***Data privacy and protection for personal data***

* **Names and IDs:**
* Mohamad IBRAHIM (191545)
* Ali MOHTI (210044)
* Ali DIA ()
* **Course:** Ethics for AI
* **Cursus:** Master AI M2
* **University:** USJ - ESIB
* **Date:** 7/12/2024

Contents

[I. OBJECTIVE 3](#_Toc187610025)

[II. E TRANSACTION LAW 81.2018 LEBANON 3](#_Toc187610026)

[III. EU GUIDELINES ON ETHICS IN AI 4](#_Toc187610027)

[IV. AI RIGHT TO PRIVACY 4](#_Toc187610028)

[References 5](#_Toc187610029)

# OBJECTIVE

The topic of data privacy and the protection of personal data under Lebanese law involves examining the key provisions that must be applied and identifying the legal and practical challenges that may impede their effective implementation. Drawing an analogy with the General Data Protection Regulation (GDPR) provides valuable insights into how these issues are addressed in a broader, more established framework.

# E TRANSACTION LAW 81.2018 LEBANON

The Lebanese Electronic Transactions and Personal Data Law defines personal data as any information enabling direct or indirect identification of a natural person (Article 1). Processing of such data involves actions such as collection, recording, organization, storage, adaptation, extraction, and deletion (Article 1). The law mandates that personal data be collected faithfully for legitimate, specific, and explicit purposes, ensuring it does not exceed the stated objectives and is retained only for the period specified in the processing declaration (Articles 87, 90). Sensitive data revealing health status, genetic identity, or sexual life is prohibited from being processed unless under specific conditions, such as for medical purposes or with explicit consent (Article 91). Data subjects have the right to inquire about their personal data, request corrections, updates, or deletion, and object to processing for legitimate reasons (Articles 99, 101, 92). They must also be informed by data processors of the identity of the processing officer, the purpose of processing, and their rights, including access and correction methods (Articles 88, 89). Data processors are required to ensure the integrity and security of data, protecting it against unauthorized access, distortion, or damage (Article 93). Certain data processing activities, such as those by educational institutions or non-profit organizations, may be exempt from licensing if deemed low risk (Article 94). Unauthorized processing, failure to comply with legal obligations, or negligent disclosure of data to unauthorized persons incurs severe penalties, including fines and imprisonment (Articles 106, 107). Additionally, judges play a role in assessing disputes involving electronic evidence and determining the proof power of electronic documents and signatures (Articles 12, 122) [1].

# EU GUIDELINES ON ETHICS IN AI

The European Union (EU) has adopted a "human-centric" approach to artificial intelligence (AI), emphasizing respect for European values, human dignity, and fundamental rights, distinguishing itself from the private-sector-led strategies of the U.S. and the government-driven models of China (*EU Human-Centric Approach to Artificial Intelligence*). The EU guidelines for trustworthy AI outline seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity and fairness, societal and environmental well-being, and accountability (*Key Ethical Requirements for Trustworthy AI*). These guidelines highlight the need for mechanisms like "stop buttons" to ensure human oversight (*Human Agency and Oversight*), secure and reliable AI systems to mitigate cybersecurity risks (*Technical Robustness and Safety*), compliance with GDPR to protect privacy through methods like encryption (*Privacy and Data Protection*), and transparent processes to enhance explainability and traceability in AI decision-making (*Transparency*). However, implementation faces challenges such as vague language, lack of regulatory oversight, and potential fragmentation from differing national frameworks, requiring coordinated EU-wide actions (*Implementation Challenges*). To address these, international standardization efforts, such as those by ISO and IEEE, focus on developing ethical and technical AI standards (*Standardization in AI*), while the EU considers mandatory transparency and accountability measures, including regulatory bodies for algorithmic decision-making (*Legislation on Transparency and Decision-Making*). Globally, the U.S. and China differ in their approaches, with the former emphasizing industry self-regulation and the latter integrating ethics into centralized AI strategies (*International Context*). Despite these challenges, the EU remains a front-runner in promoting ethical AI development [2].

# AI RIGHT TO PRIVACY

The development of robust data governance policies addressing data quality, integrity, access protocols, and privacy-preserving techniques is crucial to ensuring AI compliance with regulations like GDPR. Striking a balance between data protection and innovation is essential, particularly with emerging technologies like blockchain and IoT. AI systems pose significant risks to privacy, liberty, and justice, such as unauthorized data access and algorithmic bias, necessitating protections under frameworks like ECHR and ESC. Responsible AI principles, including transparency, fairness, accountability, and inclusivity, aim to mitigate harm and build trust in AI systems. However, transparency remains challenging due to the complexity and evolving nature of AI, requiring meaningful explanations and adherence to GDPR Articles 12-14. GDPR mandates principles like data minimization, accuracy, security, and purpose limitation for AI systems while allowing flexibility for future processing under accountability frameworks. The EU AI Act complements GDPR by providing a comprehensive framework for ethical AI development, emphasizing risk management, data governance, and human oversight for high-risk systems. It prohibits practices such as subliminal techniques, exploiting vulnerabilities, and real-time biometric identification for law enforcement. To support responsible procurement, the EU introduced model contractual clauses for public AI systems, distinguishing between high-risk and non-high-risk systems to ensure compliance and ethical development [3].

# References

|  |  |
| --- | --- |
| [1] | E Transaction Law 81, Lebanon, 2018. |
| [2] | EU Guidlines on ethics in AI, EU, 2019. |
| [3] | European Data Protection Law. |