Taşınabilir Tıbbi Cihazların Mühendislik Tasarımında Tasarıma Dayalı Gizlilik Yaklaşımı: KVKK ve GDPR Perspektifinde Veri Güvenliği

Araştırma Makalesi/Research Article

Sezen BAL[1*], Emre ÇANAYAZ[2] , Zeynep Beyza KABATAŞ SOYER[3]

[1]Bilgisayar Teknolojileri Bölümü, Marmara Üniversitesi, İstanbul, Türkiye
[2]Elektronik ve Otomasyon Bölümü, Marmara Üniversitesi, İstanbul, Türkiye
[3]Mülkiyet Koruma ve Güvenlik Bölümü, Marmara Üniversitesi, İstanbul, Türkiye

sezen.bal@marmara.edu.tr, emre.canayaz@marmara.edu.tr, zeynep.kabatassoyer@marmara.edu.tr
(Geliş/Received:22.09.2025; Kabul/Accepted:23.02.2026)
DOI: 10.17671/gazibtd.1788711

***Özet*—**Dijital sağlık teknolojilerinin yaygınlaşmasıyla evde bakım uygulamaları, giyilebilir sistemler ve taşınabilir tıbbi cihazlar aracılığıyla yoğun sağlık verisi toplanmaktadır. Bu durum, veri güvenliği ve mahremiyet risklerini artırmakta; Tasarıma Dayalı Gizlilik (Privacy by Design – PbD) yaklaşımını önemli hale getirmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation – GDPR), PbD ve Varsayılan Gizlilik (Privacy by Default – PbDf) ilkelerini açıkça düzenlerken, Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK) ise teknik ve idari tedbirler öngörmekte olup PbD'ye doğrudan atıf yapmamaktadır. Bu çalışma, nitel araştırma yaklaşımı çerçevesinde gerçekleştirilen karşılaştırmalı hukuk analiziyle, PbD'nin mühendislik süreçlerindeki uygulanabilirliğini GDPR ve KVKK kapsamında incelemektedir. Bulgular, Türkiye'de PbD'nin çoğunlukla CE sertifikasyonu ile ISO/IEC 29134 ve IEC 62304 gibi uluslararası standartlar aracılığıyla dolaylı biçimde uygulandığını göstermektedir. Sonuç olarak, hukuki düzenlemeler, mühendislik standartları ve etik ilkelerin birlikte değerlendirilmesi, taşınabilir tıbbi cihazlarda hem kullanıcı güvenliğini hem de veri mahremiyetini güçlendiren bütüncül bir çerçeve sunmaktadır. Bu yönüyle çalışma, Türkiye'de PbD'nin uygulamaya dönük olarak somutlaştırılmasına katkı sağlamakta ve dijital sağlık teknolojilerinde sürdürülebilir inovasyon için etik temelli bir yol haritası önermektedir.

***Anahtar Kelimeler*—**etik, GDPR (genel veri koruma tüzüğü), gömülü sistemler, hukuki çerçeve, KVKK (kişisel verilerin korunması kanunu), tasarıma dayalı gizlilik (Privacy by Design), taşınabilir cihazlar, tıbbi cihaz tasarımı, veri güvenliği

Privacy by Design Approach in the Engineering Design of Portable Medical Devices: Data Security from the Perspectives of KVKK and GDPR

***Abstract*—** With the widespread adoption of digital health technologies, large volumes of health data are collected through home care applications, wearable systems, and portable medical devices. This situation increases risks related to data security and privacy, making the Privacy by Design (PbD) approach increasingly important. While the General Data Protection Regulation (GDPR) explicitly regulates the principles of PbD and Privacy by Default (PbDf), Türkiye's Law on the Protection of Personal Data (KVKK) prescribes technical and administrative measures but does not directly refer to PbD. This study examines the applicability of the PbD approach in engineering processes within the scope of the GDPR and the KVKK through a comparative legal analysis conducted within the framework of a qualitative research approach. The findings show that, in Türkiye, PbD is mostly implemented indirectly through CE certification and international standards such as ISO/IEC 29134 and IEC 62304. In conclusion, the combined evaluation of legal regulations, engineering standards, and ethical principles provides a holistic framework that strengthens both user safety and data privacy in portable medical devices. In this respect, the study contributes to the practical concretization of PbD in Türkiye and proposes an ethics-based roadmap for sustainable innovation in digital health technologies.

***Keywords*—**ethics, GDPR (general data protection regulation), embedded systems, legal framework, KVKK (personal data protection law), Privacy by Design (PbD), portable devices, medical device design, data security

1. GİRİŞ (INTRODUCTION)

Dijital sağlık teknolojilerinin yaygınlaşması, giyilebilir sistemler, taşınabilir tıbbi cihazlar ve evde bakım uygulamalarının kullanımını artırmıştır. Ayrıca sensörler ve gömülü yazılımlar sayesinde büyük miktarda tıbbi veri sürekli olarak işlenebilmektedir. Kişisel verilerin güvenliği ve gizliliği, bu değişiklikler nedeniyle mühendislik tasarımlarının önemli bir parçası olmalıdır [1].

Ann Cavoukian tarafından geliştirilen Tasarımda Gizlilik (Privacy by Design – PbD) yaklaşımı, veri korumanın sistemin ilk aşamalarından itibaren gözetilmesini savunurken; Varsayılan Gizlilik (Privacy by Default – PbDf) ilkesi, varsayılan ayarların en yüksek gizlilik düzeyinde tasarlanmasını öngörmektedir [2], [3]. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), bu ilkeleri m.25 ile bağlayıcı hale getirmiş, ayrıca m.35 ile Veri Koruma Etki Değerlendirmesi (Data Protection Impact Assessment – DPIA) sürecini yüksek riskli veri işleme faaliyetleri için zorunlu kılmıştır [4]. Türkiye'de yürürlükte bulunan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), genel ilkeler (m.4) ile veri güvenliği tedbirlerini (m.12) düzenlemekte, ancak PbD ve DPIA kavramlarına doğrudan yer vermemektedir [5].

Tıbbi cihazların güvenliği ve gizliliği, uluslararası literatürde sıklıkla vurgulanmaktadır. Semantha ve ark., sağlık sektöründe PbD uygulamalarını incelemiş ve IoT tabanlı cihazlarda güvenlik zafiyetlerinin yaygın olduğunu ortaya koymuştur [6]. Ganoje, tıbbi cihaz veri yönetiminde mevzuata uyum için veri haritalama, DPIA, şifreleme ve anonimleştirme yöntemlerinin önemini vurgulamıştır [7]. Ayrıca son dönemde yapay zekâ tabanlı sağlık uygulamalarında, algoritmaların eğitildiği verilerin gizliliği ile kullanıcıya sunulan sonuçların şeffaflığı öne çıkan tartışma konularıdır [8].

GDPR ile PbD yaklaşımının birleştirilmesi üzerine yapılan çalışmalar da artmaktadır. Elshekeil ve Laoyookhong, GDPR m.25 için teknik çözümler önermiştir [9]. Lima, blockchain teknolojisinin şeffaflık, izlenebilirlik ve güvenilirlik açısından GDPR'ye uygun bir PbD sistemi oluşturma yeteneğine sahip olduğunu iddia etmektedir [10]. Kurtz ve ark., üçüncü taraf veri işleyicileri için PbD'nin kurumsal düzeyde uygulanması hakkında kapsamlı bir araştırma yayınlamışlardır [11]. Burmen, GDPR metinleri ile PbD yaklaşımını inceleyerek hangi maddelerin doğrudan PbD yaklaşımını gözettiğini ortaya koymuştur [12]. Veri koruma tartışmaları, son zamanlarda yapay zeka teknolojilerinin getirdiği risklere odaklanmıştır.

Literatürde, özellikle veri çıkarımı, yeniden tanımlama ve algoritmik önyargı gibi AI-özel risklerin mevcut DPIA süreçleri tarafından yeterince ele alınmadığı vurgulanmıştır. GDPR, DPIA'yı m.35 ile açıkça zorunlu kılarken, KVKK'da DPIA ile ilgili kavramlar bulunmamaktadır [13]. Buna karşılık, GDPR'de yalnızca m.35 değil, aynı zamanda m.24 (sorumluluk ilkesi), m.25 (PbD ve PbDf) ve m.32 (güvenlik tedbirleri) birlikte değerlendirildiğinde DPIA'nın PbD'nin uygulama araçlarından biri olduğu görülmektedir.

Türkiye'deki akademik yazında ise daha çok genel veri koruma ilkeleri ve idari/teknik tedbirler tartışılmaktadır. KVKK, PbD'ye doğrudan atıfta bulunmasa da tasarım aşamasında gizliliğin gözetilmesi gerektiğini dolaylı biçimde vurgulayan bir dizi rehber yayınlanmıştır. Örneğin, "Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler", varsayılan ayarların gizliliği garanti edecek şekilde düzenlenmesi gerektiğini açıkça belirtmektedir [14]. Sağlık verilerinin "özel nitelikli kişisel veri" olarak kategorize edilmesi, bu alanda üretilen cihazların daha yüksek güvenlik ve anonimleştirme standartlarına sahip olmasını gerektirir. Bununla birlikte, mevcut ulusal literatürde, taşınabilir tıbbi cihazların veri depolama, aktarım ve silme süreçlerinin PbD yaklaşımı ile bütünleştirilebileceğine dair doğrudan bir çalışma bulunmamaktadır. GDPR, m.25 ve m.35 hükümleriyle PbD ve DPIA süreçlerini açıkça zorunlu kılarken; KVKK'da bu kavramlara doğrudan yer verilmemekte, yalnızca genel ilkelere ve teknik-idari tedbirlere atıf yapılmaktadır. Türkiye'de sağlık verilerinin "özel nitelikli kişisel veri" olarak kabul edilmesi nedeniyle bu durum daha da önemlidir.

Bu çalışma, taşınabilir tıbbi cihazların mühendislik tasarım süreçlerinde PbD yaklaşımının GDPR ve KVKK çerçevesinde nasıl uygulandığını incelemeyi amaçlamaktadır. Çalışmanın temel araştırma sorusu, PbD ve DPIA gibi önleyici veri koruma mekanizmalarının iki düzenleme kapsamında hangi hukuki ve teknik araçlar aracılığıyla hayata geçirilebildiği ve bu farklılıkların mühendislik uygulamalarına nasıl yansıdığıdır.
Bu amaç doğrultusunda çalışma, nitel araştırma yaklaşımı kapsamında karşılaştırmalı hukuk analizi ve doküman incelemesi yöntemlerine dayanmaktadır. GDPR ve KVKK hükümleri, Kişisel Verileri Koruma Kurulu kararları ile ISO/IEC 29134 ve IEC 62304 gibi uluslararası teknik standartlar analiz edilerek değerlendirilmiştir.

2. YÖNTEM (METHODOLOGY)

Bu çalışma, nitel araştırma yaklaşımı çerçevesinde yürütülmüş olup, doküman analizi ve karşılaştırmalı hukuk incelemesi yöntemlerine dayanmaktadır. Araştırmada, taşınabilir tıbbi cihazların mühendislik tasarım süreçlerinde PbD yaklaşımının uygulanabilirliği, GDPR ile Türkiye'de yürürlükte bulunan KVKK hükümleri kapsamında incelenmiştir.
Araştırmanın veri setini GDPR'nin özellikle PbD, PbDf ve DPIA ile ilişkili olan 25. ve 35. maddeleri, KVKK'nin 4., 6. ve 12. maddeleri, KVKK'nin konuya ilişkin güncel kararları ve rehberleri ile taşınabilir tıbbi cihazların tasarım ve yazılım geliştirme süreçlerine yön veren ISO/IEC 29134 ve IEC 62304 gibi uluslararası teknik standartlar oluşturmaktadır. Ayrıca CE işaretleme süreci ve Avrupa Birliği tıbbi cihaz mevzuatı, mühendislik uygulamaları üzerindeki dolaylı etkileri bakımından değerlendirmeye dahil edilmiştir.

Doküman analizi kapsamında, ilgili mevzuat ve standartlar sistematik olarak incelenmiştir. PbD, PbDf ve DPIA kavramlarının her iki düzenleme altında nasıl ele alındığı karşılaştırmalı olarak analiz edilmiştir. Bu analiz sırasında, hukuki yükümlülüklerin mühendislik tasarım süreçlerine yansımaları, normatif değerlendirme yöntemiyle ele alınmıştır. Özellikle KVKK'da doğrudan düzenlenmeyen PbD ve DPIA mekanizmalarının, uygulamada hangi teknik ve organizasyonel araçlar aracılığıyla hayata geçirildiği ortaya konulmuştur.

Çalışmada ayrıca, taşınabilir tıbbi cihazlara ilişkin kavramsal bir örnek kullanılarak, veri yaşam döngüsü boyunca PbD yaklaşımının mühendislik, hukuki ve etik boyutları birlikte değerlendirilmiştir. Bu örnek literatürdeki yaygın uygulamalar, mevzuat hükümleri ve teknik standartlar esas alınarak oluşturulmuş kavramsal bir model niteliği taşımaktadır. Bu yöntemle, PbD yaklaşımının teorik çerçevesi ile mühendislik uygulamaları arasındaki ilişkinin analitik olarak görünür kılınması amaçlanmıştır.

Bu kapsamda analiz, hukuki düzenlemeler ile mühendislik uygulamaları arasındaki etkileşimi görünür kılmayı amaçlayan tematik bir çerçeve üzerinden yürütülmüştür. PbD, PbDf ve DPIA kavramları; (i) hukuki dayanakları, (ii) teknik karşılıkları ve (iii) mühendislik tasarım süreçlerine etkileri bakımından sınıflandırılarak değerlendirilmiştir. Bu yaklaşım, normatif hukuki gerekliliklerin teknik standartlar ve mühendislik uygulamaları aracılığıyla nasıl somutlaştığını ortaya koymayı hedeflemektedir.

3. TÜRKİYE VE AVRUPA'DA HUKUKİ ÇERÇEVE (LEGAL FRAMEWORK IN TÜRKİYE AND THE EUROPEAN UNION)

Bu bölümde, çalışma kapsamında gerçekleştirilen doküman analizi ve karşılaştırmalı inceleme sonucunda elde edilen bulgular, Türkiye ve Avrupa Birliği'ndeki hukuki çerçeve üzerinden sunulmaktadır.

Türkiye'de 6698 sayılı KVKK, kişisel verilerin korunmasına ilişkin temel kanuni düzenlemedir. KVKK, kişisel verilerin işlenmesine ilişkin olarak "amaçla sınırlılık", "veri minimizasyonu" ve "veri güvenliği" gibi genel ilkeleri benimsemekte; ayrıca veri sorumlularına teknik ve idari tedbirler alma yükümlülüğü getirmektedir. Ancak KVKK'da, GDPR'de yer alan PbD, PbDf ve DPIA gibi kavramlara doğrudan atıf bulunmamaktadır. Bu nedenle Türkiye'de veri güvenliği, büyük ölçüde genel ilkeler çerçevesinde ele alınmakta; tasarım aşamasında gizliliğin sistematik biçimde değerlendirilmesine ilişkin açık bir düzenleme bulunmamaktadır.

Bununla birlikte Kişisel Verileri Koruma Kurulu'nun güncel kararlarında bu kavramlara yer verilmektedir. Kurul'un 26.08.2024 tarihli "Araştırma Şirketlerinin İstatistiksel Araştırma Yapmak Amacıyla Rastgele Numara Çevirme ile Telefon Mülakatı Yöntemi Kullanarak Gerçekleştirdikleri Kişisel Veri İşleme Faaliyetleri" başlıklı kararında; veri sorumlularının 6698 sayılı Kanun'un 12'nci maddesi uyarınca kişisel veri işleme süreçlerinde Kanun'a uyumu sağlamak ve verileri korumak amacıyla uygun teknik ve idari tedbirleri almaları gerektiği belirtilmiştir. Kararda ayrıca, teknik ve idari tedbirler belirlenirken PbD ve PbDf ilkelerine uyulması, işleme faaliyetinin Kanun'un 4'üncü maddesinde yer alan genel ilkelere uygunluğunu sağlayacak şekilde faaliyete özgü tedbirlerin tasarlanması ve kullanılan yazılımların varsayılan ayarlarının yalnızca işleme amacı için gerekli faaliyetlere izin verecek biçimde yapılandırılması gerektiğine karar verilmiştir. Bu durum, kişisel verilerin daha etkin korunabilmesi için açık ve sistematik bir kanuni düzenlemeye duyulan ihtiyacı ortaya koymaktadır [15].

GDPR, kişisel verilerin işlenmesine ilişkin yalnızca genel ilkeleri belirlemekle kalmaz; aynı zamanda gizliliğin, ürün ve sistem tasarımının ayrılmaz bir parçası olarak ele alınmasını da zorunlu kılar. Bu kapsamda, PbD ve PbDf ilkeleri, Tüzük m.25 ile bağlayıcı hale getirilmiştir. Bu ilkelere göre, ürün ve hizmetlerin tasarım aşamasında; gereksiz veri işlenmesinin önlenmesi, veri minimizasyonu, güvenlik önlemlerinin entegre edilmesi ve verilerin şifrelenmesi gibi önleyici teknik çözümler uygulanmalıdır. Ayrıca, GDPR m.35, özellikle sağlık verileri gibi hassas nitelikli kişisel verilerin işlendiği durumlarda, DPIA yapılmasını zorunlu kılmaktadır. DPIA süreci; işlenecek verilerin niteliğini, işleme yöntemlerini, bu sürecin doğurabileceği riskleri ve bu risklere karşı alınması gereken önlemleri sistematik biçimde analiz etmeyi gerektirir. GDPR hükümlerine aykırılık durumunda, ihlal eden kurumlara yüksek para cezaları da dâhil olmak üzere ciddi yaptırımlar uygulanmaktadır. AşağıdaTablo 1, KVKK ile GDPR arasında PbD, PbDf ve DPIA bağlamında öne çıkan yapısal farkları göstermektedir [16].

KVKK, kişisel verilerin korunmasına ilişkin temel ilkeleri belirlemekle birlikte, bu ilkeleri somut ve bağlayıcı uygulamalara dönüştüren sistematik düzenlemelerden yoksundur. Buna karşılık GDPR PbD, PbDf ve DPIA gibi önleyici mekanizmaları doğrudan hukuki yükümlülük haline getirmiştir. Bu nedenle, PbD ve ilişkili yaklaşımlar Avrupa'da bağlayıcı normlar çerçevesinde uygulanırken, Türkiye'de ise bu ilkeler daha çok dolaylı yorumlar ve iyi mühendislik uygulamaları çerçevesinde teşvik edilmektedir.

4. STANDART ENTEGRASYONU (INTEGRATION OF STANDARDS)

Bu bölümde, KVKK ve GDPR kapsamında ortaya çıkan hukuki yükümlülüklerin, uluslararası teknik standartlar aracılığıyla mühendislik tasarım süreçlerine nasıl entegre edildiği analiz edilmektedir.
Tıbbi cihazlarda PbD yaklaşımının uygulanması için yalnızca hukuki düzenlemeler (GDPR, KVKK) yeterli değildir. Bu sürecin tamamlayıcı bir unsuru olarak, uluslararası teknik standartların da tasarım aşamasına entegre edilmesi gerekmektedir.

Tablo 1. KVKK ve GDPR'nin PbD, PbDf ve DPIA Açısından Karşılaştırılması

Boyut	Türkiye (KVKK)	Avrupa (GDPR)
PbD / PbDf	KVKK'de bu kavramlara doğrudan yer verilmez; yalnızca veri minimizasyonu, amaçla sınırlılık ve veri güvenliği gibi genel ilkeler çerçevesinde yükümlülük öngörülür.	GDPR m.25 uyarınca, PbD ve PbDf ilkeleri açık ve bağlayıcı şekilde düzenlenmiştir.
DPIA	KVKK kapsamında DPIA prosedürüne ilişkin doğrudan bir yasal düzenleme bulunmamaktadır.	GDPR m.35 uyarınca, özellikle yüksek riskli veri işleme faaliyetlerinde DPIA uygulanması zorunludur.
Hukuki Yaptırım	PbD ya da DPIA ihlalleri için özel bir yaptırım öngörülmemiştir; bu tür durumlar ancak genel veri güvenliği yükümlülükleri kapsamında değerlendirilebilir.	PbD veya DPIA yükümlülüklerine uyulmaması halinde, doğrudan GDPR yaptırımları uygulanabilir; bu yaptırımlar yüksek para cezalarını da içermektedir.

Tablo 2. KVKK – GDPR – ISO/IEC 29134 – IEC 62304 Karşılaştırmalı İncelemesi

Hukuki Yükümlülük	GDPR Karşılığı	KVKK Karşılığı	Uluslararası Standart	Tıbbi Cihaz Uygulama Örneği
Kişisel verilerin işlenmesi risklerini önceden analiz etme	GDPR m.35 – DPIA	KVKK'de doğrudan düzenlenmemiştir; ancak "teknik ve idari tedbirler" kapsamında dolaylı olarak risk analizi gerektirir.	ISO/IEC 29134 – PIA/DPIA Rehberi	Taşınabilir tıbbi cihaz belleğinde depolanan veriler için yetkisiz erişim, cihaz kaybı veya sızıntı risklerinin değerlendirilmesi
Yazılım geliştirme sürecinde güvenlik	GDPR m.25 – PbD ve PbDf	KVKK'de doğrudan yer almaz; m.6'da "özel nitelikli veriler" için ek güvenlik önlemleri öngörülür.	IEC 62304 – Tıbbi Cihaz Yazılım Yaşam Döngüsü	Cihaz gömülü yazılımında şifreleme, hata yönetimi, güvenli güncelleme mekanizmalarının yaşam döngüsüne entegre edilmesi
Veri minimizasyonu ve anonimleştirme	GDPR m.5(1)(c) – Data Minimization, GDPR m.25	KVKK m.4'te işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi düzenlenmiştir; m.7'de kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmiştir.	ISO/IEC 29134 (risk analizi sırasında anonimleştirme değerlendirmesi)	Yapay zeka algoritmaları için cihaz belleğinde toplanan verilerin kimlikten arındırılması
Varsayılan gizlilik (PbDf)	GDPR m.25(2)	KVKK'de açıkça yer almaz; m.4 temel ilkelere, m.5 kişisel veri işlenme şartlarına ve m.12 veri güvenliğine ilişkin yükümlülüklere atıf yoluyla dolaylı şekilde uygulanır.	IEC 62304 (yazılım yaşam döngüsü kapsamında güvenlik gereklilikleri)	Taşınabilir tıbbi cihazın varsayılan ayarının "en az veri toplama" modunda çalışması

ISO/IEC 29134 ve IEC 62304 standartları, mühendislik uygulamalarını yönlendiren ana araçlardır. ISO/IEC 29134, kişisel veri işleyen sistemlerde gizlilik açısından potansiyel risklerin belirlenmesi ve değerlendirilmesi için Gizlilik Etki Değerlendirmesi (Privacy Impact Assessment - PIA) metodolojisini ortaya koymaktadır. TSE tarafından Türkiye'de TS ISO/IEC 29134 olarak yayımlanan bu standart, KVKK'de doğrudan atıfta bulunmamasına rağmen "teknik ve idari tedbir" yükümlülüğünün uygulanmasında elverişli bir çerçeve sunmaktadır.

IEC 62304, tıbbi cihaz yazılımlarının yaşam döngüsünü düzenleyerek güvenlik süreçlerini yazılım geliştirme aşamasından itibaren bir gereklilik olarak aramaktadır. Türkiye'de TS EN 62304 olarak yayımlanan bu standart, CE işareti almak isteyen üreticiler için zorunludur. Bu nedenle güvenli tasarım, yazılımın yaşam döngüsüne güvenli güncelleme, hata yönetimi ve şifreleme mekanizmalarının entegre edilmesiyle mümkün olmaktadır.

Taşınabilir tıbbi cihazların hukuki uyumunun sağlanması ve uluslararası pazarlara erişim, bu standartların KVKK ve GDPR ile birlikte değerlendirilmesini gerektirmektedir. Tablo 2, GDPR ve KVKK hükümlerinin uluslararası standartlarla uyumunu ve bu durumun mühendislik uygulamalarına etkisini özetlemektedir. GDPR, PbD ve DPIA'yı doğrudan hukuki zorunluluk haline getirirken; KVKK bu ilkeleri genel çerçevede bırakmakta, ancak ISO/IEC 29134 ve IEC 62304 gibi standartlar aracılığıyla Türkiye'de dolaylı olarak uygulanabilmektedir. Bu durum, özellikle CE işareti hedefleyen üreticiler için standartların uygulamada normatif boşluğu tamamlayıcı bir işlev gördüğünü göstermektedir.

5.MÜHENDİSLİK BOYUTU VE ETİK SORUMLULUKLAR (ENGINEERING DIMENSION AND ETHICAL RESPONSIBILITIES)

Taşınabilir tıbbi cihazlar tasarlarken, mühendislik tasarımının yalnızca teknik işlevselliği değil, aynı zamanda veri güvenliği ve mahremiyet ilkelerini de göz önünde bulundurması gerekir. Bu nedenle, PbD yaklaşımı, mühendislerin cihazlarını tasarlarken baştan itibaren göz önünde bulundurmaları gereken temel bir prensiptir.

Uygulamada, bu yöntem, yalnızca gerekli bilgilerin toplanması (veri minimizasyonu), depolama ve iletim süreçlerinde güçlü şifreleme kullanımı, kimliksizleştirme (anonimleştirme veya pseudonimizasyon) yöntemlerinin kullanılması ve çok katmanlı erişim kontrollerinin oluşturulması ile gerçekleştirilir. PbDf ilkesi, cihazların varsayılan ayarlarının en yüksek gizlilik düzeyinde yapılandırılmasını gerektirir. Örneğin, cihazın verileri dış sistemlere otomatik olarak aktarmaması, kullanıcının bunu tercih etmesi ve kurulum sürecinde veri saklama koşullarına ilişkin açık bilgilendirme, mühendislik tasarımında gizliliğin doğrudan altına gömülmesini sağlayabilir.

Yüksek riskli veri işleme işlemlerinde kullanılan DPIA, mühendislik prosedürlerinin önemli bir bileşenidir. DPIA, cihazın hangi verileri toplayabileceği, bunların nasıl işleneceği, potansiyel riskler ve önlemler hakkında kapsamlı bir analizi içerir. DPIA, Avrupa Birliği'nde yürürlükte bulunan GDPR hükümleri uyarınca zorunlu hale getirilmişken, Türkiye KVKK kapsamında açıkça düzenlenmemiştir. Bununla birlikte, üreticilerin ISO/IEC 29134 gibi uluslararası standartlar ve CE işaretleme prosedürlerini kullanarak benzer risk değerlendirmelerini yapmaları bir zorunluluktur.

GDPR, mühendislik tasarımında gizliliği yalnızca etik sorumluluk düzeyinde değil, aynı zamanda hukuken bağlayıcı bir yükümlülük olarak ele almaktadır. GDPR m.25 ve m.35 uyarınca, mühendisler veri minimizasyonu, güvenlik önlemleri ve DPIA prosedürlerini tasarım sürecine entegre etmekle yükümlüdür. Buna karşılık, Türkiye'de yürürlükteki KVKK kapsamında PbD ve DPIA kavramlarına açık bir şekilde yer verilmemektedir. Bu nedenle, Türkiye'de mühendisler söz konusu ilkeleri daha çok etik sorumluluk ve iyi mühendislik uygulaması çerçevesinde değerlendirmektedir.

Bu nedenle, Türkiye'de mesleki sorumluluk ve uluslararası standartlara uyum çerçevesinde etik ilkelere bağlılık çok önemlidir. Ancak Avrupa'da mühendislik etiği ile hukuki yükümlülükler arasındaki sınır giderek ortadan kalkmıştır. Birçok etik ilke, doğrudan hukuki yaptırımlarla desteklenir hale gelmiştir.

Etik açıdan, mühendisler yalnızca teknik önlemlerle sorumlu değildir. Mühendislik pratiğinde etik ilkelere bağlılığın bir göstergesi, kullanıcılara verilerin toplandığı ve nasıl işlendiğini açık ve anlaşılır bir şekilde anlatmaktır. Gerçek anlamda gönüllülüğe dayalı rıza süreçlerinin oluşturulması ve çocuklar, yaşlılar ya da kronik hastalar gibi hassas gruplara özel güvenlik önlemlerinin geliştirilmesi bu etik yaklaşımın temelini oluşturur. Bu yaklaşım, Türkiye'de doğrudan hukuki yaptırımlarla desteklenmese de mesleki standartlar, uluslararası pazara erişim ve toplumsal sorumluluk açısından göz ardı edilemeyecek bir yaklaşımdır.

Aşağıdaki örnek, taşınabilir bir tıbbi cihaz için PbD yaklaşımının hukuki, teknik ve etik çerçevelerin mühendislik uygulamalarında nasıl somutlaştığını göstermektedir.

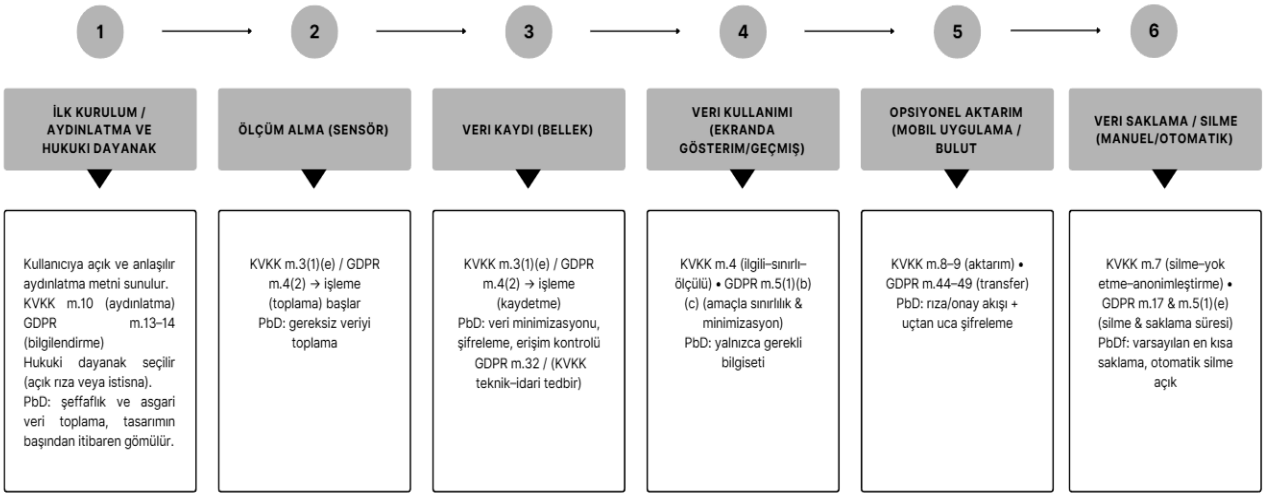
5.1. Kavramsal Örnek: Taşınabilir Glikoz Ölçüm Cihazı (Conceptual Example: Portable Glucose Monitoring Device)

Bu örnek ilgili mevzuat hükümleri, uluslararası teknik standartlar ve literatürdeki yaygın uygulamalar esas alınarak oluşturulmuş kavramsal bir model niteliği taşımaktadır. Bu model, PbD yaklaşımının taşınabilir tıbbi cihazların mühendislik tasarım süreçlerine nasıl entegre edilebileceğini göstermeyi amaçlamaktadır.

Bu kapsamda ele alınan akıllı bir glikoz ölçüm cihazı, diyabet hastalarının günlük yaşamlarında kan şekeri düzeylerini takip etmelerine izin vermektedir. Bu cihaz, kullanıcı tarafından yapılan ölçüm sonuçlarını belleğinde şifreli olarak kaydetmekte ve dış sistemlere veri aktarımını varsayılan olarak devre dışı bırakmaktadır. PbDf ilkesi nedeniyle veri aktarımı yalnızca kullanıcının açık onayıyla gerçekleşmektedir. Ayrıca, veri minimizasyonu ilkesine uygun olarak cihaz yalnızca glikoz seviyesi ve ölçüm zamanı bilgilerini işlemektedir. Bu nedenle, hekime iletilen raporlarda hastanın kimliği yerine benzersiz bir kod kullanılmaktadır. Çok faktörlü kimlik doğrulama sistemleri, erişimin hasta ve yetkilendirilmiş hekimle sınırlandırılmasını sağlamaktadır.

Cihazın piyasaya sürülmeden önce geliştirici firma tarafından gerçekleştirilen DPIA, yetkisiz erişim, veri kaybı veya yanlış ölçüm aktarımı gibi riskleri incelemektedir. Bu risklere karşı teknik önlemler (şifreleme, güvenli yazılım güncellemeleri) ve organizasyonel önlemler (yetki sınırlamaları, düzenli erişim logları denetimi) planlanmaktadır. Avrupa Birliği'nde DPIA, GDPR m.35 uyarınca bağlayıcı bir yükümlülük iken, Türkiye'de yürürlükte olan KVKK kapsamında bu kavrama doğrudan bir atıf bulunmamaktadır. Bununla birlikte, KVKK kapsamında öngörülen "teknik ve idari tedbir" yükümlülüğü ile uluslararası standartlara (ISO/IEC 29134, IEC 62304) uyum gerekliliği, benzer süreçlerin fiilen uygulanmasını gerekli kılmaktadır ve uluslararası standartlar göz önünde bulundurularak belgelenmektedir.

Mühendislerin etik sorumlulukları, yalnızca teknik ve hukuki önlemlerle sınırlı değildir. Kullanıcılara hangi verilerin toplandığı ve nasıl işlendiğini açık bir şekilde bilgilendirmek, rıza süreçlerinin gönüllülük esasına dayanması ve çocuklar, yaşlılar veya kronik hastalar gibi hassas gruplara yönelik ek güvenlik önlemleri oluşturmak da mühendislik pratiğinin önemli bir parçasıdır. Böylece, taşınabilir glikoz ölçüm cihazının veri yaşam döngüsü, veri toplama, depolama, iletim, paylaşım ve silme aşamalarında PbD yaklaşımıyla uyumludur ve kullanıcı gizliliği tasarım sürecinin önemli bir parçasıdır. Şekil 1, taşınabilir bir tıbbi cihazın veri yaşam döngüsü için mühendislik boyutunda PbD yaklaşımının nasıl uygulanabileceğini göstermektedir.



Şekil 1. Taşınabilir tıbbi cihazlarda veri yaşam döngüsü

(1) İlk Kurulum / Aydınlatma ve Hukuki Dayanak:

Kullanıcıya açık ve anlaşılır aydınlatma metni sunulur. KVKK m.10 ve GDPR m.13–14 kapsamında aydınlatma ve bilgilendirme yükümlülüğü yerine getirilir. PbD yaklaşımı gereği şeffaflık, asgari veri işleme koşulları ve kullanıcı tercihleri kurulumun başından itibaren görünür hale getirilir.

(2) Ölçüm Alma (Sensör):

KVKK m.3/1-e ve GDPR m.4(2) uyarınca ölçüm yoluyla kişisel veri elde edilmesi, işleme faaliyetinin başlangıcı niteliğindedir. PbD yaklaşımına uygun olarak yalnızca gerekli sağlık verileri (örneğin glikoz seviyesi, ölçüm zamanı) toplanır.

(3) Veri Kaydı (Bellek):

KVKK m.3/1-e (işleme tanımı: kaydetme, depolama) ve GDPR m.4(2) kapsamında verilerin belleğe alınması veri işleme faaliyeti sayılır. KVKK m.12 ve GDPR m.32 uyarınca teknik ve idari tedbirler (şifreleme, erişim kontrolü, güvenli saklama) uygulanır. PbD yaklaşımı doğrultusunda veri minimizasyonu, güvenli depolama ve erişim sınırlandırması sağlanır.

(4) Veri Kullanımı (Ekranda Gösterim/Geçmiş):

KVKK m.4 ve GDPR m.5(1)(b)(c) uyarınca amaçla sınırlılık ve veri minimizasyonu ilkeleri gözetilir. Veriler belirli, açık ve meşru amaçlarla işlenmeli ve amacıyla sınırlı tutulmalıdır. PbD ilkesine göre, yalnızca gerekli bilgiler kullanıcıya sunulur; işleme amacı dışında bilgi görüntülenmesi engellenir.

(5) Opsiyonel Aktarım (Mobil Uygulama / Bulut):

KVKK m.8–9 ve GDPR m.44–49 kapsamında kişisel veriler, ilgili kişinin açık rızasıyla üçüncü taraf sistemlere yurt içi veya yurt dışı aktarılabilir. PbD yaklaşımına uygun olarak aktarım uçtan uca şifreleme ile güvence altına alınır. Bu aşama, yüksek risk barındırabileceğinden GDPR m.35 kapsamında DPIA sürecinin yürütülmesi gerekir.

(6) Veri Saklama / Silme (Manuel / Otomatik):

KVKK m.7 ve GDPR m.17 uyarınca, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi, işleme amacı ortadan kalktığında zorunlu hale gelir. PbD ilkesi gereği, varsayılan saklama süresi en kısa süre olarak tanımlanmalı; otomatik silme mekanizmaları sistem düzeyinde uygulanmalı ve ayrıca kullanıcıya manuel silme seçeneği açıkça sunulmalıdır.

Bu yaşam döngüsü, taşınabilir tıbbi cihazların mühendislik tasarımında gizliliğin yalnızca etik bir tercih değil, GDPR kapsamında hukuki bir yükümlülük, KVKK kapsamında ise hesap verebilirlik ve iyi mühendislik pratiği gereği uygulanması gereken bir prensip olduğunu göstermektedir.

5. SONUÇLAR (CONCLUSIONS)

Bu çalışma, GDPR Tüzüğü ve KVKK hükümleri çerçevesinde PbD yaklaşımının taşınabilir tıbbi cihazların mühendislik tasarım süreçleri açısından önemini ortaya koymuştur. Bulgular, Avrupa Birliği'nde GDPR ile birlikte PbD'nin hukuki açıdan bağlayıcı bir yükümlülük haline geldiğini göstermektedir. Buna karşılık, Türkiye'de yürürlükte olan KVKK, PbD ve DPIA gibi önleyici veri koruma mekanizmalarına doğrudan yer vermemekte, daha çok genel ilkelere dayalı bir düzenleme çerçevesi sunmaktadır. Bu çerçevede PbD, DPIA, etik sorumluluklar ve uluslararası standartlara dayalı fiili uyum mekanizmaları, Türkiye'deki uygulamaların şekillenmesinde önemli rol oynamaktadır.

CE işareti süreci ile ISO/IEC 29134 ve IEC 62304 gibi uluslararası teknik standartlar, Türkiye'deki üreticiler açısından dolaylı da olsa önemli bir uyum aracı işlevi görmektedir. Bu standartlar, hem teknik kaliteyi hem de kullanıcı güvenliğini destekleyen tamamlayıcı bir düzenleme mekanizması niteliğindedir.

Nihayetinde taşınabilir tıbbi cihazların güvenilirliği yalnızca teknik performans değerlendirmeleriyle sınırlı değildir; veri gizliliği ve güvenliği tasarım aşamasından itibaren sistemin ayrılmaz bir parçası olarak ele alınmalıdır. Sağlık teknolojilerinde sürdürülebilir inovasyonun sağlanabilmesi, hukuki uyumun yanı sıra etik sorumluluklar ve iyi mühendislik uygulamalarının bütüncül biçimde değerlendirilmesini gerektirmektedir.

KAYNAKLAR (REFERENCES)

[1] F. Başkaya and H. Karacan, "Yapay Zeka Tabanlı Sistemlerin Kişisel Veri Mahremiyeti Üzerine Etkisi: Sohbet Robotları Üzerine İnceleme," *Bilişim Teknolojileri Dergisi*, vol. 15, no. 4, pp. 481-491, 2022.

[2] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles," **Information and Privacy Commissioner of Ontario**, Canada, 2009.

[3] European Data Protection Board, **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default**, Brussels, Belgium, 2020.

[4] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)," *Official Journal of the European Union*, L119, pp. 1–88, 2016.

[5] Türkiye Büyük Millet Meclisi, "6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)," Resmî Gazete, Sayı: 29677, 7 Nisan 2016.

[6] M. Semantha, et al., "Privacy by Design in Healthcare: A Systematic Review," *Journal of Medical Systems*, vol. 44, no. 8, pp. 1–14, 2020.

[7] A. Ganoje, "Data Privacy in Medical Device Management: The Role of DPIA, Encryption, and Anonymization," *Health Informatics Journal*, vol. 29, no. 1, pp. 55–72, 2023.

[8] J. Zhou and A. Kapoor, "Artificial Intelligence in Healthcare: Privacy and Transparency Challenges," AI in Medicine, vol. 118, pp. 102–113, 2021.

[9] S. A. Elshekeil and S. Laoyookhong, "GDPR Privacy by Design: From Legal Requirements to Technical Solutions," in Proc. Int. **Conf. on Information Security and Privacy**, 2017, pp. 33–41.

[10] C. Lima, "Blockchain–GDPR Privacy by Design: How Decentralized Blockchain Internet will Comply with GDPR Data Privacy," in Proc. Int. Conf. on Blockchain Applications, 2018, pp. 1–6.

[11] C. Kurtz, M. Semmann, and T. Böhmann, "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors," in Proc. **Americas Conf. on Information Systems (AMCIS),** 2018, pp. 1–10.

[12] B. Brumen, "Automated Text Similarities Approach: GDPR and Privacy by Design Principles," in Proc**. European–Japanese Conf. on Information Modelling and Knowledge Bases**, 2020, pp. 145–158.

[13] A. Galandarli, "Mitigating AI Risks: A Comparative Analysis of Data Protection Impact Assessments under GDPR and KVKK," *Journal of Data Protection & Privacy*, vol. 7, p. 252, 2025, doi: 10.69554/ATTT2755.

[14] Kişisel Verileri Koruma Kurumu, "Mobil Uygulamalarda Kişisel Verileri İşleyen Taraflara Yönelik Tavsiyeler", Bülten, Haziran-Ağustos 2025, 8, pp. 30 – 32. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/05a40150-8405-4cba-b7a9-a069c2580225.pdf

[15] Ö. B. Bayram, "Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi", *Kişisel Verileri Koruma Dergisi*. 4(1), p. 49, 2022.

[16] M.B. Kaya, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi" (2020) 78(4) İstanbul Hukuk Mecmuası 1859. https://doi.org/10.26650/mecmua.2020.78.4.000