***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](#_Toc187611426)

[II. E TRANSACTION LAW 81.2018 LEBANON 3](#_Toc187611427)

[III. EU GUIDELINES ON ETHICS IN AI 4](#_Toc187611428)

[IV. AI RIGHT TO PRIVACY 4](#_Toc187611429)

[V. GDPR 5](#_Toc187611430)

[VI. IMPACT OF GDPR ON AI 5](#_Toc187611431)

[References 6](#_Toc187611432)

# 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].

# GDPR

The GDPR establishes key principles and obligations to protect personal data. It mandates the lawful, fair, and transparent processing of data (Article 5(1)(a)), limits its use to specific, legitimate purposes (Article 5(1)(b)), and requires data minimization to what is necessary (Article 5(1)(c)). Data must be accurate and updated (Article 5(1)(d)), stored only as long as needed (Article 5(1)(e)), and controllers must demonstrate compliance (Article 5(2)). It grants data subjects rights, including access to their data (Article 15), rectification of inaccuracies (Article 16), erasure under specific conditions ("right to be forgotten") (Article 17), portability of their data to another controller (Article 20), and the right to object to processing for legitimate interests or marketing (Article 21). Controllers and processors must conduct Data Protection Impact Assessments for high-risk activities (Article 35), maintain records of processing activities (Article 30), report breaches within 72 hours (Article 33), and ensure data protection by design and default (Article 25). GDPR applies globally to entities offering goods or services to EU data subjects or monitoring their behavior, regardless of their location (Article 3). These provisions provide a robust framework for data protection, setting a benchmark for compliance worldwide [4].

# IMPACT OF GDPR ON AI

AI systems significantly influence society, transforming the economy, politics, and citizen interactions, while raising legal and ethical concerns across domains like data protection, civil liability, and discrimination (Introduction). AI's reliance on big data introduces risks such as surveillance and manipulation but offers societal benefits, including improved healthcare and governance. Profiling by AI commodifies personal data, enabling pervasive influence and decision-making (AI and Personal Data). The GDPR does not explicitly reference AI but addresses it through principles like purpose limitation, data minimization, and the regulation of profiling, which uses data to analyze or predict personal aspects heavily impacted by AI (AI in the GDPR). These principles are challenged by AI's ability to repurpose data, requiring compatibility safeguards, and its data-intensive processes, which necessitate proportionality and pseudonymization to mitigate risks. Transparency is critical, requiring data subjects to be informed about automated decision-making and its logic (AI and Data Protection Principles). Data subjects have rights under GDPR, such as access (Article 15), enabling requests for information on AI logic and impacts, and erasure (Article 17), which includes inferred data. They can also object to profiling and processing, particularly for direct marketing and statistical purposes (Article 21) (AI and Data Subject Rights). Article 22 prohibits automated decisions significantly affecting individuals unless exceptions like consent or necessity are met, with safeguards including human intervention, risk assessments, and correcting inaccuracies (Automated Decision-Making). To address legal uncertainties and uphold data protection principles, detailed guidance on AI applications, societal debate, and institutional engagement are essential, ensuring ethical AI innovation (Policy Proposals) [5].

# References

|  |  |
| --- | --- |
| [1] | E Transaction Law 81, Lebanon, 2018. |
| [2] | EU Guidlines on ethics in AI, EU, 2019. |
| [3] | European Data Protection Law. |
| [4] | GDPR. |
| [5] | Impact of GDPR on AI. |