

## The use of Artificial Intelligence in Protecting Sensitive Personal Data of a Healthy Nature in International Law - The Case of European Legislation -

استخدام الذكاء الاصطناعي في حماية البيانات الشخصية الحساسة ذات الطبيعة

الصحية في القانون الدولي - حالة التشريع الأوروبي -

Gouasmia Siham

Mohamed-Cherif Messaadia University - Souk Ahras

s.gouasmia@univ-soukahras.d

Date of submission:26/06/2024 Date of final acceptance:8/02/2025 Date of publication :mars 2025

### Abstract:

AI in healthcare is a double-edged sword, offering advancements in diagnosis, treatment, and research but raising privacy concerns regarding sensitive health data. European law addresses this by safeguarding citizen data. The (GDPR) empowers individuals with control over their health data, including access, rectification, and erasure rights.

The new Artificial Intelligence Act (AIA) builds on GDPR by setting stricter rules for high-risk AI, especially in healthcare. These regulations aim for transparency in AI use, data minimization to limit collection from each infected person, and robust security for health data. Overall, European legislation strives to balance AI's potential with health data protection.

**Keywords:** Healthy Data, Pandemics, EU Legislation, Artificial Intelligence.

ملخص:

يُمثل الذكاء الاصطناعي في مجال الرعاية الصحية سلاحًا ذا حدين، فهو من ناحية يُقدم إمكانيات هائلة للتقدم في التشخيص والعلاج والبحث الطبي، بينما يُثير من ناحية أخرى مخاوف جدية بشأن خصوصية البيانات الحساسة. ولذلك، يُعالج القانون الأوروبي هذه المسألة المُعقدة من خلال إعطاء الأولوية لحماية بيانات المواطنين. إذ تُشكل اللائحة العامة لحماية البيانات (GDPR) حجر الأساس في هذا الجهد، حيث تُتيح للأفراد تحكمًا شاملًا في معلوماتهم الصحية، بما في ذلك حقوق الوصول إليها وتصحيحها وحذفها.

كما يكمل قانون الذكاء الاصطناعي الجديد (AIA) اللائحة العامة لحماية البيانات (GDPR) من خلال وضع قواعد أكثر صرامة لأنظمة الذكاء الاصطناعي عالية المخاطر، خاصة تلك المستخدمة في مجال الرعاية الصحية، إذ تهدف هذه اللوائح إلى تحقيق الشفافية في استخدام الذكاء الاصطناعي، وتقليل البيانات للحد من جمعها من كل شخص مصاب و توفير الأمان القوي للبيانات الصحية. و بشكل عام، تسعى التشريعات الأوروبية إلى تحقيق التوازن بين إمكانيات الذكاء الاصطناعي وحماية البيانات الصحية.

الكلمات المفتاحية: البيانات الصحية، الأوبئة، تشريعات الاتحاد الأوروبي، الذكاء الاصطناعي.

Auteur correspondant : Gouasmia Siham

## Introduction:

The rise of artificial intelligence (AI) in healthcare presents a double-edged sword. While it can revolutionize medical research, diagnosis, and treatment, its use raises concerns about the privacy of sensitive health data. European legislation takes a proactive approach, aiming to harness the benefits of AI while safeguarding citizen privacy.

The (GDPR), the bedrock of European data protection, encompasses all health data, including details pertaining to an individual's physical and mental well-being, genetic makeup, and wellness practices, and empowers individuals with a comprehensive set of rights, including access, rectification (correction of inaccurate data), and erasure (deletion under specific circumstances). The recently adopted Artificial Intelligence Act (AIA) builds on the GDPR framework, categorizes AI systems based on their risk level. High-risk systems, which include those used in healthcare, face stricter regulations.

These regulations aim to ensure Transparency where Individuals should understand how AI is used in their healthcare and how it might affect them. Also, Data minimization, that only the minimum amount of data necessary should be collected and used for AI applications. And Security, Health data must be protected against unauthorized access, use, disclosure, disruption, or destruction.

The intersection of artificial intelligence (AI) and health data presents a complex landscape in European legislation. While AI offers immense potential for healthcare advancements, concerns linger regarding privacy and misuse of sensitive health information. **So what legal mechanisms The European Union has demonstrated with a strong commitment to striking a balance between safeguarding personal data and preserving public health during times of pandemics?**

The importance of this research lies in highlighting the European legislation that regarding AI in healthcare, where acknowledges the potential of AI to revolutionize healthcare but emphasizes concerns about privacy breaches for sensitive health data. It also underscores the European Union's proactive efforts to harness AI's benefits while safeguarding data privacy for citizens. From this standpoint, we can answer the problematic of this research in the following points:

### I- GDPR: as a Pillar of Data Privacy

The European Union (EU) established the (GDPR) Regulation N° 2016/679 as a cornerstone of data protection across the Union. It applies to all forms of Individual information, encompassing health records, that reveals details regarding a person's physical and mental well-being, genetic makeup, and wellness habits<sup>1</sup>. The GDPR empowers individuals with a comprehensive set of rights, including: the right to access, where Individuals can request and obtain copies of their health data held by organizations<sup>2</sup>. Along with the right to rectification, individuals hold the right to challenge the accuracy and completeness of their health data<sup>3</sup>. Furthermore, the right to erasure, also known as the right to be forgotten, grants individuals the ability to request the deletion of their health data<sup>4</sup>. These rights grant individuals significant control over their health information.

#### 1- Protection of personal data of a healthy nature through mobile applications:

Healthy data on the mobile applications is particularly sensitive, and protecting it is crucial. Health data reveals a lot about a person, including conditions, medications, and habits. Where breaches can lead to discrimination, identity theft, and even affect insurance rates. Therefore, the protection of this data must be based on a solid legal basis.

### **A. Legal basis for data processing by installing applications and storing information on the user's device**

Under Article 5 E-Privacy Guidelines, storing Content on a user's device is generally restricted. It's only permitted when the user explicitly grants consent, or when storage and access are strictly necessary for the operation of an information society service (like an application) explicitly requested by the user. This typically applies to storing data needed for apps to function properly. However, exceptions exist. Contact tracing apps may require storing temporary information like periodically changing user identifiers for those in close proximity. Additionally, uploading proximity data for contact tracing purposes might be necessary, even if not essential for the app's core functionality. In such cases, specific requirements beyond basic operation need to be met (2) While the previously mentioned conditions for information storage haven't been fulfilled, relying on user consent (option 1) remains the most suitable justification for such activities. However, the General Data Protection Regulation (GDPR) stipulates that consent must be "freely given, specific, informed and unambiguous." This means it requires a clear affirmative action from the individual, excluding implicit forms of consent such as silence or inaction<sup>5</sup>.

### **B. Legal Frameworks for National Health Authorities' Use of Health Data :**

National health authorities typically process personal data based on legal obligations outlined in EU or Member State laws. This aligns with the requirements set forth in Articles 6(1)(c) and 9(2)(i) of the GDPR, and can also be justified when processing is necessary for a public interest recognized by EU or Member State law<sup>6</sup>.

However, any national law implementing such processing must provide robust safeguards to protect individuals' rights and freedoms. The greater the potential impact on individuals' freedoms, the stricter these safeguards need to be. Existing pre-pandemic EU and Member State laws, as well as those specifically enacted to combat pandemics, can serve as legal grounds for data processing if they allow for epidemiological surveillance and comply with the additional requirements of Article 6(3) of the GDPR<sup>7</sup>.

Therefore, in order to ensure a coherent approach throughout the EU and the Directive for Member States and Application Developers, it is necessary to identify the requirements through which applications should meet the guarantee this approach to ensures alignment with European Union (EU) privacy and personal data protection legislation, specifically the General Data Protection Regulation (GDPR) and the existing Privacy Directive. It focuses solely on compliance with these overarching regulations, excluding any additional restrictions Member States might have incorporated into their national laws regarding health data processing. The current guidelines also address only voluntary applications that support the fight against the COVID 19 pandemic. Mobile applications<sup>8</sup> are one of the main technologies used by governments and commercial companies to contain the pandemic and achieve many goals. Most countries have developed applications to facilitate awareness and tracking of communication. Some countries have invested in developing these applications in the following:

- \* Demographic information: (collection of information, sensitization, provision of general instructions to avoid infection, mapping to avoid disease outbreaks).
- \* Medical assistance: (self-diagnosis, reporting, information related to access to health services).
- \* Monitoring citizens' crowds and reporting violations of relevant legal rules by means of: mandatory and non-mandatory digital applications, imposed quarantine, travel forms during quarantine, travel mapping, tracking vehicle movements for reasons beyond transportation management, monitoring interactions to identify potential disease spread)<sup>9</sup>.

The sensitive nature of health data and the purpose for which it's processed necessitate applications designed to place national health authorities as the overseeing bodies. This aligns with the GDPR's principle of accountability, ensuring these authorities bear responsibility for data protection. Additionally, access to this data should be strictly limited based on several key principles, with the most critical being the minimization of disclosure and data access itself :

- ✓ Any information stored in the final equipment cannot be shared, however, access by health authorities should be strictly limited to the communication function itself. This function acts solely as a communication channel, and health authorities won't have access to any additional data beyond what's necessary for facilitating communication.
- ✓ The Symptom Detector function can guide citizens on testing recommendations, quarantine guidance, and healthcare access, particularly for at-risk groups. This information, along with data collected by national authorities, can be used to understand COVID-19 infection rates and potentially complement primary care monitoring. In such cases, responsible health authorities and national epidemiological authorities may be granted access to the information provided by patients, while the health center can receive data for epidemiological surveillance. However, if health officials need to be contacted, disclosing app users' phone numbers to national health authorities is necessary<sup>10</sup>.

These applications contribute significantly to the fight against COVID-19. The symptom checker guides citizens on testing, self-isolation (quarantine), and minimizing transmission when seeking healthcare. It can also complement primary care monitoring and improve reporting of COVID-19 infection rates within the population. Additionally, contact tracing and warning features help identify individuals who have been in close contact with infected persons, allowing them to take informed steps like self-quarantine, testing, or symptom management<sup>11</sup>, within the framework of the electronic cloud system.

Cloud computing or e-cloud is an important part of the optimal protection of patients' health information. The cloud can achieve the combination of flexibility and choice that is needed to maximize patient care while minimizing cost and enhancing security and privacy with minimal effort. Despite increased awareness that improving access to data may help save lives, health IT systems are still increasing. These systems are often unable to ensure timely and accurate data delivery is crucial for maintaining data quality, efficiency and safety of patient care, and limits patients' ability to access and control their data, as well as their access to health data across different care and treatment providers<sup>12</sup>.

Under the Directive Law on Electronic Privacy, Cloud-based applications can ensure secure and confidential communication for users, which stipulated<sup>13</sup> can only be imposed through a necessary, appropriate and appropriate law in order to protect certain objectives. Therefore, due to the high degree of intervention of this method and the challenges it entails in terms of establishing appropriate safeguards, given the potential complexities, the committee recommends a cautious approach, requiring thorough analysis before utilizing this option. This is particularly relevant for applications that depend on voluntary participation, as success hinges on user buy-in, must be used, because this Directive Law does not include applications aimed at imposing mandatory quarantine requirements. Thus, voluntary downloadable applications offer a range of functionalities to support the fight against COVID-19. These include:

\*Providing accurate and up-to-date information to users about the pandemic and preventative measures.

\*Symptom checkers that guide individuals through self-assessment questionnaires and offer relevant advice.

\*Contact tracing and alert functions that notify users who may have been in close proximity to someone infected, advising them on self-quarantine, testing options, and available resources.

\*Telemedicine features facilitating communication between patients and healthcare professionals, enabling remote diagnosis and treatment advice<sup>14</sup>.

On this basis, health care providers and related organizations find that their policies based on electronic withdrawals clash with outdated legal restrictions, which prevent them from launching full services related to patient care and public health. For example, there are cases that are ostracized for laws that still consider outsourcing data processing to be a breach of patient confidentiality, even when the data provider is a reliable guardian, as it is legally prohibited to do anything using data unless instructed to do so by the patient or the health care institution, and addressing these barriers is imperative for all institutions<sup>15</sup>.

To the extent that cloud computing can improve care in terms of “primary” use, public policymakers should remove regulatory barriers, relying on policies that use electronic clouds, as it is right for many reasons that are not less efficient, to promote cross-border care and a “digital single market” for health, although the attitudes of different populations towards secondary use that should be licensed and how it should be used may differ, as there is a need for more public participation on secondary uses of patient data, including its value, risks and safeguards, and the appropriate degree of patient monitoring<sup>16</sup>.

Cloud-based policies enable better patient care and public health outcomes, as the health innovation guaranteed by cloud computing has enormous potential to improve human health. By enabling the intelligent, efficient and secure use of patient data, cloud computing is transforming many aspects of contemporary health care across Europe for the benefit of patients and citizens at large. Organizations working to save lives and improve health outcomes benefit from cloud computing not only when caring for patients through the “primary use of data”, but also when reusing patient data for public health purposes, research and innovation known as “secondary use”. European legislators have decided that primary uses of patient data naturally include diagnosis, patient care, as well as Health insurance systems play a crucial role in managing healthcare services. This includes ensuring the quality and cost-effectiveness of procedures, while also settling claims for benefits and services by:

- Enhanced patient participation.
- Enable healthcare professionals to be more productive and efficient.
- Using smart devices to achieve health care.
- Optimize clinical and operational effectiveness<sup>17</sup>.

## **2. Protection of personal data of a healthy nature through other digital solutions:**

Regarding national health authorities, which are identifying the data controller, the entity ultimately responsible for processing decisions and compliance with EU data protection regulations, is crucial for public health institutions. This clarity determines who informs individuals about their data, who downloads the application that collects pre-existing or newly generated data (like data from the smartphone itself), what rights individuals have regarding their data, and who bears responsibility for data breaches.... etc)<sup>18</sup>.

Private organizations are therefore working to create their own plans by introducing more controls in order to comply with government measures and protect their employees. Comprehensive enforcement of laws entails privacy-invasive measures such as interrogating individuals about their professional and private travel plans, conducting temperature checks and keeping health records along with information about potential contact with injured individuals outside the workplace. Since these procedures involve processing various types of personal data - including health data – so protecting privacy and data is critical in its dissemination, meaning that organizations should be aware that some measures have an impact on individuals' privacy and that they have the option to locate the line between safety measures that benefit public health and controls that affect individuals' privacy.<sup>19</sup> Other digital solutions and tools, often developed without specific legislation, can then be outlined to help monitor the spread of the viruses:

- \* Sites that provide health questionnaires.
- \* Use electronic bracelets.
- \* Use smart cameras for facial recognition.
- \* Thermal assays.
- \* Remote control of drones and robots.
- \* Mandatory virus testing<sup>20</sup>.

The Data Protection Authority has stated in this framework that organizations and employers may not rely on explores the legal grounds for processing public health data, excluding the specific exception outlined in Article 9(2)(i) of the GDPR, if they are implementing explicit instructions issued by government authorities, and therefore this authority advises organizations not to. The Data Protection Authority emphasizes that employers cannot "systematically and regularly" monitor or collect employee health data beyond official public health measures. This highlights the need for data processing related to COVID-19 prevention to adhere to all the fundamental principles outlined in Article 5 of the General Data Protection Regulation (GDPR). These principles include principles like purpose limitation, data minimization, and storage limitation, ensuring data collection is proportionate and adheres to strict privacy guidelines<sup>21</sup>.

#### **A- Contact tracing and warning function for injured person data:**

The applications generate randomly altered and periodically changing ephemeral identifiers for phones that contact the user periodically. One option available is to store these items on the user's device (so-called decentralized processing). Two approaches exist for storing proximity data. One option involves storing anonymized identifiers on a central server accessible by health authorities (back-server solution). However, a decentralized approach might be preferable. In this scenario, health authorities would only access proximity data directly from the infected individual's device, enabling them to contact potentially exposed persons. Crucially, this data would only be accessible after the infected person (post-testing) chooses to share it proactively. Additionally, the infected person wouldn't be informed about the identities of those potentially exposed who will be alerted<sup>22</sup>.

In all cases where Big Data poses unique data protection challenges because large datasets can be used to profile and predict individual behavior, and even anonymized data can sometimes be linked back to specific people. To address this, we need new methods that balance data privacy (which requires clear purposes for data use) with the exploratory nature of data science. This is an ongoing effort, but some promising areas include data minimization, strong anonymization techniques, and clear data usage policies<sup>23</sup>.

**B- Communication tracking and warning function For contact tracing data concerning those who may have been exposed to the infected person :**

Epidemiological principles emphasize protecting the infected person's identity from those they've been in contact with. Instead, these contacts are informed only of potential exposure during the past 16 days, allowing them to take appropriate precautions. Here, data related to the time and place of these communications should not be stored, and therefore the delivery of that data is not possible. Epidemiological communications cannot be traced to a User of an electronic application who has tested positive. National health authorities should receive limited data for contact tracing purposes. This data should only include the identities of those who had potential exposure to an infected person within a specific timeframe (48 hours before symptom onset to 14 days after) based on the closeness and duration of their contact. Additionally, national authorities can share anonymized, aggregated contact tracing data with a central body for epidemiological surveillance in collaboration with member states. This approach protects individual privacy while allowing for effective public health monitoring<sup>24</sup>.

**C- Ensuring that the individual remains under surveillance**

Building trust with users is paramount for the success of contact-tracing apps. The European Commission emphasizes several key conditions to achieve this:

**\*Voluntary Participation and Granular Consent:**

Installing the app must be voluntary and without consequences for those who choose not to. Users should be able to grant specific consent for each app function (information, symptom check, contact tracing) instead of forced bundling. However, the option to combine functionalities if offered by the provider should still be available.

**\*User Control of Data Sharing:**

Proximity data, collected through Bluetooth signals, should be stored on the user's device. Sharing with health authorities should only occur after a positive COVID-19 test and with the user's explicit consent. Health authorities must provide clear information about data processing according to relevant regulations.

**\*Guaranteed GDPR Rights:**

Users must retain all their GDPR rights, including access, correction, and deletion of their data.

**\*Proportionate Restrictions:**

Any limitations on GDPR rights must be strictly necessary, proportionate, and legally compliant.

**\*App Deactivation upon Pandemic Control:**

Apps should be automatically deactivated once the pandemic is declared under control, regardless of user action<sup>25</sup>.

The sensitive nature of health data, categorized as special personal data under GDPR, necessitates a legal basis for processing during the COVID-19 pandemic. This legal approach fosters legal certainty by achieving several objectives:

**\*Transparency and Defined Purpose:**

Specific legislation would clearly define the types of health data processed and the exact purposes for which it is used.

**\*Clear Data Controller and Access:**

The legislation would explicitly identify the data controller (entity responsible for processing) and restrict access to authorized personnel.

**\*Limited Purposes:**

Processing would be restricted to the purposes defined in the legislation, preventing unauthorized use of the data.

**\*Robust Safeguards:**

The legislation would establish safeguards to ensure that data processing does not undermine public interest or negatively impact app adoption.

**\*Inclusive Design:**

National legislators would be obligated to design solutions that are accessible and inclusive for all citizens<sup>26</sup>.

**II- The The European Union's AI Act:**

Building on the GDPR, The European Union's (AIA) <sup>27</sup> is a ground-breaking piece of legislation that regulates the development, deployment, and use of artificial intelligence (AI) systems across the European Union. Passed in March 2024, it represents the first ever comprehensive legal framework for The emergence of AI as a global phenomenon<sup>28</sup>.

The (AI Act) strikes a balance between fostering responsible AI development and minimizing burdens on businesses. It establishes clear rules and obligations for developers and deployers regarding specific high-risk AI applications. However, the act also strives to streamline regulations, particularly for small and medium-sized enterprises (SMEs), to reduce administrative and financial complexities. This focus on responsible AI development is further supported by the AI Act's inclusion within a broader policy package that promotes trustworthy AI, including the AI Innovation Package<sup>29</sup>.

The recently enacted AI <sup>30</sup> Act (EU Regulation 2024/...) builds upon the existing GDPR framework. This act categorizes AI systems based on their potential risk level. AI systems used in healthcare, due to the sensitivity of the data involved, are often classified as high-risk<sup>31</sup>. For these high-risk systems, the AIA mandates stricter regulations to ensure Transparency, Data minimization and Security. We can see more details for that, in the features of The AIA's act.

## 1- Central Elements of AI Regulation in the EU:

European Union's AIA recognizes the sensitivity of health data and implements several key provisions to safeguard it:

**A- Risk-Based Approach:** The High-risk systems, which include those used in healthcare, finance, and law enforcement, face stricter regulations<sup>32</sup>.

The EU's AIA adopts a risk-based approach, tailoring regulations to the potential harm an AI system can cause. This ensures stricter controls for high-risk systems, such as those in critical sectors or with potential for bias, while minimizing regulatory burdens for low-risk applications. The AIA categorizes AI systems into four risk levels:

\*unacceptable, high, limited, and minimal (or no) risk<sup>33</sup>.

\* AI Systems Posing Significant Risks: These systems are subject to the most stringent regulations due to their potential for significant impact on people's lives. Examples include AI used in:

-Healthcare: Diagnosing diseases, recommending treatments, or controlling medical devices<sup>34</sup>.

-Finance: Providing financial advice, granting loans, or high-frequency trading.

\*Stricter Regulations for High-Risk Systems: Compared to lower risk categories, high-risk AI systems face:

- ✓ Mandatory conformity assessments: These assessments verify the system complies with the AIA's requirements before it can be placed on the market.
- ✓ More extensive transparency obligations: Developers need to provide detailed information about the system's purpose, intended use, and potential risks.
- ✓ Human oversight: In some cases, human intervention might be necessary for critical decisions made by the AI system<sup>35</sup>.

### - Classifying AI Systems by Risk Level:

The AIA employs a risk-based approach, classifying AI systems based on their potential for harm. Healthcare AI applications, due to their potential impact on patient safety and well-being, will likely fall under various risk categories in the AIA, due to the nature of the data it uses, typically falls under the "high-risk" category<sup>36</sup>.

### - Stricter Requirements for High-Risk AI:

**\*Focus on Purpose Specification, Transparency and Explainability:** The AIA emphasizes the need for transparency in AI systems. Individuals have the right to understand how AI is being used in decision-making processes that affect them. The AIA mandates clear communication on how AI is used in healthcare and the intended purpose of data collection. Individuals have the right to understand how AI might impact their diagnosis, treatment, or access to services<sup>37</sup>.

**\*Data Minimization and Security:** The AIA promotes collecting and using only the minimum amount of data necessary for an AI application to function. This reduces the amount of sensitive data stored and minimizes the potential for breaches<sup>38</sup>.

**- Robust Security Measures:**

Additionally, it mandates robust security measures to safeguard sensitive data. where The AIA requires organizations developing and using AI in healthcare to implement robust security measures to protect health data from:

\*Unauthorized access (e.g., hacking)

\* Unintended use or disclosure

\*Disruption or destruction of data<sup>39</sup>.

**B- Prohibition of Specific High-Risk Applications, Striking a Balance:**

The AIA bans certain AI applications in healthcare that could exploit sensitive data for discriminatory or unethical purposes, where it prohibits certain high-risk AI applications altogether, particularly those that exploit sensitive data for:

- **Biometric Categorization:** This refers to assigning individuals to categories based on their health information, such as genetic predisposition to diseases. This could lead to discrimination in insurance or employment.

- **Social Scoring:** Creating a score that could influence access to healthcare, insurance, or other benefits based on an individual's health data raises ethical concerns about potential bias and discrimination<sup>40</sup>.

**2- Additional Considerations for AIA :**

A- **Alignment with GDPR:** The AIA complements the existing (GDPR) by specifically addressing AI's impact on personal data. While the GDPR grants individuals robust rights concerning their health data, such as access, correction, and deletion, the AIA focuses on regulating how AI systems process this data in the first place (Art. 15, 16 & 17 GDPR)<sup>41</sup>.

B- **Human Oversight:** While the AIA focuses on technical safeguards, it emphasizes the importance of human oversight in AI development and deployment, particularly in healthcare settings. This ensures responsible decision-making and accountability<sup>42</sup>.

**3- The AIA framework for responsible AI development, fostering trust and promoting innovation in Europe:**

The AIA offers a framework for responsible AI development, fostering trust and promoting innovation in Europe. It empowers individuals with control over their data and safeguards their privacy. However, challenges remain:

**A- Implementation:** Ensuring consistent enforcement across EU member states requires ongoing efforts from data protection authorities.

Ensuring consistent enforcement of data protection regulations across the European Union (EU) is an ongoing challenge. While EU regulations provide a common framework, member states have some flexibility in how they implement them. This can lead to differences in how data protection authorities (DPAs) interpret and enforce the rules. Additionally, DPAs in different countries may have varying levels of resources and expertise, creating inconsistencies in their enforcement capabilities.

Further complicating matters is the free flow of data across borders within the EU. When data breaches or other violations involve multiple jurisdictions, investigations become complex. Different DPAs need to cooperate effectively to share information, coordinate enforcement actions, and provide mutual assistance. Several efforts are underway to promote a more unified approach to data protection enforcement:

**\*The European Data Protection Board (EDPB):** This EU body plays a key role in ensuring consistent application of the GDPR across member states. They provide guidance and facilitate cooperation between DPAs. The EDPB also helps resolve disputes that may arise between different data protection authorities.

**\*Cooperation Mechanisms:** DPAs are required to cooperate on investigations that involve multiple jurisdictions. This includes sharing information, coordinating enforcement actions, and providing mutual assistance. Clear communication and collaboration are essential for effective cross-border enforcement.

**\*Consistency Mechanisms:** The GDPR includes mechanisms for resolving disagreements between DPAs. This ensures a unified approach to enforcement, even in complex cases that span multiple countries. Here we can say that achieving consistent enforcement of data protection regulations in the EU requires ongoing efforts from various stakeholders. The EDPB<sup>43</sup>, cooperation mechanisms, and consistency tools play a crucial role in promoting a unified approach. However, challenges remain due to national variations in implementation and resource disparities among member states<sup>44</sup>.

**B- Exemptions:** The AIA allows exemptions for law enforcement, raising concerns about potential privacy intrusions in those situations (Article 8 AIA).

We can say that there is a Specific AI Systems, because Article 8 allows member states to exempt certain AI systems used by law enforcement from some of the AIA's stricter regulations. These potentially exempted systems include Biometric Identification Systems (RBIS), These systems use facial recognition, fingerprint analysis, or other methods to identify individuals. Exemptions could apply to RBIS used in public spaces for specific purposes, such as searching for missing persons or preventing terrorism. Also Other High-Risk AI Systems, where The AIA categorizes some AI systems used in law enforcement as high-risk. While the specific applications aren't explicitly defined, exemptions from some regulations might be possible for these as well.

However The European Court of Human Rights emphasizes that personal data protection is crucial right to privacy, enshrined in Article 8 of the European Convention, was emphasized in the case of S. and Marper v. the U K. the need for strong legal safeguards to prevent misuse of personal data, especially when it's automated or used for law enforcement. These safeguards should ensure data is relevant, limited, securely stored, and not kept longer than necessary<sup>45</sup>.

Whereas Biometrics traditionally focused on verifying a person's identity using physical traits like fingerprints or iris scans. Now, however, biometric data and systems are increasingly going beyond identification to profile and categorize people. Biometric technologies typically consist of sensors (hardware) and algorithms (software) working together to capture biometric data (e.g. fingerprints) and analyze it for verification or other purposes<sup>46</sup>.

### III- Regulation 2024/886 as a recent Regulations:

There have been regulations passed in 2024, such as Regulation 2024/886 regarding instant credit transfers. While it is a recent development in the EU, doesn't directly focus on health data protection. Its primary objective is to improve the speed and standardization of euro payments within the member states (Section A). This regulation concerns financial data like account numbers, transaction amounts, and currencies.

#### 1- The relationship between the regulation 2024/886 and healthy data protection

We can find the relationship between this regulation and health data protection in this points:

**A- Regulation 2024/886:** Deals with the speed and standardization of euro payments within the EU. It focuses on financial data like account numbers, transaction amounts, and currencies.

AI and machine learning are increasingly used in important decisions like loan approvals and parole placements. These algorithms can be biased and lack transparency, but they also have the potential to be more fair and accurate than current methods. The financial services industry, with its existing regulations, is a good case study for how to manage the risks and benefits of AI. Researchers are looking into tools to analyze these algorithms and ensure they are fair, reliable and transparent. Finding the right balance between automation and human oversight is crucial. More discussion is needed on consumer experience, fairness, and managing risks. This can help us develop AI-powered financial services that are both accurate and fair<sup>47</sup>.

**B- Safeguarding Personal Health Information:** The European legal landscape for health data protection is anchored in two key regulations: the (GDPR) and the upcoming A I Act. Both regulations work in tandem to safeguard sensitive information about a person's health, encompassing both physical and mental health data. The GDPR establishes a strong foundation for individual rights and data control, while the AIA focuses on how AI systems process this sensitive data in the first place, like genetic makeup, and wellness habits (Section B).

#### 2- The connections between the regulation 2024/886 and healthy data protection

Despite not directly targeting health data, there are some tangential connections between Regulation 2024/886 and health data protection. The emphasis on robust technical security standards within the new regulation could indirectly benefit health data security (Section 2A). This is especially true if the same infrastructure is used for both healthcare payments and financial transactions related to medical services. Additionally, the focus on transparency in fees within Regulation 2024/886 aligns with the principles of the GDPR<sup>48</sup>.

While not directly related to health data, this transparency can encourage similar initiatives in the health data sector, promoting user awareness about data collection practices, some connections can be drawn:

**A- Security Infrastructure:** The emphasis on robust technical standards in Regulation 2024/886 could indirectly benefit health data protection if the same infrastructure is used for healthcare payments or financial transactions related to medical services (Article 3(2) & Annex I)<sup>49</sup>.

Since storing data inherently brings the risk of breaches by insiders or outsiders, organizations should be cautious about collecting sensitive information like ethnicity, religion, or sexual orientation. A breach of such data could have severe consequences, so a strong data security policy should prioritize minimizing collection of sensitive data like healthy data whenever possible<sup>50</sup>.

**B- Focus on Transparency:** The regulation's requirement for transparency regarding fees<sup>51</sup>, could be seen as a step towards broader user awareness about data collection and usage practices. This could potentially encourage similar transparency initiatives in the health data sector. So overall, Regulation 2024/886 is a positive development for financial transactions within the EU, but it doesn't have a direct impact on health data protection.

The transparency requirement in Regulation 2024/886 could inspire similar initiatives in other sectors, particularly health data. Why this is an interesting possibility? When we talk about Data Sensitivity, we can say that Health data is often considered highly sensitive, and there are growing concerns about how it's collected, used, and shared. Increased user awareness about data practices in the financial sector could translate to similar demands for transparency in healthcare. Public Interest also, Transparency in data collection can empower individuals and foster trust with institutions. In healthcare, understanding how health data is used can be crucial for patients to make informed decisions about their care<sup>52</sup>.

## Conclusion :

European legislation on (AI) and health data privacy represents a significant step towards responsible use of AI in healthcare. It prioritizes individual privacy while AI fosters innovation in healthcare, its continuous evolution necessitates ongoing discussions and adjustments to the legal framework will be crucial to ensure a healthy balance between technological advancements and data Safeguarding for European individuals.

The AIA places a strong emphasis on safeguarding health data through the implementation of strict regulations around its collection, use, and storage. This fosters trust in (AI) applications within healthcare and empowers individuals with greater control over their sensitive information. However, ongoing vigilance from regulatory bodies and healthcare providers is crucial for effective implementation of these safeguards.

We can conclude that the AIA prohibits certain high-risk AI applications altogether. This includes systems that use sensitive health data for Biometric categorization, where assigning individuals to categories based on their health information (e.g, genetic predisposition to disease). And Social scoring, by Creating a score that could influence access to healthcare or insurance based on health data. This two-pronged approach – strong data protection rights and targeted regulation of (AI) – aims to strike a balance between innovation and privacy. It allows the development of beneficial AI tools while protecting the privacy of Europeans' health information. However, challenges remain. Implementing these regulations requires ongoing vigilance from data protection authorities and healthcare providers. Additionally, the AIA allows for exemptions for law enforcement, raising concerns about potential privacy intrusions.

Overall, the EU (AIA) represents a significant step towards ensuring the ethical and responsible development governing the development and use of AI. This act establishes itself as a potential benchmark for international AI regulation, potentially influencing future approaches around the world for a future where AI benefits society without compromising individual privacy.

So the European legislation represents a significant step towards ensuring responsible use of (AI) in healthcare. It prioritizes individual privacy while paving the way for advancements that can improve public health outcomes.

Based on the cases we've discussed about European legislation on (AI) and health data privacy, some key results we can draw:

- Prioritizing Data Protection is The Cornerstone
- Implementation Challenges has a relation with Striking a balance between fostering innovation and protecting privacy requires, ongoing effort.
- Effective enforcement depends on consistent monitoring and ensuring compliance.

Based on the results above, some key recommendations can be drawing:

- Strengthen Data Protection Practices by Establish clear policies and procedures for handling health data used in (AI) applications.
- Enhance Regulatory Oversight, because Resource constraints can hinder data protection authorities' ability to adequately oversee compliance with (AI) regulations.
- Promote Public Awareness and Engagement, by Raising public awareness about the potential benefits and risks of (AI) in healthcare and empower individuals to protect their data privacy.
- Foster International Cooperation, especially Collaborate with international bodies to establish harmonized standards for (AI) regulation and data privacy in healthcare.

---

1 - Article 4(1) , Regulation (EU) 2016/679 of the European Parliament of 27 April 2016 on the General Data Protection Regulation GDPR, [2016] OJ L 119/1.

2 - Article 15, GDPR regulation.

3 - Article 16 GDPR regulation.

4 - Article 17 GDPR regulation.

5- (2020/c 124 i/01), information from European union institutions, bodies, offices and agencies, European commission communication from the commission guidance on apps supporting the fight against covid 19 pandemic in relation to data protection, 17 /4/ 2020, p 04.

6 - Article 6, 25 of regulation (eu) 2018/1725 of the European parliament and of the council of 23 October 2018 , on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

7- Communication from the commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, European commission, Recommendation C(2020) 2296 final of 8 April, Brussels, 2020, p 06.

8- This Directive on Privacy is not legally binding, and is without prejudice to the role of the Court of Justice of the European Union, the only institution capable of giving a reliable interpretation of EU law. See, Dragoș Mihail MĂNESCU, Personal Data between Individual Protection and the General Interest, The 4th International Conference on Economics and Social Sciences Resilience and economic intelligence through digitalization and big data analytics June 10-11, 2021, Bucharest University of Economic Studies, Romania, in

Proceedings of the 4th International Conference on Economics and Social Sciences ISSN 2704-6524, 2021, p 467.

9- solutions numériques pour lutter contre la covid-19, rapport sur la protection des données 2020 Octobre 2020 , Conseil de l'Europe, , pp 18, 19.

10- Communication from the commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, op cit, p 06.

11- This function is useful for both individuals and public health authorities, as it can play an important role in the management of containment measures, and a strategy can be developed that further supports the testing process for people with mild symptoms .Both functions may also constitute an important source of data for public health authorities, as they facilitate the transfer of such data to national epidemiological authorities and to the European Center for Disease Prevention and Control. This would help to understand patterns of transmission. If combined with test results ,estimating the positive predictive value of respiratory symptoms in a given community would provide information on the level of circulation of viruses. See, E-Health Network, Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States, Version 1.0, 15.04.2020, a platform of Member States' competent authorities dealing with digital Health, Adopted by consensus by the eHealth Network, Brussels, Belgium, 15 April 2020 , p – p 13 – 14.

12- Modern cloud-driven computing technologies and the modern vision of "citizen-oriented data" can help meet these challenges, as cloud solutions today enhance the ability to analyze data and the power of abundance in providing health care providers with more flexible computing power at a lower cost than is possible compared to traditional information technology systems, and therefore mobile-ready access ensures that data is always available to those who need it in a private and secure manner. See, Health Data: Saving Lives and Protecting Patients' Rights, A contribution to the dialogue on how to improve health in Europe while preserving privacy, May 2017, p 03.

13 - Article 5 of GDPR regulation.

14- As for the functions of the symptom checker and telemedicine, it can be said that if the application includes one or two of these functions, it will process personal health data, so a list of data that can be processed should be specified in the basic legislation applicable to health authorities. In addition, health authorities may need the phone numbers of people who used the symptom checker or checker and raised the results, as the information stored in the peripheral equipment can only be processed and accessed as much as necessary to enable the application to achieve its purpose and allow it to work. See, Communication from the commission, Guidance on Apps supporting the fight against COVID 19, op cit, pp 02, 03. P 08.

15- Health care providers should take a "patient-centered" approach by putting the totality of patient needs first, and in doing so should recognize that different safeguarding rules may be appropriate for "primary" uses of patient data (such as improving care and outcomes delivered by the individual patient) and a range of "secondary" uses (for example, by using large ( sometimes undeclared ) patient data sets to advance research, drive innovation ,and improve human health and the systems that treat us as well. See, Dragoș Mihail Mănescu, op cit, pp 467, 468.

16- Restrictions on the processing of health information can hinder the secondary use of health data regardless of the infrastructure used to process that data, which is hosted by the government itself, provided by the government, or based on electronic withdrawals. However, here, as in the case of primary use, the cloud enables the exchange of data within the need to find a practical patient-centered approach. There is no doubt that all entities that deal with patient data must store and process such data in ways that enhance trust and promote patient interests, especially with regard to

the implementation of the new data protection system in Europe, which is the general data protection regulation that looms. See, Health Data: Saving Lives and Protecting Patients' Rights, op cit, p 03.

17- Although many cases aimed at optimizing the effectiveness of data processing are more appropriately characterized by secondary uses, as is the case for improving patient engagement and health innovation in the Nordic countries, cloud-based systems are able to enable healthcare professionals to interact with patients more easily in remote or underserved areas, which can lead to better treatment outcomes by enabling faster and more frequent assessment, counseling and follow-up of patients. See, Health Data: Saving Lives and Protecting Patients' Rights, op cit, p 03.

18- Communication from the commission, Guidance on Apps supporting the fight against COVID 19, op cit, pp 02, 03.

19- The impact on the privacy of individuals should serve as an incentive for organizations to refute the idea of the inevitable trade-off between privacy and data protection on the one hand, and effective measures to protect public health on the other, because data protection principles and technical tools that allow for the right balance in this field are available to privacy professionals. See, Privacy and Data Protection in the age of COVID-19, Deloitte, Belgium, March 2020, p 02.

20- solutions numériques pour lutter contre la covid-19, op cit, pp 18, 19.

21- Privacy and Data Protection in the age of COVID-19 op cit, p 02.

22- Communication from the commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, op cit, p 06.

23 - Tjerk Timan, Zoltan Mann, "Data protection in the era of artificial intelligence, Trends, existing solutions and recommendations for privacy-preserving technologies", Big data value association (BDVA), October 2019, pp 05, 06.

24- The symptom screening function can provide an indication of the proportion of individuals who report COVID-19-compatible symptoms for example by vomiting and randomly testing a number of individuals with such symptoms, if there is the capacity to do so; it is essential to make it clear that personal health data will be ready in order to (i) provide the individual with the possibility of self-assessment, based on a set of questions asked, if they have developed COVID-19 symptoms, or (ii) to seek medical advice if COVID-19 symptoms have developed. See Adi Alsyoud and others, Exposure Detection Applications Acceptance: The Case of COVID-19, International Journal of Environmental Research and Public Health (IJERPH) · Vol 19, N° 12, June 2022, p 16, 17.

25- Dragoş Mihail MĂNESCU, op cit, p 466.

26- Ibid, p 07.

27 - This regulation establishes a uniform legal framework across the European Union for developing, selling, and using artificial intelligence (AI) systems. It aims to improve the internal market for AI, promote responsible AI that prioritizes human rights and safety, as well as the protection of health and foster innovation. The regulation also ensures a high level of protection against potential harms caused by AI systems, including threats to democracy, environmental protection, and other fundamental rights. See, Article 1/1 of EU Artificial Intelligence Act, P9\_TA(2024) 0138, European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

28 - P9\_TA(2024)0138, Artificial Intelligence Act, adopted by the European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) (Ordinary legislative procedure: first reading)

29 - Shaping Europe's digital future, European Commission, 21 February 2024, available on :

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_941](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_941)

30 - Artificial intelligence (AI), a term introduced by John McCarthy in 1955, was originally envisioned as the science of creating intelligent machines. Early efforts focused on programming machines to perform complex tasks, like chess. Today, however, the emphasis has shifted towards machines that can learn and adapt, mimicking human learning to some degree. See, Christopher Manning, Artificial Intelligence Definitions, Stanford University Human-Centred Artificial Intelligence, September 2020. <https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf>

31 - Article 6 (AIA).

32- EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

33 - EU AI Act: Risk-Classifications of the AI Regulation, Last updated after the provisional agreement of the EU co-legislators on 08.12.202, <https://www.trail-ml.com/blog/eu-ai-act-how-risk-is-classified>

34 - Person-centered care aims to address all patient problems, including non-medical ones, which can lead to medicalizing non-medical issues. This creates an ethical tension between considering the whole person and avoiding medicalization. Sven Ove Hansson and Barbro Froding, Ethical conflicts in patient-centred care, Clinical Ethics, 1–12, 2020, P 03.

35 - Risk-Based Approach: High-Risk Systems, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

36 - Article 6 AIA.

37 - Article 13 AIA.

38 - Article 5 AIA.

39 - Article 12 AIA.

40 - Article 5(1)(d) AIA .

41 - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Official Journal of the European Union, L 119/, 4.5.2016, p 43.

42 - Article 10 AIA.

43 - EDPB guidelines are documents that provide interpretations and clarifications on specific aspects of the GDPR. They are not legally binding, but they carry significant weight and influence how DPAs (Data Protection Authorities) in each member state understand and apply the regulation.

44 - Examples of these efforts include EDPB guidelines that clarify the interpretation of the GDPR on various topics. These guidelines help to ensure consistency across member states. Additionally, DPAs from different countries can conduct joint investigations for complex cross-border cases, fostering information sharing and coordinated enforcement actions. The "One-Stop Shop" mechanism further streamlines enforcement by designating a lead DPA for investigations involving companies operating in multiple EU countries. This avoids conflicting decisions from different authorities.

45 - Simona Strmečki, M.Sc., Silvija Pejaković-Đipić, data protection, privacy and security in the context of artificial intelligence and conventional methods for law enforcement, Conference: International Scientific Conference “Digitalization and Green Transformation of the EU“, eu and comparative law issues and challenges series (ECLIC) – issue 7, August 2023, p 585.

46 - The item n 18 of AIA issued on 2024, stipulated that The notion of ‘emotion recognition system’ referred to in this Regulation should be defined as an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. See also, Xiaowei Wang, Bodily harms: mapping the risks of emerging biometric tech, Access Now publications, Published in October 2023, p 10.

47 - Melissa Koide CEO, FinRegLab , AI for good: Research insights from financial services , center on regulation and markets at brookings , august 2022, P 01. A report available on :

<https://www.brookings.edu/wp-content/uploads/2022/08/AI-for-good-Research-insights-from-financial-services-3.pdf>

48 - Section 2B of General Data Protection Regulation (GDPR)..

49 - Regulation (eu) 2024/886 of the european parliament and of the council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro

50 - Marvin van Bakkum, Frederik Zuiderveen Borgesiu, Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?, computer law & security review Vol 48, Published by Elsevier Ltd, 2023, p 10.

51 - Article 8 of General Data Protection Regulation (GDPR).

52 - Amedeo Santosuosso, Giulia Pinotti, Data-Driven Decision Making. Law, Ethics, Robotics, Health, Law, Sciences and New Technologies, Open Access Series of the Interdepartmental Research Centre European Centre for Law, Science and New Technologies (ECLT) Pavia University Press, University of Pavia, Italy, 2020, p – p 88 – 91.