

## General Data Protection Regulation Compliance and Privacy Protection in Wearable Health Devices: Challenges and Solutions

### Giyilebilir Sağlık Cihazlarında Genel Veri Koruma Tüzüğü Uyumluluğu ve Gizliliğin Korunması: Zorluklar ve Çözümler

Mazlum ÖZÇAĞDAVUL<sup>a\*</sup>  

<sup>a</sup> Research Assistant, Department of Management Information Systems, Faculty of Business Administration, Ankara Yıldırım Beyazıt University, Ankara, Türkiye. [ROR](#)

<sup>a</sup> Araştırma Görevlisi, Yönetim Bilişim Sistemleri Bölümü, İşletme Fakültesi, Ankara Yıldırım Beyazıt Üniversitesi, Ankara, Türkiye. [ROR](#)

<sup>\*</sup> Corresponding Author / İletişimden Sorumlu Yazar, E-mail: [mozcagdavul@aybu.edu.tr](mailto:mozcagdavul@aybu.edu.tr)

#### ARTICLE INFO

##### Article History:

Received: 14.10.2024

Accepted: 25.11.2024

Publication: 23.12.2024

##### Citation:

Ozcagdavul, M. (2024). General data protection regulation compliance and privacy protection in wearable health devices: challenges and solutions.

Artuklu Health, 10, 29-37.

<https://doi.org/10.58252/artukluhealth.1566573>

#### ABSTRACT

**Introduction:** Wearable health devices have transformed personal health management by providing real-time monitoring and personalized care. However, the vast amounts of sensitive data collected by these devices pose significant privacy risks, particularly in compliance with the General Data Protection Regulation (GDPR). The GDPR enforces strict requirements around consent, data minimization, and the right to be forgotten. Ensuring GDPR compliance is a major challenge for developers and manufacturers of wearable health devices.

**Methods:** This study employs a systematic review to analyze current literature on GDPR compliance challenges in wearable health devices. Data were extracted from peer-reviewed studies, industry reports, and legal analyses published between 2010 and 2024. Key themes were identified through thematic analysis, focusing on consent management, data minimization, encryption, and privacy-by-design strategies.

**Results:** The review found that security breaches and informed consent are the most significant challenges in ensuring GDPR compliance. Many wearable devices collect excessive amounts of data, conflicting with GDPR's data minimization principle. Privacy-by-design and encryption were identified as critical solutions, though these approaches introduce trade-offs in device functionality and user experience.

**Conclusion:** Addressing GDPR compliance in wearable health devices requires a balance between robust data protection and usability. Solutions like privacy-by-design and encryption are essential but require careful implementation to avoid performance impacts. Future efforts should focus on improving user consent management and developing more efficient data governance frameworks.

**Keywords:** GDPR compliance, Wearable health devices, Data privacy, Consent management

#### MAKALE BİLGİLERİ

##### Makale Geçmişi:

Geliş Tarihi: 14.10.2024

Kabul Tarihi: 25.11.2024

Yayın Tarihi: 23.12.2024

##### Atf Bilgisi:

Özçagdavul, M. (2024). Giyilebilir sağlık cihazlarında genel veri koruma tüzüğü uyumluluğu ve gizliliğin korunması: zorluklar ve çözümler.

Artuklu Health, 10, 29-37.

<https://doi.org/10.58252/artukluhealth.1566573>

#### ÖZET

**Giriş:** Giyilebilir sağlık cihazları, gerçek zamanlı izleme ve kişiselleştirilmiş bakım sağlayarak kişisel sağlık yönetimini dönüştürmüştür. Bununla birlikte, bu cihazlar tarafından toplanan büyük miktarda hassas veri, özellikle Genel Veri Koruma Tüzüğü (GDPR) ile uyumluluk açısından önemli gizlilik riskleri oluşturmaktadır. GDPR rıza, veri minimizasyonu ve unutulma hakkı ile ilgili katı gereklilikler getirmektedir. GDPR uyumluluğunu sağlamak, giyilebilir sağlık cihazları geliştiricileri ve üreticileri için büyük bir zorluktur.

**Yöntem:** Bu makale, giyilebilir sağlık cihazlarında GDPR uyumluluk zorluklarına ilişkin mevcut literatürü analiz etmek için sistematik bir inceleme kullanmaktadır. Veriler 2010 ve 2024 yılları arasında yayınlanan hakemli çalışmalardan, endüstri raporlarından ve yasal analizlerden elde edilmiştir. Tematik analiz yoluyla rıza yönetimi, veri minimizasyonu, şifreleme gizlilik odaklı tasarım stratejilerine odaklanan kilit temalar belirlenmiştir.

**Bulgular:** İnceleme, güvenlik ihlalleri ve bilgilendirilmiş onayın GDPR uyumluluğunun sağlanmasında en önemli zorluklar olduğunu ortaya koymuştur. Birçok giyilebilir cihaz, GDPR'nin veri minimizasyonu ilkesiyle çelişen aşırı miktarda veri toplamaktadır. Gizlilik odaklı tasarım ve şifreleme kritik çözümler olarak tanımlanmıştır, ancak bu yaklaşımlar cihaz işlevselliği ve kullanıcı deneyiminde ödünleşimlere yol açmaktadır.

**Sonuç:** Giyilebilir sağlık cihazlarında GDPR uyumluluğunun ele alınması, sağlam veri koruması ve kullanılabilirlik arasında bir denge gerektirir. Gizlilik odaklı tasarım ve şifreleme gibi çözümler çok önemlidir ancak performans etkilerinden kaçınmak için dikkatli bir uygulama gerektirir. Gelecekteki çabalar, kullanıcı onayı yönetimini iyileştirmeye ve daha verimli veri yönetimi çerçeveleri geliştirmeye odaklanmalıdır.

**Anahtar Kelimeler:** GDPR uyumluluğu, Giyilebilir sağlık cihazları, Veri gizliliği, Rıza yönetimi

## 1. Introduction

Wearable health devices have significantly transformed personal health monitoring and management over the past decade. From basic fitness trackers to sophisticated medical sensors, these devices empower individuals to monitor vital signs and other health indicators in real-time, facilitating proactive health management and timely medical interventions (Kazanskiy, Khonina and Butt, 2024). The global market for wearable health devices has seen rapid expansion, driven by increasing consumer demand for personalized healthcare solutions and the growing prevalence of chronic diseases that benefit from continuous monitoring (Hein, Vrijens and Hiligsmann, 2020). These developments are part of the broader trend toward digital health, where technology plays a pivotal role in healthcare delivery, patient engagement, and chronic disease management (Abernethy et al., 2022).

However, the widespread adoption of these devices has raised significant concerns regarding data privacy and security, particularly in light of the stringent requirements imposed by the General Data Protection Regulation (GDPR), enacted by the European Union in 2018. GDPR sets a high standard for the protection of personal data, especially sensitive health data, by enforcing strict regulations such as explicit consent, data minimization, purpose limitation, and the right to erasure (Tikkinen-Piri, Rohunen and Markkula, 2018). For developers and manufacturers of wearable health devices, ensuring compliance with GDPR presents a complex challenge, as it requires a delicate balance between robust data security and user-friendly functionalities (Thapa and Camtepe, 2021).

Wearable health devices collect and process large amounts of personal data, including sensitive health information such as heart rate, blood pressure, glucose levels, and sleep patterns. Furthermore, obtaining explicit, informed consent for the collection and use of such data remains a challenge, as the complexities of data processing are not always easily communicated to users (Solove, 2013).

The GDPR principle of data minimization, which requires that only the necessary amount of personal data be collected and processed, creates practical challenges for the design and functionality of wearable devices (Tene and Polonetsky, 2011; Nissenbaum, 2011). Many wearable devices are designed to collect comprehensive health data to offer detailed insights, yet this often conflicts with GDPR's strict data minimization

requirements (Tankard, 2016). In addition, the "right to be forgotten" presents another significant challenge for manufacturers, requiring robust data management systems that can securely and completely erase personal data upon request (Wright and De Hert, 2012).

This study aims to explore the complexities of GDPR compliance in the context of wearable health devices, focusing on the critical challenges faced by developers, manufacturers, and users. It will also propose potential solutions to address these challenges, including encryption techniques, improved anonymization methods, and user-centric consent management platforms. By examining existing literature and emerging trends, this study seeks to provide actionable insights to promote a privacy-centric innovation culture within the wearable health device sector while ensuring compliance with GDPR.

Wearable health devices, ranging from fitness trackers to advanced medical sensors, have become integral to personal health monitoring and management (Sætnan, Schneider and Green, 2018). These devices offer real-time tracking of health metrics such as heart rate, glucose levels, and sleep patterns, empowering users to take proactive control over their health. As the adoption of these technologies grows, so do concerns about the privacy and security of the vast amounts of sensitive personal health data they collect (Stewart, 2019; Syu et al., 2023).

In 2018, the European Union enacted the General Data Protection Regulation (GDPR), a comprehensive framework designed to protect personal data, including sensitive health information. GDPR imposes strict requirements, such as explicit user consent, data minimization, and the right to erasure, all aimed at safeguarding individual privacy. Despite these regulations, ensuring compliance in the context of wearable health devices poses unique challenges, as continuous data collection and real-time processing make it difficult to align with GDPR principles.

Developers and manufacturers of wearable health devices must navigate the complexities of GDPR compliance while maintaining device functionality and user-friendly features. This background highlights the growing importance of developing robust solutions to protect personal health data and ensure regulatory adherence (Sokolova, 2021).

## 2. Methods

### 2.1. Research Design

This study employs a systematic review methodology to explore the challenges and solutions related to GDPR compliance and privacy protection in wearable health devices. A systematic review is an effective approach for synthesizing findings from existing research, providing a comprehensive and structured overview of the subject matter. This methodology allows for the identification of trends, gaps, and areas of consensus or divergence within the literature. By examining the latest studies, this review aims to present a thorough understanding of GDPR's impact on wearable health devices and propose actionable solutions to address the identified challenges.

### 2.2. Research Questions

The systematic review is guided by the following research questions:

1. What are the primary challenges faced by developers and manufacturers of wearable health devices in achieving GDPR compliance?
2. What solutions have been proposed or implemented to address these challenges?
3. How effective are these solutions in ensuring data privacy and security while maintaining the functionality of the devices?

### 2.3. Inclusion and Exclusion Criteria

To ensure the relevance and quality of the included studies, the following criteria were applied:

#### 2.3.1. Inclusion criteria:

- Peer-reviewed journal articles, conference papers, and authoritative industry reports.
- Studies that focus on GDPR compliance, privacy protection, and wearable health devices.
- Research published between 2010 and 2024 to capture relevant developments in GDPR and wearable technology.
- Articles written in English.

#### 2.3.2. Exclusion criteria:

- Non-peer-reviewed articles, editorials, opinion pieces, and news articles.
- Studies that do not specifically address wearable health devices or GDPR compliance.

- Research published before 2010 unless it is particularly relevant to foundational GDPR issues.

### 2.4. Search Strategy

The literature search was conducted across several electronic databases to ensure comprehensive coverage of the topic. The following databases were used:

PubMed: Focused on healthcare and wearable technology studies.

IEEE Xplore: Captured research on the technological aspects of wearable devices and data security.

Google Scholar: Broader scope to include grey literature and additional relevant articles.

The search terms and Boolean operators used include:

- “GDPR” and “wearable health devices”
- “data privacy” and “wearable technology”
- “data protection” and “smartwatches”
- “compliance” and “fitness trackers” and “health data”

The search was refined by filtering for publication date (2010-2024) and language (English). Additionally, reference lists of selected studies were manually reviewed to identify any further relevant articles.

### 2.5. Data Extraction

Data from the selected studies were extracted using a standardized data extraction form. The following information was collected from each study:

- Authors and year of publication: To track the timeline and key contributors to the field.
- Study type: Qualitative, quantitative, mixed-methods study, systematic reviews and meta-analyses, case studies, or technical papers
- Research focus: Specific challenges or solutions related to GDPR compliance.
- Key findings: Main outcomes of the study, especially regarding privacy protection strategies.
- Implications for practice: How findings can be applied in the development or regulation of wearable health devices.

### 2.6. Data Analysis

The extracted data were synthesized using a thematic analysis approach, facilitated by the use of NVivo software. NVivo provides advanced tools for coding, organizing, and analyzing qualitative data, enabling researchers to identify patterns and

themes more systematically. Through this process, common themes, challenges, and solutions related to GDPR compliance and wearable devices were identified. Specifically, NVivo was used to import and manage qualitative data from the selected studies, allowing for the efficient coding of text segments into categories. The software's query and visualization tools, such as word frequency analyses and thematic mapping, were leveraged to ensure a comprehensive and structured interpretation of the data. This systematic approach enhanced the reliability and depth of the thematic analysis, providing valuable insights into the challenges of ensuring GDPR compliance within the context of wearable technologies.

The identified themes were grouped into the following categories, corresponding to the research questions:

- Challenges in GDPR Compliance: Issues such as consent management, data minimization, and the right to be forgotten.
- Proposed solutions: Strategies including privacy-by-design, encryption, and pseudonymization.
- Effectiveness of solutions: Evaluation of the success of these strategies in ensuring privacy and regulatory compliance.

### 2.7. Quality Assessment

The quality of the included studies was assessed using the Critical Appraisal Skills Programme (CASP) checklist, which evaluates the methodological rigor of qualitative and quantitative research. The checklist was used to assess the clarity of research questions, appropriateness of the methodology, and robustness of the findings. Only studies that met the quality criteria were included in the final synthesis, while studies with significant methodological flaws were excluded to ensure the reliability of the review's conclusions.

### 2.8. Limitations

This systematic review has several limitations:

- Language bias: The review includes only studies published in English, potentially excluding relevant research in other languages.
- Timeframe: The review covers studies published between 2010 and 2024, potentially missing earlier foundational work or very recent research that has not yet been published.
- Publication bias: The reliance on electronic databases may lead to a publication bias, as studies with negative or non-significant results are less likely to be published.

### 2.9. Ethical Considerations

As this study involved a review of existing literature and did not involve primary data collection, no formal ethical approval was required. However, ethical considerations were maintained by ensuring an accurate representation of the findings and proper attribution to all original sources.

### 3. Results

The results of this systematic review provide insights into the key challenges and solutions related to GDPR compliance in wearable health devices. A thematic analysis was conducted, revealing that the most critical challenges include consent management, data minimization, security breaches, and ensuring the right to be forgotten. These challenges, though widely acknowledged, require technical solutions like encryption, pseudonymization, and privacy-by-design to enhance compliance. The effectiveness of these solutions varies, with encryption and privacy-by-design showing the most promise, although they come with trade-offs such as increased costs and reduced device functionality. Additionally, the literature highlights the need for user-friendly consent management and improved data governance. Overall, the findings suggest that while technological advancements can address many GDPR issues, a balance between data protection and usability is crucial for the successful deployment of wearable health technologies.

#### 3.1. GDPR Compliance Challenges

The most prominent themes in GDPR compliance challenges were security breaches, consent management, data minimization, the right to be forgotten, and cross-border data transfer.

**Table 1.** GDPR Compliance Challenges

| Challenge                   | Proportion |
|-----------------------------|------------|
| Security Breaches           | %30        |
| Consent Management          | %24        |
| Data Minimization           | %21        |
| Right to Be Forgotten       | %15        |
| Cross-border Data Transfers | %10        |

##### 3.1.1. Consent management

Managing informed consent is a significant issue, especially in the context of wearable health devices that continuously collect and process sensitive personal data. GDPR mandates that consent must be informed, specific, and explicit (Voigt and Von dem Bussche, 2017). However, research has shown that many users struggle to understand the complexities of data collection, processing, and sharing practices (Solove, 2013; Tikkinen-Piri et al., 2018).

Inadequate consent management, where users are not fully informed about how their data will be used, can lead to non-compliance with GDPR, resulting in fines and breaches of privacy (Wright and De Hert, 2012; Hoofnagle, Van Der Sloot and Borgesius, 2019). A lack of transparency in the terms and conditions of wearable health devices further exacerbates this problem, as many consent forms are long and difficult to interpret (Goddard, 2017). To address this, user-centric consent management platforms and simpler privacy notices are recommended to improve transparency and user engagement (Tankard, 2016; Paul and Irvine, 2014).

### 3.1.2. Data minimization

Data minimization is a core GDPR principle that presents a significant challenge for wearable health devices. The regulation requires that organizations collect only the minimal amount of data necessary for a specific purpose (Voigt and Von dem Bussche, 2017). However, many wearable devices, particularly in the healthcare sector, collect excessive amounts of data, often beyond what is necessary for their function (Granata et al., 2022; Roehrs et al., 2017). For example, devices tracking heart rate or glucose levels might also collect location data, activity levels, and even sleep patterns, much of which is unnecessary for the intended medical use (Galvin and DeMuro, 2020; Wright & De Hert, 2012). This is especially problematic as many wearable devices are designed to continuously collect data, making strict adherence to the principle of data minimization difficult. To mitigate this, researchers have suggested that developers implement privacy-by-design principles to limit unnecessary data collection from the outset (Cavoukian, 2010; Granata et al., 2022) and regularly audit the data collected to ensure it remains within the necessary scope (Tikkinen-Piri et al., 2018).

### 3.1.3. Security breaches

Security breaches pose a critical threat to GDPR compliance, particularly in the realm of wearable health devices, which handle large amounts of sensitive personal data. GDPR mandates that appropriate security measures must be implemented to protect data from unauthorized access, accidental loss, or theft (Voigt and Von dem Bussche, 2017; Goddard, 2017). However, many wearable devices lack robust encryption and other security measures, leaving them vulnerable to breaches (Galvin and DeMuro, 2016; Doherty, 2014). Researchers argue that end-to-end encryption and regular security audits are critical to reducing the risk of security breaches (Hein, Vrijens and Hiligsmann, 2020; Solove, 2013;

Fernández-Alemán et al., 2013). Moreover, organizations must adopt secure communication protocols, such as multi-factor authentication (Tikkinen-Piri et al., 2018; Wang et al., 2018).

### 3.1.4. Right to be forgotten

The right to be forgotten is a GDPR provision that allows individuals to request the deletion of their personal data, but ensuring the full deletion of user data from wearable devices presents a technical challenge (Wright and De Hert, 2019; Voigt and Von dem Bussche, 2017; European Union, 2016). Wearable devices often synchronize data with cloud storage or external databases, complicating the process of complete data erasure, especially when backups and redundant systems are involved (Goddard, 2017; Tikkinen-Piri et al., 2018). Ensuring compliance with the right to be forgotten is further challenged by the fact that health-related data may be embedded in larger datasets, making it difficult to isolate and delete specific user data (Granata et al., 2022; Narayanan and Shmatikov, 2010). Moreover, companies often store user data in multiple locations across global servers, making data deletion logistically complex (Hein, Vrijens and Hiligsmann, 2020; Solove, 2013). Effective solutions include improving data retention policies and implementing automatic data erasure tools that ensure all copies of data are securely deleted from both primary and backup systems (Roehrs et al., 2017; Voigt and Von dem Bussche, 2017).

### 3.1.5. Cross-border data transfers

Cross-border data transfers pose significant challenges for GDPR compliance, particularly as wearable health devices often operate on cloud-based infrastructure spread across multiple jurisdictions. GDPR restricts the transfer of personal data outside the European Economic Area (EEA) unless adequate protections are in place (Tikkinen-Piri et al., 2018; Goddard, 2017). Ensuring that data transferred across borders is protected by GDPR-level standards is particularly difficult given the varying privacy regulations across countries (Wright and De Hert, 2012; Covington and Carskadden, 2013). For example, the invalidation of the EU-U.S. Privacy Shield has left many companies in legal limbo, as existing mechanisms like Standard Contractual Clauses (SCCs) are complex to implement and enforce (Voigt and Von Dem Bussche, 2017; Tikkinen-Piri et al., 2018). Smaller wearable device companies often lack the resources to navigate these legal requirements, further complicating cross-border compliance (Granata et al., 2022). Researchers suggest that robust data protection strategies, such as using encryption for all data transfers



and limiting the storage of data in regions with weaker protections, can mitigate risks (Narayanan and Shmatikov, 2010; Wang et al., 2018). Additionally, binding corporate rules (BCRs) can be implemented to ensure that international transfers comply with GDPR standards (Hein, Vrijens and Hilgsmann, 2020; Tikkinen-Piri et al., 2018).

### 3.2. Technical solutions

Several technical solutions were proposed across the reviewed studies to address these GDPR challenges, with a focus on encryption, pseudonymization, and privacy-by-design. The Technical Solutions Comparison Table provides a detailed comparison of these solutions, outlining their strengths and weaknesses.

**Table 2.** Technical Solutions Comparison Table

| Technical Solution          | Strengths  | Weaknesses   |
|-----------------------------|--|--|
| End-to-End Encryption       | High level of data protection during transmission and storage. | Increases processing time and may reduce device performance. |
| Pseudonymization            | Helps in anonymizing personal data, reducing privacy risks.    | Potential for re-identification in large datasets.           |
| Privacy-By-Design           | Builds privacy considerations directly into the design phase.  | Can limit functionality and increase development costs.      |
| Multi-Factor Authentication | Provides an additional layer of security for user access.      | Can be cumbersome for users, leading to poor adoption.       |
| Blockchain Technology       | Enhances transparency and immutability of transactions.        | Still emerging and can be computationally intensive.         |

#### 3.2.1. End-to-end encryption

End-to-end encryption was found to be one of the most effective methods for securing sensitive health data during both transmission and storage. Studies such as those by Ioannidou and Sklavos (2021) and Wang et al. (2018) demonstrate that encryption significantly reduces the risk of unauthorized access and data breaches. However, the primary drawback is that encryption increases processing time and can negatively affect the performance of wearable devices, especially those requiring real-time data processing. This can create challenges in ensuring both security and usability in health monitoring applications.

#### 3.2.2. Pseudonymization

Pseudonymization is another critical tool for GDPR compliance, as it helps in anonymizing personal data and reducing privacy risks. This method allows for the separation of identifiers from

personal data, making it more difficult to re-identify individuals in large datasets (Narayanan and Shmatikov, 2010). Despite its advantages, pseudonymization is not foolproof; the potential for re-identification remains a concern, particularly in datasets that include indirect identifiers or when combined with external data sources.

#### 3.2.3. Privacy-by-design

Privacy-by-design is a proactive approach that integrates privacy considerations into the development phase of wearable devices (Cavoukian, 2010; Martínez-Pérez, De La Torre-Díez and López-Coronado, 2015). This strategy is highly effective in ensuring that devices comply with GDPR from the outset by minimizing data collection and embedding robust security features. However, implementing privacy-by-design principles can increase development costs and limit the functionality of devices, as it often requires careful balancing between privacy features and performance capabilities (Wright and De Hert, 2012).

#### 3.2.4. Multi-factor authentication

Multi-factor authentication (MFA) provides an additional layer of security by requiring users to verify their identity through multiple authentication factors. This method strengthens data protection and helps prevent unauthorized access, especially in health devices that collect highly sensitive data (Tikkinen-Piri et al., 2018). However, MFA can be cumbersome for users, leading to poor adoption and reduced user satisfaction. Ensuring ease of use while maintaining security is a key challenge with this approach.

#### 3.2.5. Blockchain technology

Blockchain technology has emerged as a promising solution for enhancing transparency and the immutability of transactions in wearable health devices (Kuner, 2020; Baldini et al., 2018). Blockchain's decentralized structure ensures that once data is recorded, it cannot be altered, providing a secure and transparent mechanism for data sharing. Despite these advantages, blockchain technology is still emerging and can be computationally intensive, which may hinder its widespread adoption in wearable devices that require lightweight, efficient processing (Granata et al., 2022; Butpheng, Yeh & Xiong, 2020).

### 4. Future Research

Future research should explore several key areas to enhance GDPR compliance in wearable health devices, particularly in sensitive health contexts. One critical area is remote health monitoring, where wearable devices are used to track real-time

data for chronic conditions like diabetes or cardiovascular diseases. Ensuring secure data transmission and compliance with GDPR, especially in telemedicine, is a priority. Moreover, Future research should focus on addressing the ethical and regulatory challenges associated with mental health wearables, particularly those designed to monitor mood, stress levels, and sleep patterns. Specifically, studies should explore innovative methods to ensure informed consent is both comprehensive and user-friendly, especially for individuals with a limited understanding of data privacy. Furthermore, research should investigate advanced techniques for data minimization, such as federated learning or differential privacy, to enhance user confidentiality without compromising device functionality or insights.

For wearables tailored to elderly care, future work should emphasize designing user interfaces and device functionalities that cater to senior users with limited technical literacy. This includes studying the effectiveness of simplified user interfaces, voice-controlled functionalities, and real-time caregiver notifications. In parallel, research should evaluate the efficacy of customized privacy frameworks and consent models that account for the cognitive and physical limitations often encountered by older adults.

Finally, in the context of wearable devices used in clinical trials, research should prioritize developing standardized protocols to ensure compliance with GDPR and other global data protection regulations. This includes creating dynamic consent mechanisms that allow participants to manage their data permissions over time and examining the feasibility of anonymized or pseudonymized data sharing to facilitate health research. Such studies should also assess the potential of wearable technologies to improve the accuracy, timeliness, and scalability of data collection in clinical settings. Collectively, these research areas will contribute to advancing privacy-centric and user-friendly wearable health technologies that align with ethical and regulatory standards while fostering innovation in healthcare and clinical research.

## 5. Conclusion

The findings of this review highlight both the opportunities and challenges associated with GDPR compliance in wearable health devices. As these devices increasingly become part of everyday health management, ensuring the protection of sensitive personal data is more crucial than ever. The technical solutions analyzed—such as end-to-end encryption, pseudonymization, privacy-by-design, multi-factor authentication, and blockchain technology—

are key in addressing the core GDPR principles of data security, minimization, and user consent. However, each of these solutions comes with significant trade-offs that must be carefully managed.

End-to-end encryption provides a robust security mechanism but can negatively impact device performance. This is particularly problematic in health wearables that rely on real-time data processing, such as glucose monitors and heart rate trackers. Thus, future innovations in encryption should focus on improving processing efficiency without compromising security.

Pseudonymization, though effective in reducing privacy risks, still carries the risk of re-identification, especially when combined with external data. This suggests a need for continuous refinement of anonymization techniques and more rigorous data governance to ensure that datasets remain de-identified in practice, not just theory.

Privacy-by-design presents an essential framework for ensuring that wearable devices are compliant with GDPR from the ground up. However, the increased costs and potential limitations in device functionality must be balanced carefully. Incorporating privacy features early in the design process can reduce long-term compliance costs, but manufacturers must also consider how these features impact user experience and device usability.

Multi-factor authentication (MFA) has been highlighted as a valuable tool in protecting user access to sensitive health data. However, its complexity can deter users from engaging with the technology, particularly when ease of use is a key selling point for many wearable devices. To ensure widespread adoption, future MFA solutions should focus on providing seamless and intuitive user experiences while maintaining the highest level of security.

Blockchain technology shows significant promise for improving transparency and the integrity of data transactions, especially in cross-border data transfers, which are a major GDPR concern. Yet, the computational intensity of blockchain makes it difficult to implement in devices that prioritize low energy consumption and lightweight processing. More research is needed to explore ways of integrating blockchain technology efficiently into wearable devices.

Furthermore, the right to be forgotten and cross-border data transfers remain particularly challenging to implement, given the global nature of data storage and the reliance of many wearable devices on cloud infrastructures. Organizations must improve their data retention policies and deletion mechanisms, ensuring that user data is fully erased from all servers, including backups, when

requested. Similarly, ensuring GDPR compliance in cross-border data transfers requires stricter adherence to standard contractual clauses, and more advanced encryption techniques to secure data as it moves between jurisdictions.

In light of these challenges, a multi-layered approach is recommended. A combination of privacy-by-design, robust encryption, secure authentication, and effective anonymization techniques is necessary to create a holistic data protection framework. Additionally, improving user awareness and simplifying consent processes will be crucial to ensure that individuals can make informed decisions about how their data is used and shared.

The review also underscores the need for ongoing monitoring and audits to ensure that wearable health devices remain compliant with evolving GDPR standards. As privacy regulations continue to develop and the capabilities of wearable technology expand, manufacturers and developers must stay proactive in their approach to data protection. Failure to address these challenges not only exposes organizations to legal risks but also undermines user trust, which is essential for the continued adoption of wearable health devices.

In conclusion, while significant progress has been made in developing solutions to enhance GDPR compliance, there remains considerable work to be done. Moving forward, manufacturers must focus on creating more efficient, user-friendly, and secure systems that protect sensitive health data without compromising the functionality of wearable devices.

#### Article Information / Makale Bilgileri

**Evaluation:** Two External Reviewers / Double Blind

**Değerlendirme:** İki Dış Hakem / Çift Taraflı Körleme

**Ethical Consideration:** As this study involved a review of existing literature and did not involve primary data collection, no formal ethical approval was required. However, ethical considerations were maintained by ensuring accurate representation of the findings and proper attribution to all original sources.

**Etik Beyan:** Bu çalışma mevcut literatürün gözden geçirilmesini içerdiğinden ve birincil veri toplamayı kapsamadığından, resmi bir etik onay gerekmemiştir. Bununla birlikte, bulguların doğru bir şekilde temsil edilmesi ve tüm orijinal kaynaklara uygun şekilde atıfta bulunulması sağlanarak etik hususlar korunmuştur.

**Similarity Screening:** Done – iThenticate and intihal.net

**Benzerlik Taraması:** Yapıldı – iThenticate ve intihal.net

**Ethical Statement / Etik Bildirim:** [health@artuklu.edu.tr](mailto:health@artuklu.edu.tr)

#### Authorship Contribution/ Yazar Katkıları:


|   |           |
|---|-----------|
| Research Design (CRediT 1)                                | MÖ (100%) |
| Data Collection (CRediT 2)                                | MÖ (100%) |
| Research - Data Analysis - Verification (CRediT 3-4-6-11) | MÖ (100%) |
| Writing the Article (CRediT 12-13)                        | MÖ (100%) |
| Development and Revision of the Text (CRediT 14)          | MÖ (100%) |


**Conflict of Interest:** No conflict of interest declared.

**Çıkar Çatışması:** Çıkar çatışması beyan edilmemiştir.

**Financing:** No external funding was used to support this research.

**Finansman:** Bu çalışma sırasında herhangi bir finansal destek alınmamıştır.

**Copyright & Licence:** The authors own the copyright of their work published in the journal and their work is published under the CC BY-NC 4.0 licence 

**Telif Hakkı & Lisans:** Yazarlar dergide yayınlanan çalışmalarının telif hakkına sahiptirler ve çalışmaları CC BY-NC 4.0 lisansı altında yayımlanmaktadır. 

#### References

- Abernethy, A., Adams, L., Barrett, M., Bechtel, C., Brennan, P., Butte, A., Faulkner, J., Fontaine, E., Friedhoff, S., Halamka, J., Howell, M., Johnson, K., Long, P., McGraw, D., Miller, R., Lee, P., Perlin, J., Rucker, D., Sandy, L., Savage, L., ... Valdes, K. (2022). The Promise of Digital Health: Then, Now, and the Future. *NAM perspectives*, 2022, <https://doi.org/10.31478/202206e>.
- Baldini, G., Botterman, M., Neisse, R., and Tallacchini, M. (2018). Ethical design in the Internet of Things: Privacy and data protection by design and default. *Computer Law & Security Review*, 34(3), 602-616. <https://doi.org/10.1007/s11948-016-9754-5>
- Butpheng, C., Yeh, K. -H., & Xiong, H. (2020). Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry*, 12(7), 1191. <https://doi.org/10.3390/sym12071191>
- Cavoukian, A., Taylor, S., and Abrams, M. E. (2010). Privacy by Design: Essential for organizational accountability and strong business practices. *Identity in the Information Society*, 3, 405-413. <https://doi.org/10.1007/s12394-010-0053-z>
- Covington, M. J., and Carskadden, R. (2013, June). Threat implications of the Internet of Things. In 2013 5th international conference on cyber conflict (CYCON 2013) (1-12). IEEE.
- European Union. (2016). General Data Protection Regulation (GDPR). *Official Journal of the European Union*, L119/1.
- Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á., & Toval, A. (2013). Security and privacy in electronic health records: a systematic literature review. *Journal of biomedical informatics*, 46(3), 541-562. <https://doi.org/10.1016/j.jbi.2012.12.003>
- Galvin, H. K., & DeMuro, P. R. (2020). Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019. *Yearbook of medical informatics*, 29(1), 32-43. <https://doi.org/10.1055/s-0040-1701987>
- Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705. <https://doi.org/10.2501/IJMR-2017-050>



- Granata, F., Di Nunno, F., and de Marinis, G. (2022). Stacked machine learning algorithms and bidirectional long short-term memory networks for multi-step ahead streamflow forecasting: A comparative study. *Journal of Hydrology*, 613, 128431. <https://doi.org/10.1016/j.jhydrol.2022.128431>.
- Hein, A. E., Vrijens, B., and Hilgsmann, M. (2020). A digital innovation for the personalized management of adherence: Analysis of strengths, weaknesses, opportunities, and threats. *Frontiers in Medical Technology*, 2, 604183. <https://doi.org/10.3389/fmedt.2020.604183>
- Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>
- Ioannidou I, Sklavos N. On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. *Cryptography*. 2021; 5(4):29. <https://doi.org/10.3390/cryptography5040029>
- Kazanskiy, N. L., Khonina, S. N., and Butt, M. A. (2024). A review on flexible wearables-Recent developments in non-invasive continuous health monitoring. *Sensors and Actuators A: Physical*, 114993. <https://doi.org/10.1016/j.sna.2023.114993>
- Kuner, C. (2020). The GDPR and International Organizations. *AJIL Unbound*, 114, 15–19. <https://doi:10.1017/aju.2019.78>
- Martínez-Pérez, B., De La Torre-Díez, I., and López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems*, 39, 1-8. <https://doi.org/10.1007/s10916-014-0181-3>
- Narayanan, A., and Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information". *Communications of the ACM*, 53(6), 24-26. <https://doi.org/10.1145/1743546.1743558>
- Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, 140(4), 32-48. [https://doi.org/10.1162/DAED\\_a\\_00113](https://doi.org/10.1162/DAED_a_00113)
- Paul, G., and Irvine, J. (2014, September). Privacy implications of wearable health devices. In *Proceedings of the 7th International Conference on Security of Information and Networks* (117-121). <https://doi.org/10.1145/2659651.265968>
- Roehrs A, da Costa C, da Rosa Righi R, de Oliveira K Personal Health Records: A Systematic Literature Review *J Med Internet Res* 2017;19(1):e13 <https://doi.org/10.2196/jmir.5876>
- Setnan, A.R., Schneider, I., & Green, N. (Eds.). (2018). *The Politics and Policies of Big Data: Big Data, Big Brother?* (1st ed.). Routledge. <https://doi.org/10.4324/9781315231938>
- Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880.
- Sokolova, A. (2021). Risk perception and personality characteristics as determinants in the use of mHealth technology in the context of personal fitness (Bachelor's thesis, University of Twente).
- Stewart, L. (2019). Big data discrimination: Maintaining protection of individual privacy without disincentivizing businesses' use of biometric data to enhance security. *BCL Rev.*, 60, 349.
- Syu, J. H., Lin, J. C. W., Srivastava, G., and Yu, K. (2023). A comprehensive survey on artificial intelligence empowered edge computing on consumer electronics. *IEEE Transactions on Consumer Electronics*. <https://doi.org/10.1109/TCE.2023.3318150>
- Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8. [https://doi.org/10.1016/S1353-4858\(16\)30056-3](https://doi.org/10.1016/S1353-4858(16)30056-3)
- Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, 129, 104130. <https://doi.org/10.1016/j.compbiomed.2020.104130>
- Tene, O., and Polonetsky, J. (2011). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online*, 64, 63.
- Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. <https://doi.org/10.1016/j.clsr.2017.05.015>
- Voigt, P., and Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR). A practical guide*, 1st ed. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-57959-7>
- Wang, Y., Kung, L., Wang, W.Y.C., and Cegielski, C.G. (2018). An integrated big data analytics-enabled transformation model: Application to health care. *Information & Management*, 55(1), 64-79. <https://doi.org/10.1016/j.im.2017.04.001>
- Wright, D., and De Hert, P. (2012). *Introduction to privacy impact assessment. In Privacy impact assessment* (pp. 3-32). Dordrecht: Springer Netherlands. <https://doi.org/10.1007/978-94-007-2543-0>