

Digital Governance and Fundamental Rights: A Critical Analysis of Jordan's Data Protection Law

PhD. candidate **Rand Tuffaha AL-HUSSAINI**¹

Abstract

This article analyzes Jordan's Personal Data Protection Law (PDPL) of 2023 and its enforcement via the compulsory Sanad digital identity system. The PDPL marks Jordan's initial effort to oversee personal data handling in a more digital society, arising from a backdrop of political opposition, public anxieties, and substantial uncertainty regarding the implications of regulation for government authority. This study uncovers considerable disparities between the protections outlined in the law and their actual implementation, based on legal analysis. The study examines the structural autonomy of the Personal Data Protection Council, which, due to its composition under ministerial control, raises issues regarding potential conflicts of interest and political meddling. The analysis reveals that mandatory biometric registration via Sanad establishes a techno-feudal system in which citizens are required to relinquish data rights to obtain vital government services. Although the PDPL includes clear consent clauses, extensive exemptions for public authorities and the coercive effects of digital exclusion weaken the law's ability to safeguard fundamental rights, especially for digitally illiterate groups in rural and tribal areas.

Keywords: data protection, digital governance, techno-feudalism, Jordan, biometric surveillance, Sanad platform.

JEL Classification: K24, K38, K40

DOI: 10.62768/PLPA/2026/15/1/02

Please cite this article as: Al-Hussaini, Rand Tuffaha, „Digital Governance and Fundamental Rights: A Critical Analysis of Jordan’s Data Protection Law”, <i>Perspectives of Law and Public Administration</i> 15, no. 1 (March 2026): 26-49.	Article History Received: 15 November 2025 Revised: 19 January 2026 Accepted: 09 February 2026
---	--

1. Introduction

The 2023 Jordanian Personal Data Protection Law (herein after as PDPL), is Jordan’s first real attempt at regulating how personal data is processed. Although it can be said the story behind it was not smooth given the nature of the community, as it started with political resistance, public fears, and a lot of uncertainty about what this law could mean, it can be said that this step is challenging. While Jordan has been pushing hard to digitalize everyday life from e-government services to e-commerce the laws meant to protect people in that digital space did not keep up. This gap is not lost on everyone: some officials recognize the urgency and speak up, others stay

¹ Rand Tuffaha Al-Hussaini - Faculty of Law and Political Sciences, University of Szeged, Hungary, rand.hussaini@gmail.com, ORCID: 0009-0003-3745-2182.

silent, and many still don't see it as a problem at all. Some even see regulation itself as dangerous tool that could lead to even more government control. There are many elements in that can be considered to measure how well any regulation or law is being implemented in Jordan, as many challenges arise, including digital illiteracy, other aspects of raising awareness are neglected.

Despite its regional focus, Jordan's pursuit for digitalization is inextricably connected to a global transformation in the digital economy. This change is characterized by a new, extractive logic of capital accumulation, which some scholars refer to as "techno-feudalism".² This new paradigm marks an important transition from traditional capitalism. It can be distinguished by the dominance of digital platforms, which procure a new type of value from what he refers to as "cloud capital" rather than markets and profits.³ According to this concept, users of large digital platforms are no longer just clients; rather, they become "cloud serfs," generating massive amounts of data through their online activities, which platform owners then utilize to produce more value and increase their position of dominance.

The introduction of this new economic philosophy led to an interesting debate. A researcher analysis of the subtle differences between "techno-feudalism" and "platform capitalism," observes that, while the names may differ both concepts allude to a system in which a small number of dominating corporations accumulate money through rent-seeking and data extraction.⁴ Erik Swyngedouw defines the "rent-information-services nexus" as the new key axis for capital accumulation, arguing that the traditional exploitation of labor in commodity production has given way to the capture of knowledge and data as a form of rent.⁵

According to another researcher, the current state of capitalism is more aggressive and technologically advanced than a new kind of feudalism. According to this opinion considering huge tech corporations' ability to operate outside of nation-states' effective regulatory reach gives them the power to establish new forms of extraction and enclosure that are nevertheless founded on capitalist processes.⁶

Understanding this global theoretical context is crucial for analyzing Jordan's approach with the aforementioned law. The PDPL can be seen as a state-level response to the challenges posed by this new digital economy. It represents an attempt by the Jordanian government to assert a degree of digital sovereignty and allegedly to regulate the flow of data, and perhaps to provide its citizens with a measure of protection against the extractive logic of platform capitalism.

² Giannēs Baruphakēs and Michaēl S. Zumpulakēs, "On Technofeudalism: What Killed Capitalism? An Interview with Yanis Varoufakis," *Economic Thought* 11, no. 2 (2023): 25-30.

³ Yanis Varoufakis, *Technofeudalism: What Killed Capitalism* (London: The Bodley Head, 2023), p. 70 et seq.

⁴ Jeremy Gilbert, "Techno-Feudalism or Platform Capitalism? Conceptualising the Digital Society," *European Journal of Social Theory* 27, no. 4 (2024): 561-578.

⁵ Erik Swyngedouw, "Capitalism Is Over, but the New Is Worse: Reflections on Rent, Services, and Capitalist Feudalism," in Frank Moulaert and Abid Mehmood (eds.), *The Value of Place*, (Cheltenham: Edward Elgar Publishing, 2025), 23-39, <https://doi.org/10.4337/9781035347926.00009>.

⁶ Nicholas Gane, "Capitalism Is Capitalism, Not Technofeudalism," *Journal of Classical Sociology*, vol. 25, issue 4, (2024), <https://doi.org/10.1177/1468795X241269293>.

In this article, the scope of the law is detailed, who is protected, what kinds of data are processed, and which bodies are responsible for enforcing it. In addition to examining two annexed instructions to the PDPL and how they contribute to this legal painting. What legal remedies are available if someone's rights are violated can be in question. Understanding this is important, especially as Jordan rolls out digital systems like Sanad⁷, which relies on biometric data. My goal is to see how this law is actually capable of protecting people in a digital world and how it leaves room for exclusion, misuse, and unlawful surveillance.

2. Birth of the Legal Frame

The PDLP applies to the processing of personal including sensitive data carried out by both public and private entities operating within or outside the Kingdom, as long as the data concerns natural persons located in Jordan.⁸ "Personal data" is defined broadly to include any information that directly or indirectly identifies a person, while sensitive data covers more specific categories such as biometric, health, genetic, financial, religious, and political information.⁹ Do these definitions differ from GDPR? The law also applies retroactively to data processed before its entry into force.¹⁰ The material scope of the law includes the full range of data processing, such as collection, storage, transmission, modification, and deletion.¹¹ However, the law excludes personal data processed by natural persons for purely personal purposes and introduces broad exceptions for processing without consent in cases involving public authorities, public interest, or legal obligation.¹² Knowing these provisions suggest a wide material scope, their open-ended nature, particularly around exceptions, clearly creates uncertainty regarding the law's actual reach, especially in high-risk areas such as biometric data processing.

⁷ Sanad is Jordan's unified digital identity platform and gateway to government services, allowing citizens to access over 550 government services through a single digital identity using biometric authentication. The platform was launched as part of Jordan's digital transformation strategy and is integrated with biometrics for security. As of November 2025, approximately 1.8 million digital identities have been activated through the Sanad application, with the government targeting 3.5 million activated digital IDs by the end of 2025.

⁸ Jordanian Personal Data Protection Law No 24 of 2023 s 3(a.) This Law passed This law was passed on September 17, 2023, when it was published in the Official Gazette, and entered into force six months later on March 17, 2024. Organizations that process personal data were granted a one-year grace period for full compliance, which concluded on March 17, 2025.

⁹ Ibid s 2. Definitions (Personal Data, Sensitive Personal Data). تعريف البيانات الشخصية وتعريف البيانات الشخصية الحساسة. *Personal Data*: Any data or information related to a natural person that directly or indirectly identifies them, regardless of its source or form. This includes data concerning the individual, their family status, or their location. *Sensitive Personal Data*: Any data or information related to a natural person that directly or indirectly indicates their origin, race, political opinions, religious beliefs, financial status, health, physical or mental condition, genetic data, *biometric data*, criminal record, or any information deemed sensitive by the Council if its disclosure or misuse could harm the individual concerned.

¹⁰ Ibid s 3(a).

¹¹ Ibid s 2 (definition of 'processing').

¹² Ibid ss 3(b), 6.

The adoption of PDPL in 2023 generated considerable debate and different opinions among policymakers, practitioners and observers regarding its adequacy and transparency in protecting fundamental rights.

3. The Establishment of Supervision Bodies

3.1. On Motivations

When it comes to The Personal Data Protection Council, which had been established under Chapter 3 (Article 17) of the PDPL holds the main task of overseeing the implementation of data protection provisions. However, its composition under ministerial leadership raises significant concerns regarding its independence and compliance with international standards. On a positive note, the establishment of the council signs a significant development in Jordan's approach to data governance.¹³ In theory, the creation of a designated body to supervise the application of data protection rules is a positive step toward formalizing oversight mechanisms in the digital environment. A clear institutional framework can potentially enhance legal certainty, coordinate enforcement efforts, and contribute to building public trust in digital systems such as biometric registration platforms and the Sanad digital identity system which will be discussed later.

Looking at the other face of the coin, the Council's structural design raises serious concerns regarding its independence and effectiveness. The Council is chaired by the Minister of Digital Economy and Entrepreneurship and includes representatives from various governmental bodies and private sector stakeholders, the Council consists of 12 members in total: the Minister of Digital Economy and Entrepreneurship as Chair, plus 11 members including the Information Commissioner (Vice-Chair), the General Commissioner for Human Rights, the President of the National Cyber Security Center, a representative from the Central Bank of Jordan, two representatives from security agencies, and four specialized individuals appointed by the Council of Ministers representing the telecommunication, banking, and information technology sectors. This composition means that at least 8 out of 12 members (67%) are government or security agency representatives, with only 4 members (33%) from the private sector.¹⁴

This composition fundamentally undermines the Council's autonomy, creating great risks of conflict of interest, political interference and a lack of impartiality in enforcement actions due to the predominance of members from the governmental side. In contrast, looking at international standards, the European Union's General Data Protection Regulation (GDPR), to be exact, require that supervisory authorities be entirely independent from external influence, both in law

¹³ Jordanian Personal Data Protection Law No 24 of 2023 s 16. "A Council referred to as the "Personal Data Protection Council" shall be formed, chaired by the Minister and is..."

¹⁴ Mohammad Al An'imat, "Technical Protection for Electronic Banking Operations in Jordan," *Curentul Juridic*, no. 1(92) (2023): 94-109.

and in practice.¹⁵ Under Article 52 GDPR, supervisory authorities must act with complete independence, free from governmental or private sector pressure in the performance of their tasks. The Jordanian model clearly fails to meet this standard as the inclusion of executive branch officials in decision-making processes compromises the Council's ability to serve as a neutral arbiter of rights violations.

Since the legal perspective is now clear, it's important to discuss the human rights perspective, as the lack of independence raises profound concerns about the Council's capacity to protect data subjects effectively. An authority embedded within ministerial structures may prioritize governmental interests such as national security or administrative efficiency over individual rights to privacy, non-discrimination and legal remedy, which is logical in a sense considering Jordan's system is semi-authoritarian as mentioned in the BTI Transformation Index of 2024 report, "*Jordan is a semi-authoritarian state in which all domestic actors are dependent to varying degrees on the state and its agents. The operating environment and political rules are determined and interpreted according to the needs of the Hashemite regime and must be followed by reformers and anti-reformers alike*".¹⁶ So, the Council's dual role in both promoting and regulating digital initiatives creates an inherent tension that may compromise its objectivity.

The Council's internal operating procedures, as published in the *Official Gazette*, confirm this structural issue: the President of the Council is the Minister of Digital Economy and Entrepreneurship, and members include appointed representatives from executive agencies and public institutions.¹⁷ These provisions not only undermine the Council's autonomy, but also violate international expectations of independent supervisory authorities tasked with overseeing data protection compliance, the analysis will be detailed later in this section.

3.2. Legal Analysis of the Council's Operating Instructions

The operating instructions of the Personal Data Protection Council, published in the *Official Gazette*, is one of 12 documents published later after the main articles of the law were approved, some were even published 1 or 2 years later in 2024 and 2025.¹⁸ In the Jordanian legal system, instructions (تعليمات/Ta'īmāt) occupy the fourth

¹⁵ 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 (General Data Protection Regulation), Official Journal of the European Union L 119/1, art. 52.

¹⁶ Bertelsmann Stiftung, *BTI 2024 Country Report – Jordan* (Bertelsmann Stiftung 2024) <https://bti-project.org/en/reports/country-report/JOR>, accessed 10 November 2025.

¹⁷ Ministry of Digital Economy and Entrepreneurship, Instructions for the Personal Data Protection Council Working Mechanism for 2025, issued pursuant to Paragraph (C) of Article (16) of the Personal Data Protection Law No. 24 of 2023, https://www.modcc.gov.jo/ebv4.0/root_storage/en/eb_list_page/instructions_for_the_pdp_council_work_in_2025-0.pdf, accessed 10 November 2025.

¹⁸ Ibid., Access to all documents on the ministry's official website. Available official English translation for some of the documents can be found here: https://modcc.gov.jo/EN/List/The_law_regulations_and_instructions, accessed 10 November 2025.

tier of the legal hierarchy, below the Constitution, laws, and regulations. Instructions are binding administrative directives issued by ministers or government agencies to implement laws and regulations within their jurisdictions. They are legally binding on entities under the issuing authority's supervision, but they are subordinate to higher legal instruments and cannot contradict the PDPL or any other law. Instructions are subject to judicial review by administrative courts, which can annul them if they exceed the authority granted by the parent law or violate constitutional principles. Regulations (أنظمة/Anẓimah) are issued by the Council of Ministers and have broader binding force than instructions, while guidance documents and standards are non-binding interpretive tools. Under the PDPL, the Council is empowered to issue instructions and standards to regulate data processing activities, but the primary authority to process personal data rests with controllers (data processors) who must comply with the law's requirements, including obtaining consent or establishing another legal basis for processing.¹⁹

The legal sources on executive provisions of the PDPL are as follows:

- a) Instructions for the Functioning of the Personal Data Protection Council for the Year 2025;
- b) Instructions on the Register of Data Protection Officers, Processors, and Controllers;
- c) Instructions on the Personal Data Protection Register;
- d) Regulation on the Mechanisms and Procedures of the Unit's Operations;
- e) Regulation on Licenses and Permits;
- f) Regulation on Data Disclosure;
- g) Standards for Accrediting Personal Data Protection Officers;
- h) Accreditation Form for Personal Data Protection Officers;
- i) List of Critical Infrastructure Sectors Requiring Accreditation of the Officer by the Personal Data Protection Council;
- j) Guidance Manual for Drafting a Privacy Policy;
- k) Instructions on Technical, Organizational, and Security Measures for the Year 2025;²⁰
- l) Regulation on Data Subject Rights and the Procedures for Prior Consent and Its Withdrawal.

The focus first on (a) and (b) as they are the most detailed, as for the Instructions for the Functioning of the Personal Data Protection Council document which surprisingly came very late, considering the law came into force in 2023. These

¹⁹ Arabic terms are transliterated according to the United Nations Romanization System. See United Nations Group of Experts on Geographical Names, 'Romanization System from Arabic Letters to Latinized Letters 2007' (Eleventh United Nations Conference on the Standardization of Geographical Names, New York, 8-17 August 2017) UN Doc E/CONF.105/137/CRP.137

²⁰ There are currently two versions published on the same official website holding the same title yet have similar content to an extent yet different wording and added English terms, surprisingly the one published in 2024 is more detailed than the one published in 2025, which causes confusion in which is actually in force and which is the older version, or whether both are considered legally binding. The one published in 2025 can be accessed here <https://modec.gov.jo/AR/List> and the one published in 2024 can be accessed here http://www.nitc.gov.jo/EBV4.0/Root_Storage/AR/tawfiq/, accessed 10 November 2025.

documents outline the internal structure and procedures governing the body tasked with supervising the implementation of the 2023 PDPL. While the issuance of such instructions indicates a trial to institutionalize oversight, a closer look reveals several legal and structural weaknesses that undermine the Council's effectiveness as it will be clarified later. These weaknesses are particularly obvious when assessed against European standards, such as those articulated in the General Data Protection Regulation (GDPR), and when viewed through a human rights lens. To put the regulation sections into details as follows:

Section 2: Regarding Chairmanship and Membership Composition:

Section 2 of the Council's operating instructions does not actually explain the composition of the Council or who its members are. It only defines a few key term such as "Council," "President," and "Law" and refers back to the main legislation.²¹ The real structure of the Council is set out in Article 16 of the PDPL, where it is made clear that the Minister of Digital Economy and Entrepreneurship chairs the Council. The rest of the members are appointed from specific government-controlled bodies, including the Cyber Security Center, the Central Bank, security agencies, and a few sector representatives. The General Commissioner for Human Rights is also listed as a member, that on the surface suggests some human rights-based input, but even with that, there is no guarantee of independence, because there is no requirement for member qualifications, no restriction preventing conflicting instructions from other government agencies, no inclusion of civil society and no assurance that rights-focused voices have any institutional power (e.g. right to veto Council decisions) within the Council. In my view, this is especially problematic because the same ministry that develops and promotes digital platforms like Sanad is also tasked with regulating them. From a governance perspective, this creates a serious conflict of interest. Under the GDPR, supervisory authorities must be fully independent and free from external influence.²² That standard is not met here. Oversight is concentrated in the hands of the very institution it is supposed to oversee, which undermines both the legitimacy and effective protection of rights by the Council.

Section 3: Meetings and Decision-Making. According to Section 3 of the Council's operating instructions, the Council is required to meet at least once every two months, or whenever the President deems it necessary.²³ We can note here that there is no provision allowing members themselves to call for a meeting, which means the Council's most basic procedural function (i.e. its ability to convene) is entirely subject to the Minister's discretion. This is a notable concentration of procedural control and power in a regulatory body that is supposed to provide oversight. In contrast to models where a quorum of members can compel a meeting, Jordan's Council can only meet when invited by the very actor it is supposed to oversee, not to mention he chairs the Council and holds the tie-breaking vote, further concentrates authority. Unlike independent data protection authorities in the EU, which often have

²¹ See note 14 above.

²² Regulation (EU) 2016/679, art. 52.

²³ Ministry of Digital Economy and Entrepreneurship, Instructions for the Personal Data Protection Council Working Mechanism (note 19 above), art. 3.

staggered terms, clear appointment criteria, and independent voting procedures, Jordan's model grants excessive procedural control to one political representative. It opens the door to biased, one-sided operation and executive overreach.

Section 4-5: Appointing the Secretary and Conflict of Interest. Moving on to Section 4, the President of the Council appoints own Secretary (أمين سر/ Amīn Sīrr) to manage the Council's internal operations or if translated directly from Arabic, it would mean (The person who maintains the secrets) If the Secretary is absent, the President appoints a replacement from within the Ministry's Data Protection Unit.²⁴ On the surface it seems this Section deals with administrative tasks, but the fact that the President, who is the Minister of Digital Economy and Entrepreneurship as mentioned earlier, has full discretion over appointing and replacing the Secretary, even temporarily, reinforces the centralized and top-down nature of the Council's structure. The role of Secretary is closely tied to managing the Council's institutional records and ensuring procedural accountability, disclosure of personal data doesn't fall under the Secretary's roles. Giving the Minister unilateral control over this position, without Council approval or independent oversight, is inconsistent with international good practice, especially where sensitive issues such as law enforcement data are at stake. So far it would support to biased operation.

Meanwhile Section 5 outlines a formal process for managing conflicts of interest. It requires members to immediately disclose any direct or indirect personal interest that may compromise their independence. Upon disclosure, the member must abstain from discussion and voting on the issue. This takes us back again to the President as he can also request the member to leave the meeting room during the relevant discussion. The Secretary's role is to document the disclosure, adjust quorum and voting counts accordingly, and record the abstention in the minutes.²⁵ Although the article appears to be stronger than projected, it ultimately depends on voluntary compliance and internal confidence, which is a major flaw for a Council entrusted with overseeing powerful public institutions. This provision requires withdrawal from discussion not merely abstention, which can be said that it goes beyond classic conflict of interest prohibitions. Nevertheless, there is still no external enforcement or transparency in the process. There is no institutional unit/ethical body to monitor noncompliance *ex lege and in situ*, no requirement to make a public record of recusals, and no means to confirm undeclared conflicts.

Section 6-7: Delegation and Confidentiality. This Section clarifies that the President represents the Council before external bodies, and may delegate this task to another Council member by a written and specific delegation, and the President must be informed of any representation carried out on their behalf.²⁶ This arrangement allows the President complete authority over who represents the Council externally, including in high-profile legal or public engagements. While mandating delegation in

²⁴ Ibid., art 4.

²⁵ Ibid., art 5.

²⁶ 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, Official Journal of the European Union L 119/1, art. 59.

writing is a basic precaution, there is no requirement for group control or voting, nor is there any obligation to reflect such representations in public records. In effect, the Council's external voice is still managed by the same executive actor that it is supposed to supervise. Thus, the Council's credibility as an independent oversight body is missing, particularly when it comes to topics such as biometric surveillance or digital identity governance, which require public trust.

Confidentiality provision in Section 7 is standard, but looking at the bigger picture, the lack of transparency mechanisms is striking. Meanwhile Article 59 of the GDPR, while protecting sensitive data, requires supervisory authorities to report publicly and regularly on their activities.²⁷ In Jordan's case, the Council's discretion over what is revealed and when, which could possibly mirror opacity, reduce public trust, and limit civil society engagement.

The structural deficiencies identified in the Council's design are reflected in Jordan's broader performance on fundamental rights protection. According to the World Justice Project Rule of Law Index 2025, Jordan ranks 100th out of 143 countries globally on fundamental rights, with an overall score of 0.46 out of 1.0.²⁸ More specifically, on the sub-factor measuring freedom from arbitrary interference with privacy, Jordan scores only 0.33, placing it 94th globally and below the global average of 0.47.²⁹ This empirical assessment corroborates the concerns raised in this analysis: Jordan's institutional framework for protecting privacy and data protection rights is demonstrably weaker than international standards. The absence of an independent supervisory authority, combined with broad exceptions for state surveillance, directly contributes to this poor performance on privacy protection metrics.

3.3. Assessment of the Instructions

In summary, while the Personal Data Protection Council's operating instructions show a formal commitment to oversight and coordination, the structure and procedures outlined in Articles 2-7 reveal a body that is deeply integrated into the executive branch, lacking both institutional independence and functional impartiality. From a legal and civil standpoint, this design has the potential to undermine data subjects' trust, reduce accountability, and jeopardize Jordan's compliance with recognized data protection standards in Europe. Structural reform, particularly the establishment of an independent monitoring institution, is required to effective protection. Only eight articles to regulate the framework or a very important council, yet it doesn't clarify how this contributes to data protection, it seems like these articles had been copied from other Jordanian council establishing regulations, nothing can be considered new or detailed, and it portrays who is in power over portraying relevant

²⁷ Ibid.

²⁸ World Justice Project, "Rule of Law Index 2025: Jordan – Fundamental Rights" (Washington, DC: World Justice Project, 2025), <https://worldjusticeproject.org/rule-of-law-index/country/2025/Jordan/Fundamental%20Rights>, accessed November 6, 2025.

²⁹ Ibid.

responsibilities, accountability, and duties.

In other words, the Council's operating instructions resemble a hierarchical command structure more than a functional guidebook for data protection oversight. The text focuses heavily on defining roles, authority levels, and centralized decision-making, rather than outlining clear procedural mechanisms for investigating data protection violations and or enforcing compliance in providing remedies for supervision. From a legal design perspective this reflects an administrative logic rooted in centralized authority rather than participatory or governance based on rights. This structural arrangement has also serious implication from a human rights perspective by showcasing an oversight body embedded within the executive branch and chaired by the Minister as mentioned before. This raises the flags for lacking the institutional independence which are deemed necessary to safeguard fundamental rights such as the right to privacy,³⁰ the right to an effective remedy³¹ and equality before the law.³² Instead of functioning as a neutral protector of data subjects' rights, the Council's design risks reinforcing executive discretion and facilitating unchecked data surveillance, thus undermining the very rights it was purportedly created to protect. Finally, it can be said that the title being as the "Council's Operating Instructions" is not serving the content well, as it would be more legally professional to name it "The Organizational Structure of the Council".

The institutional design observed in both the Council and Registry instructions clearly portray a broader structural pattern in Jordanian lawmaking. Oversight bodies are frequently formed in the image of ministerial committees or councils across various sectors, landing authority in the hands of ministers, directors, or governors, rather than in independent entities. This formulaic design is not only shown in the PDPL; as the author's research finds it replicates institutional arrangements found in numerous Jordanian regulatory frameworks, where centralized control replaces independent authority in data protection, and legal drafting tends toward repetition rather than reform. The instruction documents annexed to the PDPL are binding administrative directives issued pursuant to Article 18 with legal force subordinate to the law itself, is a simple example for this, which in turn may render ineffective even the modest protections nominally provided by the PDPL. Their language is generic, often recycled from other administrative bylaws, and fails to provide meaningful clarity on key issues such as oversight mechanisms, enforcement procedures, biometric-specific safeguards, or standards for transparency and public accountability, which in turn leads to doubts about whether the legislative intent was to genuinely protect data rights, or merely to symbolically fill a legislative gap, or maybe, merely an image for show while everything runs on tradition standards.

In short, while the Council instructions and the Registry of Data Officers are formally positioned as the regulatory bylaws of Jordan's personal data governance

³⁰ International Covenant on Civil and Political Rights, adopted December 16, 1966, entered into force March 23, 1976, 999 U.N.T.S. 171, art. 17.

³¹ *Ibid.*, art. 2(3).

³² *Ibid.*, art. 26; Constitution of the Hashemite Kingdom of Jordan (1952, as amended), art. 6.

framework,³³ their language and implementation show concerning legal and institutional fragilities. They outline hierarchical procedures and bureaucratic roles as follows: appointment procedures for Council members, delegation authority for the President, confidentiality requirements for members, and secretariat management by the Minister. It fails to establish clear standards for overseeing high-risk data processing activities, particularly in the realm of biometric technologies. Who is responsible for these shortcomings? The PDPL does not specify which entity, not the Council, the Unit, Controllers, nor the government is accountable for ensuring biometric-specific safeguards. There is no mention of biometric-specific safeguards such as consent withdrawal mechanisms, no defined redress mechanisms for data subjects, and no evidence of independent oversight structures capable of limiting discretionary state access to sensitive data. This legal ambiguity and vagueness are especially problematic in the context of digital identity systems such as Sanad platform, which relies heavily on biometric authentication (i.e. fingerprints and iris scans) for identity verification, registration, service access and overall national digital inclusion. In the author's view, such absence of clear legal protection in these foundational governance texts allows platforms like Sanad to operate in a regulatory blackhole.³⁴

4. The Dilemma of Consent and Sanad System

On another important note, the PDPL appears to adopt a strong consent-based framework. Article 4 of the PDPL establishes the fundamental principle that personal data processing requires consent. Meanwhile, its internal logic has a series of contradictions that undermine this foundation in practice. For example, Article 4 of PDPL establishes that personal data may only be processed a) with the prior consent of the data subject or b) in cases expressly permitted by law (*ex lege*). Article 5 defines valid consent as written, explicit, specific, and informed.³⁵ While Article 6 immediately introduces a broad set of exceptions (regulating *ex lege* entitlement) that allow for data processing without consent including in cases of public interest, health purposes, or the functions of public entities without offering safeguards or criteria to prevent abuse. According to Article 6, the Processing is lawful and permissible without obtaining Consent or informing the Data Subject in the following cases:

1. Processing carried out directly by a competent public entity to the extent necessary for the performance of its legally assigned tasks according to the enacted legislation or through other entities contracted with the public entity, provided that the contract includes compliance with all obligations and conditions stipulated in this law, regulations, and instructions issued pursuant to the Law.

³³ The Registry of Data Officers (an official record of Controllers, Processors, and Data Protection Officers established under Article 18(D) of the PDPL).

³⁴ Alaeldin Alkhasawneh, "The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do We Need to Comply with the GDPR?," *Journal of Legal, Ethical and Regulatory Issues* vol. 23, issue 2 (2020): 5-10.

³⁵ Jordanian Personal Data Protection Law No. 24 of 2023, ss. 4-5.

2. If it is necessary for preventive medical purposes, medical Profiling, or the provision of healthcare by a licensed practitioner of any medical profession.
3. If it is necessary for protecting the life or vital interests of the Data Subject.
4. If it is necessary to prevent a crime or to disclose it by a competent authority or to prosecute crimes committed in violation of the law.
5. If it is required or permitted by any legislation or executed by a decision of the competent court.
6. If it is necessary for entities under the supervision and oversight of the Jordanian Central Bank to conduct their functions as determined by the Jordanian Central Bank, including the transfer and exchange of Data within and outside the Kingdom of Jordan.
7. If it is in accordance with the regulations pursuant to this law.
8. If it is necessary for scientific or historical research purposes, provided that it does not involve making any decision or action concerning a specific individual.
9. If it is necessary for statistical purposes, national security requirements, or for the public interest.
10. If the data being Processed is made publicly available by the Data Subject.

In addition to the data that has been processed shall not be retained after the purpose of the processing is fulfilled, unless otherwise specified by legislation.

Due to the wide legal basis for data processing *ex lege*, two questions arise that how are public interests measured and by what standards. Also, what determines the importance of the functions of public entities which leads to access over supposedly protected data? My field experience attempting to register for Jordan's digital ID via the Sanad platform, it was never asked to provide written or electronic consent, nor was informed in writing of what data would be collected or how it would be used. My verbal expression of interest in testing the system was treated as implied authorization for biometric data processing, including attempts to scan the fingerprints and irises. This experience illustrates a practical reliance on assumed or informal consent despite the legal requirement for documentation. It also raises serious concerns about the implementation of the law's requirement of valid consent particularly in high-risk technologies such as biometric authentication. In systems like Sanad, the distinction between consent-based and exception-based processing becomes blurred leaving individuals uncertain of their rights and unable to challenge misuse.

4.1. The Digitalization of IDs in Jordan

Sanad (سند), meaning "support" or "backing" in Arabic³⁶, is the national digital identity and service access platform launched by the Jordanian Ministry of Digital Economy and Entrepreneurship.³⁷ The Sanad platform was launched by the Ministry

³⁶ Ibid., Schedule 2 (Arabic definition of sensitive data), <https://www.arabdict.com/ar/>, accessed November 6, 2025.

³⁷ Ministry of Digital Economy and Entrepreneurship, "Sanad Application Overview" (Amman: Ministry of Digital Economy and Entrepreneurship, 2025), https://www.modee.gov.jo/En/NewsDetails/The_Mini

of Digital Economy and Entrepreneurship as a key part of Jordan's national e-government and digital transformation strategy. Interestingly, it was introduced before the (PDPL) was passed. As Jordan's push to digitalize services like e-government rapidly outpaced the creation of laws to protect personal data in that new digital space. This means Sanad was effectively launched into a regulatory blackhole. When it was introduced, there was no specific law or regulation that defined the standards for biometric governance or the protocols for user consent. This legal gap allowed the platform to be deployed and begin processing sensitive data without the specific data protection framework or safeguards that the PDPL would later (theoretically) provide. It has been developed as part of Jordan's broader e-government and digital transformation strategy, this platform has a vision to ease access to government service including civil status records, driving licenses, health records, social security enrollment, and tax services through a single authenticated digital identity. Sounds tempting to save time and energy, but registration for Sanad requires the collection and verification of biometric identifiers, mainly fingerprints and iris scans linking physical identity to a digital profile.

In practice, Sanad is available for use by both Jordanian citizens and non-Jordanian residents within the Kingdom. According to the platform's publicly available terms of service the initial registration requires users to submit basic information including their National ID or Personal Number, email address, and personal phone number, which are then stored within the Ministry of Digital Economy and Entrepreneurship's e-government systems.³⁸ Upon login users must enter their National ID/Personal Number and a password to access services. The application further specifies that user information may be disclosed to entities in the public or private sector, or by law, purportedly to provide optimal services or to protect the rights and safety of users or others, including responding to governmental requests which sounds typical or classic for any app or online platform.³⁹

If we look at it from a data protection and human rights perspective, the consent mechanism is legally ambiguous: users are compelled to agree to data collection and potential third-party sharing as a condition of access without meaningful choice or granular consent options. Second, this consent must be based on detailed information of rights, risks and right to withdraw the consent. Thirdly, the scope of permissible data disclosures is framed in broad and undefined terms, which allows information sharing with public and private actors based on undefined notions of service optimization or safety. Fourth, the transfer of data processing to third parties without clear guarantees (oversight mechanisms, contractual conditions) is problematic regarding compliance with core data protection regulation in law and principles such as data minimization and accountability under international standards

stry_of_Digital_Economy_and_Entrepreneurship_on_Sunday_launched_an_updated_version_of_the_egovernment_service_Sanad_application%20accessed%2026%20April%202025, accessed November 6, 2025.

³⁸ Ministry of Digital Economy and Entrepreneurship, "Sanad Terms of Use," <https://sanad.gov.jo/en/terms-of-use>, accessed November 6, 2025.

³⁹ Ibid.

like the GDPR.⁴⁰

Additionally, no mention is made in the Sanad platform materials of special protections for sensitive data categories, that includes biometric identifiers collected during registration. In the light of absence of biometric-specific protections and given the weak regulatory framework previously discussed, the Sanad platform effectively operates within a legal loophole by placing the burden of risk disproportionately on users, many of whom may not be fully aware of the extent or implications of data processing activities conducted through the system given the fact that digital illiteracy is still a problem in Jordan.

4.2. Data Processing Mechanism on Sanad Platform

First, let us take a look at the general picture of Sanad personal data processing mechanism:⁴¹

1. Information collected by the SANAD app may be transferred to entities in the public or private sector, or by law, to provide optimal services or to protect the rights and safety of users or others, or to investigate fraud or respond to government requests while ensuring privacy for all users. This data transfer occurs under Article 6 of the PDPL, which permits processing without consent for public interest, service provision, and government requests, though the law government services does not specify clear criteria or safeguards for such transfers.

2. The Ministry of Digital Economy and Entrepreneurship is entitled to cooperate with data processing companies to improve the level of digital government services (such as online document issuance, civil registry access, social security applications, and e-government portal authentication). The Ministry will use appropriate methods to protect and maintain the confidentiality of information as required by law.

Although the Ministry (MoDEE) is the principal organization responsible for developing and operating the Sanad platform, the legal framework governing its biometric data processing is notably deficient. As mentioned earlier in the analysis, the Personal Data Protection Council which is theoretically tasked with overseeing compliance under the PDPL, clearly lacks structural independence as it is chaired by the same Minister who directs the Ministry responsible for Sanad's deployment. Consequently, there is a complete conflict of interest, no genuine independent oversight of the platform's data processing legality. Despite the PDPL's recognition of biometric data as "sensitive personal data"⁴² requiring explicit and written consent under Articles (4 and 5), the Ministry appears to rely on the broad exceptions enumerated in Article (6) specifically those relating to public service provision in

⁴⁰ Regulation (EU) 2016/679, art. 5(1)(c), art. 5(2).

⁴¹ Ministry of Digital Economy and Entrepreneurship, "Sanad – Frequently Asked Questions," <https://www.sanad.gov.jo/en/modules/faq>, accessed November 6, 2025.

⁴² According to the definitions in Article (2) of the PDPL, biometrics are fall under the definition of sensitive personal data. This is the only sentence that mentions biometrics explicitly and clearly in said law.

order to justify the collection and processing of biometric data without obtaining proper documented consent from users.⁴³ So, Sanad started operation without any specific law or regulation that defines biometric governance standards, consent protocols or independent audit. This regulatory loophole created because Sanad launched before the PDPL entered into force and the PDPL's biometric provisions remain vague, specifically Article 6's broad public interest exception, which allows government entities to process data without consent or clear limitations and it enables the platform to function outside the core and scope of protections envisioned by the PDPL, resulting in raising safety concerns about data processing, protection, human rights and the general abuse of power.

4.3. Alternative Verification Methods

The risks inherent in Sanad's biometric processing framework are compounded by the platform's limited and problematic alternative verification pathways. In cases where biometric enrollment fails (see my attempted registration) users are instructed to authenticate their identity through a linked bank account within the Jordanian financial system. However, not all banks in Jordan are currently contracted with the Ministry of Digital Economy and Entrepreneurship to integrate with Sanad's infrastructure not all banks in Jordan are currently contracted, so basically speaking, bank participation in Sanad integration is voluntary, not mandatory.⁴⁴ If a user does not already possess an eligible bank account, the proposed solution is to immediately open a new account, a process often facilitated within minutes. This leaves individuals with little meaningful choice: either enroll in the banking system without proper information of data processing, consent and conditions of a bank contract, thus subjecting themselves to another layer of biometric data collection and surveillance or choose to remain excluded from accessing e-government services.

It is worth mentioning that many banks operating in Jordan also requires biometric authentication as part of their Know Your Customer (KYC) procedures,⁴⁵ including facial recognition or fingerprint scanning for account verification, mobile banking access and regulatory compliance under Central Bank which fall outside the PDPL's scope as they are issued under separate banking regulations, creating parallel

⁴³ Jordanian Personal Data Protection Law No. 24 of 2023, ss. 4-6.

⁴⁴ Field note, Sanad registration attempt (Amman, April 2025). During author's field experience, the employee attempted to create the author's digital ID fifteen times out of a seventeen-attempt limit. Upon failure, he explained that because the author's bank was not contracted with the Ministry of Digital Economy and Entrepreneurship, the author would need to create a new bank account in order to proceed with registration. Although the author mentioned holding a frozen account with another Jordanian bank, it was not among the approved institutions. The author was then offered the option to open a new account with a contracted bank, which the author declined. This terminated the registration process, as no alternative to biometric authentication or a partnered bank account was available.

⁴⁵ Example, Jordan Kuwait Bank, "Biometric Authentication Services Overview," <https://www.jkb.com/en/individuals/digital-banking/biometric-authentication-services>, accessed November 6, 2025.

data processing requirements.⁴⁶ In the author's view, the supposed alternative method to biometric enrollment in Sanad does not meaningfully eliminate biometric dependency; it simply shifts the burden onto parallel financial systems equally reliant on sensitive personal data. This dynamic exacerbates the risk of exclusion for individuals who cannot or do not wish to submit their biometrics and solidifies the position of a model of identity verification that is structurally dependent on biometric processing without offering accessible opt-out mechanisms or non-biometric pathways. From a human rights perspective, the absence of proper or classic alternatives undermines the principle of free and informed consent and raises more issues under the right to equality, privacy protections, and non-discrimination in which all are cherished and guaranteed under international law.

The right to privacy, as enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), guarantees that no individual shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence.⁴⁷ Secondly, the right to equality before the law and non-discrimination,⁴⁸ demands that digital identity systems be designed and implemented in a manner that does not disproportionately exclude or disadvantage certain groups particularly individuals who, for technical, personal, religious, or philosophical reasons, may not wish or be able to enroll biometric identifiers. The question of whether or not the government plans to pay attention to this issue lies on the shoulders of policymakers and regulatory authorities, who bear the responsibility to ensure that digital identity systems are designed and implemented in compliance with international human rights standards, particularly the right mentioned earlier. Free consent also means that no disadvantage or advantage may arise from the use of the (public) service.

By conditioning access to essential government services on mandatory (*ex-lege*) biometric enrollment, either directly through Sanad or indirectly via banking institutions, Jordan's digital identity framework risks violating these fundamental protections and human rights. The absence of accessible, non-biometric alternatives undermines the principle of free and informed consent as articulated in international data protection instruments such as European Convention 108⁴⁹ and protocols and those also echoed in the GDPR.⁵⁰ Specifically speaking, GDPR Recital 32 emphasizes that consent must be freely given, specific, informed, and unambiguous and must not be a condition for access to services unless strictly necessary such as ticking a box on a website or selecting technical settings, indicating the data subject's agreement to the processing of their personal data. Importantly, silence, pre-ticked boxes, or inactivity

⁴⁶ Central Bank of Jordan, *Instructions of Anti-Money Laundering and Counter Terrorist Financing for Electronic Payments and Money Transfer Companies No 12/2018* (Amman: Central Bank of Jordan, 2018).

⁴⁷ International Covenant on Civil and Political Rights, 999 U.N.T.S. 171, art. 17.

⁴⁸ *Ibid.*, art. 26.

⁴⁹ Council of Europe, *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS No. 223, opened for signature October 10, 2018.

⁵⁰ Regulation (EU) 2016/679, recital 32, arts. 4(11), 7.

do not constitute valid consent.⁵¹ The structure embedded in Sanad's design and operational framework can be considered a failure to uphold these basic human rights standards, thus bringing serious questions about the seriousness in intentions and lawfulness of Jordan's current digital identity and biometric governance practices and efforts.

It is needed to conduct awareness campaigns about fundamental rights and technology, workshops to fight digital illiteracy, even with the tribal society being a challenge to navigate.

5. Discussion on Jordanian Digital System

From a human rights lens, Jordan creates the visible trappings of a rights-based framework. Specifically, the PDPL grants citizens explicit rights on paper. As I identified earlier, these include the right to give explicit and written consent (Art 4-5), the right to withdraw that consent (Art 10(a)(2)), and the right to request the deletion of their personal data (Art 17(d)). This is the spectacle, as in a public-facing performance of compliance with global norms. The Sanad platform is transitioning from an optional convenience to a mandatory infrastructure for all public services which clearly directs the citizens and refugees alike to the illusion of freedom and consent. This creates a structural paradox. The law gives a right (e.g., Art 17 deletion), but the state's infrastructure for Sanad makes exercising it impossible without catastrophic consequences. If a citizen exercises their Article 17 right to delete their biometric data, they are de facto excluded from the mandatory Sanad system and, by extension, from accessing their basic rights as a citizen. This is not a choice; it is an ultimatum.

Additionally, Jordan is legally bound to follow Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR). The country is a state party to the ICCPR, having ratified it in 1976.⁵² By doing so, Jordan has undertaken international legal obligations to respect and ensure the rights in the Covenant, including the right to an effective remedy. The Jordanian digital framework creates a structural violation that right, as guaranteed under Article 2(3) of the ICCPR. This article is not merely aspirational; it places a positive obligation on the state to provide remedies that are supposed to be effective in practice not just in theory, and to have that remedy determined by a competent authority (Art 2(3)(b)).⁵³ The Jordanian

⁵¹ Regulation (EU) 2016/679, recital 32. It is worth noting that Recital 43 clarifies that consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. This supports earlier arguments mentioned in this research.

⁵² International Covenant on Civil and Political Rights, adopted December 16, 1966, entered into force March 23, 1976, 999 U.N.T.S. 171, art. 2(3). Jordan acceded to the Covenant on May 28, 1975. See UN Treaty Collection, "Chapter IV. Human Rights. 4. International Covenant on Civil and Political Rights," https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=en,

⁵³ Human Rights Committee, General Comment No. 31 on Article 2 of the Covenant: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004).

system, as analyzed in this paper, fails this legal test on both counts. In the examples given earlier regarding Sanad transitioning the administrative system in Jordan, this creates a structural paradox that renders the remedy punitive. If a citizen exercises their Article 17 right to delete their biometric data, the practical result is not reparation; it is de facto exclusion from the state leading to an inability to access administrative services, education, or civil status records. A remedy that forces a citizen to choose between their right to privacy and their right to health, by inflicting catastrophic civil exclusion, is not effective by any legal standard.

Secondly, the law fails the competent authority test. Even if a citizen were to seek this flawed remedy, Article 2(3)(a) requires a mechanism to challenge an official acting in an official capacity.⁵⁴ The competent authority designated by the PDPL to hear such a claim is the Personal Data Protection Council (Art 16). As mentioned earlier, this Council is chaired by the Minister of Digital Economy and Entrepreneurship. This is the very official, acting in an official capacity, who is responsible for developing, promoting, and mandating the Sanad platform, the very instrument causing the violation. This creates a legal absurdity where the citizen is required to seek a remedy from the architect of the violation. The 2025 reform, therefore, the author believes it portrays a pure legal theatre because it focuses on the Department's minor procedures while studiously avoiding this core, unconstitutional conflict, ensuring no effective remedy can ever exist.

6. Comparative Analysis: Jordanian PDPL vs. GDPR and Human Rights Commitments

As a result of the aforementioned analysis, a systematic comparison of the Jordanian PDPL against the GDPR and international human rights commitments reveals several factors that can be summarized in the table below. The **Table 1** provides a simple comparative analysis of the core provisions relevant to this chapter's research concerns.

Table 1. Comparative Analysis: Jordanian PDPL vs. GDPR

Core Provision	Jordan PDPL (Law No. 24 of 2023)	GDPR & Human Rights Standards	Gap/Deficiency Analysis
----------------	-------------------------------------	-------------------------------	-------------------------

⁵⁴ International Covenant on Civil and Political Rights, 999 U.N.T.S. 171, art. 2(3)(a).

Core Provision	Jordan PDPL (Law No. 24 of 2023)	GDPR & Human Rights Standards	Gap/Deficiency Analysis
1. Supervisory Authority Independence	Council chaired by Minister of Digital Economy; 8 of 12 members are government officials (67%); no structural independence (Art 16)	Supervisory authority must act with complete independence, free from external influence (GDPR Art 52)	Critical deficiency: Ministerial control undermines independence; violates GDPR Art 52 requirement for autonomous oversight
2. Legal Basis for Processing	Broad consent-based framework BUT extensive exceptions for "public interest" and "legal obligation" without clear definition (Art 6)	Six clear, exhaustive lawful bases with strict interpretation; no blanket "public interest" exception (GDPR Art 6)	Loophole: Vague "public interest" exception allows unlimited government data processing without accountability
3. Sensitive Data Protection	Includes financial data as "sensitive" but grants Council discretionary power to add/remove categories (Art 2)	Biometric data for unique identification is explicitly a special category requiring specific, narrowly defined legal basis (GDPR Art 9)	Missing: No explicit protection for biometric data; no special safeguards for Sanad's mandatory biometric enrollment
4. Consent Requirements	Requires consent but undermined by extensive exceptions; no clear definition of valid consent in main law (Art 4-6)	Consent must be freely given, specific, informed, and unambiguous; right to withdraw consent at any time (GDPR Art 4(11), 7)	Weakness: Exceptions swallow the rule; mandatory Sanad enrollment contradicts "freely given" consent principle
5. Data Subject Rights	Rights to access and deletion mentioned but not detailed; procedures delegated to subordinate regulations (Art 5)	Comprehensive and detailed rights including access (Art 15), erasure (Art 17), portability (Art 20), all specified in main regulation	Procedural gap: Rights exist on paper but lack implementation mechanisms; no portability right

Core Provision	Jordan PDPL (Law No. 24 of 2023)	GDPR & Human Rights Standards	Gap/Deficiency Analysis
6. Transparency & Accountability	No requirement for public reporting; Council meetings at discretion of Minister (Instructions Art 3)	Supervisory authorities must produce public annual reports on activities (GDPR Art 59); transparency by design	Accountability deficit: No public reporting requirement; no transparency mechanisms; ministerial discretion over disclosure
7. Remedies & Enforcement	Right to effective remedy vague; complaints handled by Council (compromised by lack of independence); must seek remedy from body chaired by Minister	Right to effective judicial remedy against supervisory authority AND controller (GDPR Art 78-79); right to compensation for material/non-material damage (GDPR Art 82); independent adjudication	Access to justice gap: No independent remedy mechanism; no explicit right to compensation; Council judges its own government
8. Biometric Data Governance	Classified as sensitive data BUT subject to same broad exceptions; no specific safeguards for mandatory systems like Sanad (Art 2, 6)	Biometric data for unique identification is special category requiring explicit consent OR substantial public interest with specific, proportionate safeguards (GDPR Art 9)	Critical gap: Mandatory biometric enrollment (Sanad) operates without specific legal basis, consent mechanism, or proportionality assessment
9. Legal Hierarchy & Certainty	Complex web of 12 subordinate implementation documents (instructions, regulations, standards); binding force unclear	GDPR is directly applicable regulation; hierarchy is clear; implementing acts must be consistent with main regulation	Legal uncertainty: Fragmented regulatory framework; instructions may contradict law; unclear binding force creates enforcement gaps

Core Provision	Jordan PDPL (Law No. 24 of 2023)	GDPR & Human Rights Standards	Gap/Deficiency Analysis
10. Equality & Non-Discrimination	Mandatory biometric enrollment for Sanad creates two-tiered system: those who comply vs. those excluded from e-government services	Processing must not result in discrimination (GDPR Recital 71); right to equality and non-discrimination is fundamental right (ICCPR Art 26, Jordanian Constitution Art 6)	Structural discrimination: Sanad creates digital exclusion for those unable/unwilling to provide biometrics; no alternative pathways; violates equality principle

Source: comparison made by the author based on legislative provisions

7. Conclusion

In conclusion, this fast-paced development rendered in Jordan reveals a deeper contradiction within the PDPL. Although the law formally grants individuals the right to withdraw consent and request deletion of their personal data,⁵⁵ the fast shift toward Sanad-based service access suggests that exercising these rights could effectively result in exclusion from essential government functions. If access to public services becomes fully dependent on maintaining a digital identity linked to biometric authentication, then the rights to data withdrawal and deletion become hollow guarantees, available in theory, but inaccessible in practice. This contradiction highlights a fundamental weakness in Jordan’s emerging digital governance model by showcasing the tension between proclaimed data rights protections and the realities of mandatory centralized biometric systems that offer individuals little meaningful choice or recourse.

All what has been mentioned so far, falls under the Personal Data Protection Directorate, which is not mentioned as a term in the PDPL. It’s defined as the body within the ministry that holds the council mentioned earlier. It’s defined on the ministry’s website as “It is the organizational unit specialized in protecting personal data and ensuring the right to privacy by ensuring compliance with the provisions of the PDPL (No. (24) of 2023) and the regulations and instructions issued pursuant thereto in the Hashemite Kingdom of Jordan. The unit aims to strengthen the position of the Hashemite Kingdom of Jordan in the field of personal data protection and legislation and policies supporting the protection of the digital environment.”⁵⁶

According to my assessment, the PDPL suffers from significant structural

⁵⁵ Jordanian Personal Data Protection Law No. 24 of 2023, ss. 4(b)(2), 8(f), 10(a)(2), 17(d).
⁵⁶ Ministry of Digital Economy and Entrepreneurship, "Personal Data Protection Directorate," <https://www.modcc.gov.jo/EN/Pages/>, accessed April 28, 2025. Last accessed on April 28, 2025. The ministry's website is constantly crashing and may not be found temporarily.

deficiencies that undermine its capacity to protect individuals' fundamental/human rights effectively. Among the PDPL weaknesses is the extensive discretionary authority granted to governmental bodies, combined with the absence of an independent supervisory authority tasked with overseeing compliance, although they named a council to supervise compliance, the author came to many conclusions showing multiple short-comings and contradictions. Parallel to this issue, the law's ambiguous language concerning national security exceptions further risks facilitating intrusive data practices without meaningful safeguards. Although domestically promoted as a step toward modernizing data governance, the PDPL's framework may, in practice, reinforce existing power asymmetries and facilitate surveillance under the appearance of legal protection. Observations raised by civil society organizations, including Access Now and SMEX correspond with such emphasize the law's inability to adhere to global data protection standards, such those set forth by the GDPR.⁵⁷

What are the directions for future analysis? Looking forward, in-depth examination is required as to why the PDPL is not applied in the identification processes for Syrian refugees or Palestinian displaced persons.⁵⁸ Instead, personal identification in these cases is governed by separate systems administered by UNHCR and UNRWA under their respective Memoranda of Understanding with the Jordanian government.⁵⁹ These parallel frameworks operate outside the national legal system giving a flag about state responsibility and legal accountability. When compared to the standards set by the GDPR it becomes clear that these humanitarian registration systems lack many of the legal safeguards that would otherwise be required under international human rights and data protection law.⁶⁰

Additionally, Jordan's use of biometric technologies in border and immigration contexts such as through its e-visa system deserves attention in light of the principle of non-refoulement under the Refugee Convention,⁶¹ as well as the broader EU-Jordan cooperation on migration and mobility. Official sources claim compliance with open data principles and data protection commitments,⁶² but the lack

⁵⁷ Access Now, "Jordan's Flawed Data Protection Law Grants the Government Excessive Powers," press release, September 20, 2023, <https://www.accessnow.org/press-release/jordan-flawed-data-protection-law>, accessed April 26, 2025; SMEX, "Jordan's Personal Data Protection Law: Between Protection and Control," September 20, 2023, <https://smex.org/ar/البيانات-الشخصية-2-الأردن>, accessed November 10, 2025.

⁵⁸ André Bank, "Syrian Refugees in Jordan: Between Protection and Marginalisation," *GIGA Focus Middle East*, no. 3 (2016): 1–10.

⁵⁹ Memorandum of Understanding between the Government of Jordan and the United Nations High Commissioner for Refugees (1998), <https://www.unhcr.org/sites/default/files/legacy-pdf/5461e6070.pdf>, accessed April 28, 2025.

⁶⁰ 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 (General Data Protection Regulation), *Official Journal of the European Union* L 119/1.

⁶¹ Convention Relating to the Status of Refugees, opened for signature July 28, 1951, 189 U.N.T.S. 137, entered into force April 22, 1954, art. 33.

⁶² European Commission, "EU–Jordan: A New Partnership to Better Manage Mobility and Migration," press release, October 9, 2014, https://europa.eu/rapid/press-release_IP-14-1109_en.htm, accessed November 10, 2025.

of detailed legal provisions and independent oversight raises doubts about the adequacy of such claims.

This research will also consider how Jordan's commitments under the EU Mobility Partnership,⁶³ and subsequent frameworks for cooperation on digital governance and migration intersect with its domestic laws and biometric practices.⁶⁴ This line of inquiry is particularly relevant not only for understanding current policy gaps, but for questioning whether data-driven governance models in migration management are compatible with international standards and the rights of vulnerable populations.

Bibliography

1. Alkhasawneh, Alaeldin, "The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do We Need to Comply with the GDPR?," *Journal of Legal, Ethical and Regulatory Issues* vol. 23, issue 2 (2020): 5-10.
2. An'imat, Mohammad Al, "Technical Protection for Electronic Banking Operations in Jordan," *Curentul Juridic*, no. 1(92) (2023): 94-109.
3. Bank, André, "Syrian Refugees in Jordan: Between Protection and Marginalisation," *GIGA Focus Middle East*, no. 3 (2016): 1-10.
4. Baruphakēs, Giannēs and Zumpulakēs, Michaēl S. "On Technofeudalism: What Killed Capitalism? An Interview with Yanis Varoufakis," *Economic Thought* 11, no. 2 (2023): 25-30.
5. Central Bank of Jordan, *Instructions of Anti-Money Laundering and Counter Terrorist Financing for Electronic Payments and Money Transfer Companies No 12/2018* (Amman: Central Bank of Jordan, 2018).
6. Council of Europe, *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS No. 223, opened for signature October 10, 2018, <https://rm.coe.int/16808ac918>.
7. European Commission, "EU-Jordan: A New Partnership to Better Manage Mobility and Migration," press release, October 9, 2014, https://europa.eu/rapid/press-release_IP-14-1109_en.htm, accessed November 10, 2025.
8. Gane, Nicholas, "Capitalism Is Capitalism, Not Technofeudalism," *Journal of Classical Sociology*, vol. 25, issue 4, (2024), <https://doi.org/10.1177/1468795X241269293>.
9. Gilbert, Jeremy, "Techno-Feudalism or Platform Capitalism? Conceptualising the Digital Society," *European Journal of Social Theory* 27, no. 4 (2024): 561-578.
10. Memorandum of Understanding between the Government of Jordan and the United Nations High Commissioner for Refugees (1998), <https://www.unhcr.org/sites/default/files/legacy-pdf/5461e6070.pdf>, accessed April 28, 2025.
11. 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 (General Data Protection Regulation),

⁶³ Hashemite Kingdom of Jordan, Open Government Data Policy, Jordan e-Government Portal: <https://form.jordan.gov.jo/wps/portal/Home/OpenDataMain/OpenDataUser>, accessed November 10, 2025.

⁶⁴ European Parliament and Council, "Joint Declaration Establishing a Mobility Partnership between the Hashemite Kingdom of Jordan and the European Union and its Participating Member States," October 9, 2014.

- Official Journal of the European Union L 119, 4.5.2016, pp. 1–88.
12. Swyngedouw, Erik, "Capitalism Is Over, but the New Is Worse: Reflections on Rent, Services, and Capitalist Feudalism," in Moulaert, Frank and Abid Mehmood (eds.), *The Value of Place*, (Cheltenham: Edward Elgar Publishing, 2025), 23-39, <https://doi.org/10.4337/9781035347926.00009>.
13. United Nations, *Convention Relating to the Status of Refugees*, opened for signature July 28, 1951, 189 U.N.T.S. 137, entered into force April 22, 1954, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-relating-status-refugees>.
14. United Nations, Human Rights Committee, *General Comment No. 31 of the Covenant: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004), <https://digitallibrary.un.org/record/533996?v=pdf>.
15. United Nations, *International Covenant on Civil and Political Rights*, adopted December 16, 1966, entered into force March 23, 1976, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
16. Varoufakis, Yanis, *Technofeudalism: What Killed Capitalism* (London: The Bodley Head, 2023).
17. World Justice Project, "Rule of Law Index 2025: Jordan – Fundamental Rights" (Washington, DC: World Justice Project, 2025), <https://worldjusticeproject.org/rule-of-law-index/country/2025/Jordan/Fundamental%20Rights>, accessed November 6, 2025.