.

***Sürekli iyileştirme yaklaşımı:*** KVKK uyum süreçlerinin düzenli olarak gözden geçirilmesi ve iyileştirme fırsatlarının belirlenmesi sağlanmalıdır. Bu konu kurum kültürünün ayrılmaz bir parçası olarak ele alınmalıdır.

***Hukuki destek:*** KVKK ve veri koruma konularında uzman hukukçulardan destek alarak, yasal gerekliliklere uyum sağlamak önemlidir. Yasal risklerin erken teşhis edilmesi ve kurumsal karar alma süreçlerinin tasarlanmasında mevzuata uyumu güvence altına alacak uygulamaların yapılması açısından hukuki danışmanlık ve destek alınması önerilmektedir. KVKK ve veri koruma konularında uzman hukukçulardan destek almak, kurumların yasal gerekliliklere uyum sağlaması ve hukuki riskleri minimize etmesi açısından kritik öneme sahiptir. Yasal risklerin erken teşhisi ve kurumsal karar alma süreçlerinin mevzuata uygun şekilde tasarlanması, kurumların KVKK uyum süreçlerini etkin biçimde yönetmesine katkı sağlar. Bu bağlamda hukuki danışmanlık ve uzman desteği, yalnızca uyum süreçlerinin doğru yürütülmesi açısından değil, aynı zamanda otomasyon ve dijital araçların uygulanmasında yasal çerçeveyi güvence altına almak açısından da önemlidir.

Çalışmanın ana konusu olan KVKK uyum süreçlerinde otomasyon araçlarından yararlanılması açısından, farklı dijital araçların seçimi ve kullanımı yalnızca operasyonel verimliliği artırmakla kalmayıp, aynı zamanda hukuki uyum risklerinin azaltılmasına da katkı sağlayabilir. Örneğin, otomatik veri işleme kayıtları, başvuru yanıt sürelerinin izlenmesi ve veri ihlali raporlamaları gibi süreçler hem operasyonel hem de hukuki gereklilikler açısından önem taşır. Buna ek olarak, günümüzde dijitalleşme hızı ve yeni teknolojilerin veri işleme süreçlerine entegrasyonu göz önüne alındığında, mevcut KVKK'nın dijital teknolojilere uyumlu şekilde güncellenmesi**,** veri koruma ve veri yönetimi süreçlerinde ortaya çıkabilecek sorunların önlenmesi için temel bir gerekliliktir. Çalışmada bu husus doğrudan ele alınmamış olup, gelecekteki araştırmalarda KVKK'nın dijitalleşmeye uygun hale getirilmesi ve otomasyon süreçleri ile entegrasyonunun incelenmesi önerilmektedir.

Burada politika önerisi olarak sunulan her bir konu başlığında belirtilen iyileşme alanlarına yönelik gelecekte yeni araştırmalar yapılması ve farklı sektörler için teknoloji tabanlı çözümler üretilmesi hem sektör çalışanlarına hem de veri güvenliğini sağlamaya dönük denetleyici ve düzenleyici kurumlara yön vererek önemli bilgilerin ortaya konması yoluyla katkı sağlayabilir.

## SONUÇ

Türkiye'deki kurumların KVKK uyum süreçlerinde karşılaştıkları operasyonel zorlukları ve otomasyon çözümlerinin potansiyelini ortaya koymayı amaçlayan bu araştırmanın sonuçları, kurumların veri envanteri yönetimi, ilgili kişi başvurularının işlenmesi ve yasal süreçlere uyum gibi alanlarda otomasyon araçlarına yatırım yaparak uyum süreçlerini iyileştirebileceklerini göstermektedir. Ancak, otomasyonun tek başına yeterli olmadığı, insan faktörünün ve veri koruma kültürünün de önemli olduğu unutulmamalıdır. Kurumların, çalışanlarının eğitimine, farkındalığına ve motivasyonuna yatırım yaparak, uyum süreçlerini daha başarılı bir şekilde yönetmeleri mümkündür.

Burada önemli olan, otomasyon uygulamalarının KVKK uyumunu yalnızca bir yasal zorunluluk olarak görmek yerine, kurumsal süreçlerde verimlilik, sürdürülebilirlik ve stratejik değer sağlayan bir araç olarak konumlandırılmasıdır. Otomasyonun etkin kullanılmasıyla birlikte güç kazanılabilecek alanları üç ana başlık altında ele almak mümkündür: Birincisi, kurumsal açıdan operasyonel

verimliliğin artırılması ve aynı zamanda maliyet tasarrufunun olmasıdır. Manuel olarak yürütülen KVKK süreçleri hem zaman alıcı hem de yüksek hata payı içeren operasyonlara dönüşebilir. Oysa uygun bir otomasyon kullanımı ile bu durumu kökten değiştirme imkânı olabilir. Azalan manuel iş gücü ihtiyacı, daha hızlı tamamlanan süreçler ve olası cezalardan kaçınma sayesinde otomasyon, orta ve uzun vadede önemli bir etkinlik elde edebilir.

İkincisi, otomasyon kullanımı ile kurumsal risk yönetimi faaliyetlerinde ve yasal uyum güvencesi açısından avantaj sağlanabilir. Manuel yapılan işlerdeki hata payının ortadan kalkması yanında, anlık tespit ve veri güvenliği için hızlı müdahale fırsatlarını artırabilir. Burada en önemli katkısı, otomasyon kullanımı ile hem zararı en aza indirme imkânı, hem de Kişisel Verileri Koruma Kurumu'na yapılması gereken 72 saatlik bildirim yükümlülüğünü yerine getirmede kolaylaştırıcı etkisi olabilir.

Üçüncüsü ise, KVKK uyum faaliyetlerinin doğası gereği sadece bir olay veya vaka için değil, sürekli devam eden bir süreç olarak tasarlanması gerekliliğidir. Otomasyon, bu uygulama sürecinin sürdürülebilirliğini sağlar. Aynı zamanda her türlü raporlama ihtiyaçlarının karşılanması yoluyla kim, ne zaman, hangi veriye erişti; hangi başvuruya ne zaman cevap verildi gibi sorulara verilen yanıtlarla oluşturulan bu kayıtlar, olası bir denetimde veya hukuki süreçte kurum için stratejik önemi olan bir kanıt niteliği taşır ve şeffaflığı sağlar.

Bu çalışmada kullanılan anketi cevaplayan örneklem, çalışmanın bir kısıtı olarak düşünülmektedir. Bu açıdan söz konusu anket sorularının daha geniş bir örneklem ile KVKK kapsamında görev alanlar yanında sürecin tüm paydaşlarını kapsayacak biçimde genişletilerek araştırmanın yenilenmesi ve elde edilen yeni bulgular çerçevesinde ihtiyaçların belirlenerek politika önerileri geliştirilmesi, literatüre katkı sağlayacak bir alan olarak değerlendirilmektedir.

**KAYNAKÇA**

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

Athey, S., Tibshirani, J. ve Wager, S. (2019). Generalized random forests. The Annals of Statistics 47 (2), 1148 – 1178.

Barati, M. ve Rana, O. (2020). Enhancing User Privacy in IoT: Integration of GDPR and Blockchain. In Blockchain and Trustworthy Systems; Zheng, Z., Dai, H.N., Tang, M., Chen, X., Eds.; Springer: Singapore, pp. 322–335.

Biau, G. (2012). Analysis of a Random Forests Model. Journal of Machine Learning Research 13 (2012) 1063-1095, https://www.jmlr.org/papers/volume13/biau12a/biau12a.pdf Erişim tarihi: 08.08.2025

Biau, G., L. Devroye, and G. Lugosi (2008). Consistency of random forests and other averaging classifiers. Journal of Machine Learning Research 9 (9).

Boulesteix, A.-L., A. Bender, J. Lorenzo Bermejo, and C. Strobl (2012). Random forest gini importance favours snps with large minor allele frequency: impact, sources and recommendations. Briefings in Bioinformatics 13 (3), 292–304.

Brown, A., ve Green, T. (2019). Adoption of data protection tools in organizations: A case study approach. International Journal of Cybersecurity, 8(1), 22-35. https://doi.org/10.xxxx

Bulut M. (2020). Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler, Ankara Barosu Dergisi, 2020/3, ss-101-150, DOI: 10.30915/abd.811902.

Chatsuwan, P., Phromma, T., Surasvadi, N. ve Thajchayapong, S. (2023). Personal data protection compliance assessment: A privacy policy scoring approach and empirical evidence from Thailand's SMEs, Heliyon, Volume 9, Issue 10, 2023, e20648, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2023.e20648,

Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K. ve Fensel, A. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. Sensors, 22(7), 2763. https://doi.org/10.3390/s22072763

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

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340. https://doi.org/10.2307/249008

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of "high risk" in the General Data Protection Regulation. Computer Law ve Security Review 35 (6). DOI: https://doi.org/10.1016/j.clsr.2019.105342

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.

Dülger, M. V., (2021). KVKK Uygulamasında ve Uyum Sürecinde Ortaya Çıkan Soru ve Sorunlar (Questions and Problems Arising in KVKK Application and Compliance Process). SSRN: https://ssrn.com/abstract=3792288 http://dx.doi.org/10.2139/ssrn.3792288 Erişim: 08.08.2025

ENISA (European Union Agency for Network and Information Security) (2016). Guidelines for SMEs on the security of personal data processing. https://www.enisa.europa.eu/sites/default/files/publications/WP2016%203-2%206%20Data%20Controllers%20Risk.pdf , Erişim: 08.08.2025

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 ve Security, 2019(9), 9-11. https://doi.org/10.1016/s1361-3723(19)30095-8

European Data Protection Supervisor (2025). Data Protection Impact Assessment (DPIA). https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en Erişim: 08.08.2025

Gartner (2022). State of Privacy — The European Union, by Analyst(s): Bart Willemsen, Bernard Woo, Nader Henein. ID G00762813, Private Report

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

GeeksforGeeks (2025). Random Forest Approach in R Programming. https://www.geeksforgeeks.org/r-language/random-forest-approach-in-r-programming/ Erişim tarihi: 20.08.2025

Güllebağatur, H. (2024). Şirketlerin KVKK Uyum Sürecinde Karşılaştığı Zorluklar, https://www.gdprdanismanlik.com/2024/01/30/sirketlerin-kvkk-uyum-surecinde-karsilastigi-zorluklar/ Erişim tarihi: 08.08.2025

Haddouchi M. ve Berrado A. (2024). A survey and taxonomy of methods interpreting random forest models, Computer Science, Machine Learning, https://arxiv.org/pdf/2407.12759

Kartal, M. T. (2018). Kişisel verilerin korunması: Türk bankacılık sektörü üzerine kavramsal bir değerlendirme. Uluslararası Ekonomi ve Yenilik Dergisi, 4(1), 1-18.

KPMG (2019). GDPR: The importance of employee awareness. https://home.kpmg/xx/en/home/insights/2019/05/gdpr-the-importance-of-employee-awareness.html. Erişim: 18.08.2025

KVKK (2016). 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete: 07.04.2016/29677, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698veMevzuatTur=1veMevzuatTertip=5 Erişim: 15.10.2025

Mobofis (2025). KOBİ'lerin Büyümesini Engelleyen 5 Operasyonel Problem ve Çözümleri, https://www.mobofis.com.tr/blog-detay/kobilerin-buyumesini-engelleyen-5-operasyonel-problem-ve-cozumleri Erişim: 08.08.2025

OECD (2023). Emerging privacy-enhancing technologies: Current regulatory and policy approaches. OECD Digital Economy Papers, No. 351, OECD Publishing, Paris.

PwC (2018). GDPR: Building a culture of data protection. https://www.pwc.com/gx/en/services/consulting/cybersecurity/data-protection/gdpr.html. Erişim: 08.08.2025

Savaş, R. N., Zaim, A. H., ve 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.

Schein, E. H. (2010). Organizational culture and leadership (4th ed.). Jossey-Bass.

Smith, J., ve Johnson, L. (2020). Compliance with data protection regulations: A study of organizational tools and employee behavior . Journal of Information Privacy, 15(2), 45-60.

Tang A. (2023). Privacy in Practice Establish and Operationalize a Holistic Data Privacy Program, Taylor and Francis Publications, ISBN: 978-1-032-12546-6 (hbk).

Üstün Y. ve Günal A. N. (2020). İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi, Kişisel Verileri Koruma Dergisi. 2(2), 61-74.

Venkatesh, V., ve Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186-204.

Wilson, D., ve Thompson, R. (2021). The role of training in GDPR compliance: An empirical study. Journal of Organizational Behavior, 42(4), 567-582.

## Ek 1: Modelde Kullanılan Değişken Listesi

| Değişken | Değişken ile İlgili Anket Sorusu | Değişken Adı |
|---|---|---|
| x1 | Kurumunuzun çalışan sayısını ifade ediniz. | Çalışan sayısı |
| x2 | Kurumunuzun tipini belirtiniz. | Kurum tipi |
| x3 | İç denetim birimi kaç kişiden oluşmaktadır? | İç denetçi sayısı |
| x4 | Biriminiz daha önce KVKK'yı içeren bir denetim yaptı mı? | Yapılan KVKK Denetimi |
| x5 | Kurumunuzda KVKK ile ilgili çalışmalar yapılırken hangi görevdeydiniz ? | Görev Yeri |
| x6 | Kurumda KVKK'nın yönetiminden kim sorumludur? | KVKK Sorumlu Yönetim |
| x7 | Kurum olarak Kişisel Veri Envanterinizi nasıl tutuyorsunuz ? | KVKK Envanter Yönetimi |
| x8 | Kurum olarak Kişisel Veri Envanterinizi özel bir yazılım ile tutuyorsanız... | KVKK Yazılımı Var/Yok |
| x9 | Kişisel Veri Envanteri Yönetiminde Karşılaşılan Veri Sınıflandırma Zorlukları en Büyük Zorluklardandır | KVKK Veri Sınıflaması |
| x10* | Kişisel Veri Envanteri Yönetiminde süreçlerin ve envaterin güncellenmesi en Büyük Zorluklardandır | KVKK Süreç ve Envanter Yönetimi |
| x11 | Kişisel Veri Envanteri Yönetiminde farklı sistemler ve kaynaklar arasında uyumu sağlamak en Büyük Zorluklardandır | Sistem ve Kaynak Uyumu |
| x12 | Kişisel Veri Envanteri Yönetiminde otomasyon ve entegrasyon eksikliği en Büyük Zorluklardandır | Otomasyon Eksikliği |
| x13 | Kişisel Veri Envanteri Süreçlerinizi Otomatikleştirmek İçin araç kullanıyorsanız kullandığınız Araçlardan Memnun Musunuz? | Otomasyon Memnuniyeti |
| x14 | KVKK Uyum Sürecinde Envanter Yönetiminin Rolünü Nasıl Değerlendiriyorsunuz? | Envanter Yönetiminin Rolü |
| x15 | Kişisel Veri Envanteri Yönetimi İçin Kullandığımız Çözümün kapsamlı raporlama eksikliği vardır | Raporlama Eksikliği |
| x16 | Kişisel Veri Envanteri Yönetimi İçin Kullandığımız çözümün kullanımı kolay değildir | KVKK Çözüm Kolaylığı |
| x17 | Kişisel Veri Envanteri Yönetimi İçin Kullandığımız çözümün entegrasyon sorunları vardır | KVKK Entegrasyon Sorunu |
| x18 | Kişisel Veri Envanteri Yönetimi İçin Kullandığımız çözümün güncelleme ve bakım maliyetleri yüksektir | Program Bakım Maliyeti |
| x19 | Şu Anda Kullandığımız Sistemlerde Kişisel Veri Envanteri Güncellemelerini otomatik olarak sürekli yapıyoruz | Otomatik Güncelleme Var/Yok |
| x20 | Şu Anda Kullandığınız Sistemlerde Kişisel Veri Envanteri Güncellemelerini manuel olarak düzenli aralıklarla yapıyoruz | Manuel Güncelleme Var/Yok |
| x21 | Şu Anda Kullandığımız Sistemlerde Kişisel Veri Envanteri Güncellemelerini yalnızca gerekli olduğunda yapıyoruz | Gerektiğinde Güncelleme Var/Yok |
| x22 | Şu anda kişisel veri topladığımız her süreçte, sürece özel bir aydınlatma metni kullanıyoruz. | Aydınlatma Metni Var/Yok |

| | | |
|---|---|---|
| x23 | Kişisel Veri Envanteri Yönetimi İçin Sürekli güncelleme ve raporlama özelliği Olmazsa Olmazdır | Sürekli Güncelleme Raporu Var/Yok |
| x24 | Kişisel Veri Envanteri Yönetimi İçin Kullanıcı dostu arayüz özelliği Olmazsa Olmazdır | Kullanıcı Dostu Arayüz Var/Yok |
| x25 | KVKK Uyum Sürecinde Kişisel Veri Envanteri Yönetiminin Şirketiniz/kurumunuz Üzerindeki Etkisini Nasıl Değerlendiriyorsunuz? | KVKK Yönetime Etkisi |
| x26 | Kurumunuzda/Şirketinizde kullanılmıyorsa Kişisel Veri Envanteri yönetimini basitleştiren ve otomatikleştiren bir çözümü benimseme olasılığınız nedir? | Çözüm Kullanma Olasılığı |
| x27 | Veri Sahibi Erişim Taleplerinin tamamını (İlgili Kişi Başvurusu) şu anda manuel olarak yönetiyoruz | Veri Erişim Talebi Manuel Yönetim |
| x28 | Veri Sahibi Erişim Taleplerinin tamamını (İlgili Kişi Başvurusu) şu anda otomatik araçlar kullanarak olarak yönetiyoruz | Veri Erişim Talebi Otomatik Yönetim |
| x29 | Veri Sahibi Erişim Taleplerinin tamamını (İlgili Kişi Başvurusu) şu anda üçüncü parti hizmet sağlayıcı kullanarak yönetiyoruz | Veri Erişim Talebi 3. Taraf destekli Yönetim |
| x30 | Veri Sahibi Erişim Talepleri kurumunuza hangi sıklıkla gelmektedir | Veri Erişim Talebi Sıklığı |
| x31 | Organizasyonunuzda tek bir İlgili Kişi Başvurusu işlemek için ortalama ne kadar zaman harcıyorsunuz? | Başvuru İşleme Süreci |
| x32 | Organizasyonunuzda tek bir İlgili Kişi Başvurusu işlemek için ortalama kaç adam gün harcanıyor? (Teknik, Hukuk, Uyum, Departman yetkilileri vb.) | Başvuru İşlemeye Harcanan Birim Süre |
| x33 | İlgili Kişi Başvurusu işleme süresini bir otomasyon aracı ile dakikalara indirmek operasyonel verimliliğinizi olumlu anlamda önemli ölçüde etkiler mi? | Başvuru İşlemenin Otomasyona Dönmesi ile Verimlilik Artışı |
| x34 | İlgili Kişi Başvurusu işleme sürecinde veri toplama ve doğrulama aşamasında çok zorlanmaktayız | Veri toplama ve doğrulama zorluğu |
| x35 | İlgili Kişi Başvurusu işleme sürecinde Yasal değerlendirme ve uyum kontroller aşamasında çok zorlanmaktayız | Yasal değerlendirme ve uyum kontrolleri zorluğu |
| x36 | İlgili Kişi Başvurusu işleme sürecinde Yasal süre içinde yanıt verme konusunda çok zorlanmaktayız | Yasal sürede yanıt verme zorluğu |
| x37 | İlgili Kişi Başvurusu işleme sürecinde teknik kaynakların yönetimi konusunda çok zorlanmaktayız | Teknik kaynak yönetimi zorluğu |

*:x10- bağımlı değişken ve diğerleri bağımsız değişken olarak alınmıştır.

## ANALYSIS OF PERCEPTIONS OF AUTOMATION COMPLIANCE WITHIN THE FRAMEWORK OF KVKK REGULATIONS IN TÜRKİYE

**Sezer KAHYAOGLU**
**Yenal ARSLAN**
**Mustafa ÖZÇAKIR**

### EXTENDED ABSTRACT

In today's rapidly digitalizing world, protecting personal data is essential for safeguarding property and privacy. Legal frameworks, such as the Personal Data Protection Law (KVKK) in Türkiye and the European Union's General Data Protection Regulation (GDPR), have established various obligations aimed at ensuring data security. However, the increasing volume and complexity of data create practical challenges in protecting personal data and managing related activities. These challenges arise from the need to establish and reorganize a new organizational structure that integrates compliance processes related to the Personal Data Protection Law. In this context, automation tools are crucial for the effective functioning of systems set up for data protection and regulatory compliance. This study investigates the use of automation tools to comply with KVKK regulations in Türkiye. Survey questions were designed to assess the adoption and willingness of personnel involved in the compliance process to use these tools and techniques, and the current situation in this area was analyzed. The study employed Likert-scale questions in addition to collecting demographic information about the participants. The empirical results were obtained using the R program's random forest algorithm, and policy recommendations were presented based on the findings. As a pioneering analysis of the KVKK compliance process, this study aims to enrich the literature and serve as a valuable resource for regulatory institutions, stakeholders involved in the process, and researchers.

Based on the key findings of this study, the following strategic recommendations are proposed to address the challenges encountered in KVKK compliance processes and to maximize the benefits of automation solutions:

1. Automating Data Inventory Management: It is essential to automate the creation and updating of data inventories to save time and reduce costs. Recommended actions include reviewing existing business processes and developing a holistic approach by integrating additional modules into the current system.

2. Optimizing KVKK Application Processing: To comply with legal deadlines, it is important to automate the processes of collecting, verifying, evaluating, and responding to data subject applications. The application processing should be managed comprehensively, with checkpoints established throughout the workflow to ensure effectiveness and efficiency.
3. Automating Data Security Breach Detection and Reporting: Establishing systems that automatically detect and report data security breaches is crucial for early risk identification and mitigation. This proactive approach helps coordinate the necessary responses to such incidents.
4. Employee Training: Increasing employee knowledge and awareness of KVKK and data protection issues is vital for fostering their engagement in compliance efforts.
5. Creating a Data Protection Culture: It is essential to cultivate a culture of data protection within the organization, encouraging employees to take ownership of their data protection responsibilities and promoting awareness.
6. Support from Senior Management: Gaining support from senior management is critical for resource allocation and prioritizing compliance processes. It is advised to assign relevant boards or committees duties aligned with corporate governance principles to ensure management's commitment to these processes.
7. Continuous Improvement Approach: Regularly reviewing KVKK compliance processes to identify improvement opportunities is necessary. This should be regarded as an integral part of the corporate culture.
8. Legal Support: To meet legal requirements, it is important to seek guidance from legal experts specializing in KVKK and data protection. Obtaining legal consultancy can help identify risks early and ensure compliance within corporate decision-making processes.

Future research on the recommended areas for improvement, as well as the development of technology-based solutions for various sectors, could provide valuable insights and guidance for industry employees and supervisory and regulatory bodies responsible for ensuring data security.