حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

Position Paper on the Personal Data Protection Draft Law by Decree from a Human Rights–Based Perspective

7amleh - The Arab Center for the Advancement of Social Media
2023

Position Paper on the Personal Data Protection Draft Law by Decree from a Human Rights–Based Perspective

Researcher: Cathrine Abuamsha

Revised and edited by: Andersen Palestine

Arabic language is edited by: Ritaj for Managerial Solutions

Graphic Design: Kamil Qalalwe

—---------

Contact us:

Email: info@7amleh.org

Website: www.7amleh.org

Telephone: +972 (0)774020670

Find us on social media: 7amleh

This paper aims to review the Personal Data Protection Decree draft, presenting a clear position on it—a stance deeply rooted in the bedrock principles of the 2003 Amended Basic Law and the relevant international conventions and standards. Through the prism of this analysis, 7amleh - The Arab Center for the Advancement of Social Media aspects tied to transparency, the imperative for the cabinet to unveil this draft for public discussion, and the significance of these elements and stepping stones. The narrative then veers into exploring the essential, overarching principles of privacy, advocating for their inclusion within the draft. It also delves into the commitment to embedding the rights of data subjects, weighing the accomplishments and pitfalls on this front. The paper wraps up with a compendium of recommendations, a path forward to refining the legal landscape surrounding the right to privacy in Palestine, aiming for a more constitutional and human rights–centered approach.

Introduction

In the intricate web of the digital world, privacy and protection are cardinal digital rights. These rights are interwoven with every individual's footprint in the digital space, including the use of various platforms and applications of social media.[1] While several international conventions touch on the right to privacy, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR) explicitly and fundamentally enshrine its protection in Articles 12 and 17 thereof, respectively. As the right to privacy evolves and permeates more profoundly into the myriad layers of individual and collective existence, intersecting with digital spaces, identity, and life beyond the screens, this right is recognized as a cornerstone for individuals to enjoy and exercise their sundry rights and freedoms both online and offline. In 2015, this imperative prompted the United Nations Human Rights Council to initiate the first mandate on privacy: The Special Rapporteur on the right to privacy.[2] Around the world, countries are developing laws to guide the actualization of this right both offline and online. According to the United Nations Conference on Trade and Development (UNCTAD),[3] 137 out of 194 countries have legislated applicable privacy and data protection laws, while Palestine is ensconced within the minimal 9 percent that have draft laws on this matter, none of which have seen the light of day. [4]

Following Palestine's accession to seven fundamental international human rights conventions in 2014—especially the unconditional embrace of ICCPR, the onus is squarely on the Palestinian Authority (PA) to undertake all conceivable steps, including the enactment of legislations, to comply and honor all its commitment and avowals vis-à-vis rights and freedoms under this covenant, with privacy being a key component.[5] Despite these binding commitments and the provisions of Article 1 (10) of 2003 Amended Basic Law, which categorically states, "Basic human rights and liberties shall be protected and respected," and Article 17, which clearly puts it, "Homes shall be inviolable; they may not be subject to surveillance, broken into or searched, except in accordance with a valid judicial order and in accordance with the provisions of the law," a comprehensive and integrated Palestinian law on privacy protection concept, grounds, and rules—including the aspect of digital personal data—is conspicuously absent. This legislation is crucial

1 "The right to privacy in the digital age." United Nations, November 1, 2013. Available at: https://www.ohchr.org/en/stories/201310//right-privacy-digital-age.

2 "The Special Rapporteur on the right to privacy." United Nations. Available at: https://www.ohchr.org/en/special-procedures/sr-privacy.

3 UNCTAD official website. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

4 "Data Protection and Privacy Legislation Worldwide." Available at: https://rb.gy/hs93q.

5 "International Covenant on Civil and Political Rights," Article 2. UN. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

for empowering Palestinians to comprehend their rights and duties and to ascertain accountability for any indiscriminate exploitation of data, irrespective of the sector, be it civil, private, public, or others, in keeping with the State of Palestine's obligations under international conventions and covenants.[6] Nonetheless, a committee, assigned in 2016 to draft a law on personal data protection, is still entangled in the deliberations within the cabinet and has been referred to the concerned ministries for review and observations for the third time. [7]

A human rights organization, 7amleh channels its unwavering effort to advance Palestinian digital rights. Integral to its mission, 7amleh seeks to promote the right to privacy and digital personal data protection. The center publishes several reports, surveys, studies, and guides, shining a light on the multifaceted landscape and concept of privacy as well as emphasizing the paramount importance of protecting sensitive data from the clutches of Israeli occupation and any form of unauthorized intrusion, exploitation, processing, and communication within the sensitive tapestry of Palestinian society. These concerted efforts are augmented by extensive training programs, workshops, and seminars, all geared toward raising public awareness about this critical right and laying it out for constant public debate. 7amleh also engages in a suite of digital campaigns and advocacy meetings aimed at bringing positive change in the landscape of the right to privacy and pressuring decision-makers to make a law protecting personal data and the right to privacy—legislation ingrained in constitutional ethos, participatory praxis, transparency, human rights approaches, and international global standards. Aligned with this commitment, this position paper from 7amleh reviews the Palestinian Personal Data Protection Decree draft, according to its third reading, dated June 15, 2022, rendering analytical observations and in-depth analysis of its articles.

Concepts and References

Before delving into the observations on the personal data protection draft decree, it is perhaps imperative to define the term personal data. These data include any pieces of information, whether directly or indirectly related to a particular individual, that facilitate the determination of their identity. The scope of personal data is comprehensive, including, but not limited to, names, addresses, birth dates, email addresses, phone numbers, photographs, electronic account information, social media details, medical records, financial specifics, and identification numbers. These data can be used to

6 Although Cyber Crimes Decree No. 10 of 2018 does touch upon the right to privacy in article 22, it merely stands as a broad prohibition against privacy violations. A full framework is required in the form of a law that examines every aspect of privacy, recognizing it as an inherent human right.

7 Hashtag Palestine 2022, p. 18. 7amleh - The Arab Center for the Advancement of Social Media. Available at: https://7amleh.org/202302/02//hashtag-palestine-1119-palestinian-digital-rights-violations-during-the-year-2022.

recognize an individual, communicate with them, analyze their behavior, or offer them a slew of services.

Privacy, a cardinal basic human right,[8] draws the invisible lines dictating the extent to which society can intrude into individual lives, with personal data a pivotal frontier within these limits.[9] Article 17 of the ICCPR firmly states, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." For any intervention to be legitimate and nonarbitrary, both offline and online, it must conform to the principles of legality, necessity, proportionality, and judicial authorization—meaning that an independent judicial body sanctions the interference.

At their core, personal data protection laws are anchored with a key raison d›être: to uphold the privacy and protection of personal information and regulate the mechanisms that others interact or handle. This aim is realized by enforcing essential conditions and procedures that construct the legal boundaries for the processes involving these data—from collection and storage to processing and transmission, among others. This body of laws should lay down the relevant crimes in this field and the corresponding penalties,[10] whether the intrusion occurs through immediate human involvement or through systems and programs that automatically amass, store, process, transfer, or share data without the need for direct human intervention.

Following a meticulous review of the draft Palestinian Personal Data Protection Decree, 7amleh furnishes its observations, principally grounded in the principles of Palestinian Basic Law, the seminal international human rights conventions (to which the State of Palestine has acceded), reports and recommendations of the United Nations Special Rapporteur on the right to privacy, and other relevant international standards. Beyond this, 7amleh substantially embraces the tenets of the European Union General Data Protection Regulation (GDPR), which stands, in the present discourse, as the most inclusive, accurate, affirmative, and congruent framework, harmonizing with the global principles of human rights for personal data protection offline and online.

8 "International Covenant on Civil and Political Rights," Article 17. op. cit.

9 "Wāqiʿ al-Khuṣūṣiya wa-Ḥimāyit al-Bayānāt ar-Raqmiya fy Filasṭīn [The landscape of privacy and data protection in Palestine: Exploratory study]." Available at: https://7amleh.org/202125/08//hmlh-ytlq-tqryr-jdyd-hwl-waqa-alkhswsyh-whmayh-albyanat-fy-flstyn.

10 The European Union General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/art-1-gdpr/.

Review of Draft Decree No. () of 2022 on Personal Data Protection

As the third reading stands, Draft Decree No. () of 2022 on Personal Data Protection unfolds across ten pages, featuring thirty-nine articles sorted into six distinctive chapters. Throughout these chapters, the draft addresses both the procedural and substantive dimensions of personal data protection: Definitions and General Provisions, The Formation of the Authority and Its Responsibilities, Personal Data Processing, Personal Data Exchange and Transfer, Sanctions, and, ultimately, Final Provisions. While the initiation of this law is commendable and a significant stride toward fortifying the rights of Palestinians, its developmental stages and content are infused with several elements that necessitate scrutiny and critique. These points of concern are as follows:

- **Transparency and Public Consultation**

The Palestinian Basic Law makes it clear that the power derives from the people.[11] Therefore, it is imperative for decision-makers to engage the public and civil society in every phase of law creation. This involves the public disclosure of draft laws and a transparent exposition of the underlying reasons and justifications for such legislation, opening the floodgates for stakeholders, concerned parties, and the members of the public to share their reflections and critiques within well-established and unequivocal timelines. Pursuing genuine public consultations and unrestricted, comprehensive deliberations is nonnegotiable, bringing experts and representatives of civil society organizations, academia, the bar association, and the private sector to the table—including electronic service providers and other stakeholders. In the same vein, accessible avenues for the public members to participate in the consultations and share their insights should be provided. These observations should be channeled to inform the drafts before they are signed into law. This avoids a top-down imposition that undermines the collaborative value inherent in the legislative process. [12] The sine qua non of full disclosure of every public information about these laws and regulations asserts the unassailable imperative for public information access legislation, an inalienable human right.

In the current Palestinian context—the Palestinian political division since 2007 and the suspension of the Legislative Council and its eventual dissolution by Supreme Constitutional Court Ruling No. 102018/—the PA president, i.e., head of the executive power, has been using the exceptional power to make decrees based on Article 43 of the Palestinian Basic Law. It is perhaps fitting to indicate that this power is reserved for "in cases of necessity that cannot be delayed, and when the Legislative Council is not

11 The Palestinian Amended Basic Law of 2003, Preamble.

12 Lessons from the EU GDPR. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.accessnow.org/wp-content/uploads/201901//Updated-version-BOOKlet.pdf.

in session, to issue decrees that have the power of law." Although these decrees have predominantly violated the prerequisites of Article 43, over four hundred such decrees addressing a range of issues[13] have nonetheless been proclaimed from 2007 to the time of writing this position paper. The vast majority of these have not been opened up to public debate or comment. This persistent exclusion underscores enduring apprehensions about the implications of not sidelining Palestinians in their diversity in the deliberation and understanding of the draft decree on data protection—a law devised to regulate their personal data and lives. These concerns are especially troubling given the proposal's progression to its third reading at the cabinet. This scenario marks a blatant disregard for one of the core principles for sound legislation and compliance with human rights standards, deviating from the optimal practices in the cabinet's legislative drafting guide and the public consultations manual. It emphasizes the critical and immediate need for the long-anticipated promulgation of robust information access law.

- **Personal Data: Legal Principles**

Personal data protection legislation must ab initio delineate, with utmost clarity, the essence of data. It should draw lines among the different types and establish protection tiers for each—be it mere personal or sensitive personal data, like those uncovering particularly delicate personal attributes, such as an identity number. The law is expected to provide clear-cut definitions and outline the fundamental tenets of every process the data undergo. It should encompass all related entities: the user/owner, the controller, and the processor(s) or distributors (to third entities). The eight principles below are instrumental in establishing the legal framework for data processing, including security, transmission, and exchange procedures: [14]

1. **Lawfulness, fairness and transparency:** Data must be processed lawfully, fairly and transparently in relation to the subject of the data according to clear legal grounds, a transparent, legitimate purpose(s), or both. The legal foundation must, at its core, be in harmony with the tenets and articles of the ICCPR and the overarching principles of human rights.

2. **Purpose limitation:** Data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible manner. For example, detecting specifics of a crime, crime prevention, and maintaining national peace and order, provided that these objectives are well-defined and accessible to the average members of the public.

13 "Al-Qararāt bi-Qānūn wa-Ṣiyāghit at-Tashriʿāt wal-Mushawarāt al-Aāmma [Decrees, Legislation, and the Public: A Discussion on Consultations.]" Wattan. Available at: https://www.wattan.net/ar/news/380753.html

14 EU GDPR. Chapter 5. Available at: https://gdpr-info.eu/

3. **Data minimization:** Collected/processed/transmitted/shared data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy:** Utmost accuracy should be maintained when dealing with personal data, and provisions should be made for individuals to modify and erase their data through simple, straightforward procedures. This includes IT steps and solutions to ensure the preservation and updating of data and establishing standards to erase or rectify any inaccurate smidgen of information. Every reasonable step must be taken to ensure the protection and confidentiality of data and prevent any unauthorized or illegal usage or violations.

5. **Storage limitation:** Personal information should not be stored for longer than necessary for the purposes for which the personal data are processed.

6. **Upholding the rights of data subjects:** Every data processing must be executed with profound respect for the rights of the data subjects.[15]

7. **Integrity and confidentiality:** Data should be processed to ensure optimal security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

8. **Appropriateness:** It is incumbent upon the authorities to enforce constraints on data transmission between jurisdictions to ensure optimal protection. Such processes should permit the uninhibited flow of this data but obstruct its transfer when the receiving jurisdiction is incapable of assuring an acceptable protection level. Hence, the originating state must know and comprehend the protection standards and criteria within the receiving jurisdiction.

Upon a thorough review of the personal data protection draft decree, it is evident that, to a large extent, the principles outlined above have been integrated into its articles. Nevertheless, there is a conspicuous emphasis on data collection and processing, sidelining pivotal elements like data transmission and dissemination. With care, the draft delves into the essence of legitimacy and the crucial importance of establishing clear parameters for the purpose and duration of personal data processing. It highlights the sine qua non of acquiring informed consent from the data subjects and reinforces their inherent right to challenge any part of the data processing. While the draft allows the restriction of data review under several conditions, it does not allocate due diligence to

15 Procedural Guide to Palestinian Personal Data: Protection in the Digital Space. 7amleh, June 13, 2023. Available at: https://7amleh.org/202313/06//procedural-guide-to-palestinian-personal-data-protection-in-the-digital-space

the accuracy of the data and other data subject's rights, including the right to erasure. This omission risks the data itself and the subject's rights.

- **Rights of Data Subjects**[16]

To protect personal information, legislation must lay down all the rights of the users/data subjects with utmost clarity and in explicit, understandable terms. Such provisions must be easily quantifiable when examining different scenarios associated with data processing, even those of a complex nature. In this vein, 7amleh's Procedural Guide to Palestinian Personal Data Protection in the Digital Space sheds light on every relevant right, its nuances, and the conditions for application. These rights are formulated to affirm that the subjects of personal data have comprehensive control and transparency over the ways their data are handled and the consequent processing, instituting protective measures for any illicit or unfair handling of such data.

In light of this, we underscore critical observations concerning the compliance of the draft decree with the rights of the data subjects, drawing upon the bases laid out in the EU GDPR and other international benchmarks, including the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).[17] These rights are critical to personal data, without which exhaustive and appropriate data protection remains infeasible.[18]

1. **Right to Access Information and Personal Data:** Collectors of personal data are mandated to provide access to individuals whose data are collected and ensure comprehensive and transparent disclosure regarding the methods, purposes, and duration of such collection and processing. Additionally, data controllers and processors must uphold transparency by promptly informing individuals when there is an intention to utilize their data divergent from the original purposes, outlining all aspects of the new purpose, thus maintaining individuals' control over their data and safeguarding their rights. Furthermore, entities, in their roles as controllers and processors of data, are under an obligation to maintain a record of the proceedings involved in data processing. This record should explicitly contain the name and contact information of the entity exercising control over the data. The purpose of data processing, a description for the classification of the data being processed and the subjects, the entities that will be able to access the data, the processes of transferring data to other countries, the

16 EU GDPR. Chapter 3. Available at: https://gdpr-info.eu/

17 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108). Available at: https://www.coe.int/en/web/data-protection/convention108-and-protocol.

18 Access Now, op. cit.

duration of storage of each type of data, and a general description of the organizational and technical measures put in place to maintain the confidentiality of the information, in addition to any other necessary particulars. Within its thirty-nine provisions, the draft decree addresses the right to access data by data subjects, particularly Articles 25, 27, and 28.

2. **Right to rectification:** This inherent right empowers the subjects of the data to seek corrections or modifications to any personal data about them that is either inaccurate or incomplete. It encompasses the right to proffer supplementary or rectifying statements from the data subject. The negligence in rectifying inaccurate or incomplete personal information becomes a breeding ground for sustained propagation and utilization of these inaccuracies. This failure exacerbates the dissemination of misleading and misinformation, engendering a climate where misinformation flourishes, having adverse repercussions on individuals' personal and professional reputations. What is more, it could also give rise to individual decisions anchored on flawed or unsuitable grounds. While globally, this right is enshrined as foundational entitlement in the legal frameworks and legislations of data protection, the Palestinian personal data protection draft decree data has, notwithstanding its mention in Article 25, conspicuously omitted to elucidate its substance and the mechanism of its execution or even discussing its admissibility under delineated terms, merely stipulating: "The data subject may 1) request rectifying their data. It does not delve into the details or acceptance conditions that follow such a request. Most importantly, no affirmation ensures that the request procedures are simple and accessible for average members of the public.

3. **Right to erasure ('right to be forgotten'):** This right empowers the data subject to request the controller to erase their personal data under specific conditions, such as the lack of legal grounds for retaining or processing the data or the fulfillment of the data collection purposes. The draft decree should set these conditions and instances. However, this fundamental right is conspicuously absent from the personal data protection draft decree, raising pertinent questions about the motives behind such omission. This neglect to codify the right to erasure ('right to be forgotten') can result in significant risks, including privacy violations and the continued unauthorized use of data, potentially leading to unfair categorizations of individuals and the subsequent erosion of trust, with possible negative legal and economic repercussions for the entities managing or processing the data. Thus, it is crucial to enshrine, respect, and enforce this right to safeguard privacy and align with the international and human rights conventions that the State of Palestine, being a signatory to numerous human rights treaties, is obligated to uphold and implement.

4. **Right to restriction of processing:** In our interconnected world, every individual holds the unassailable right to call for a halt in processing their data under certain circumstances, particularly when they challenge the accuracy of said data or discern the processing to be unlawful. [19] Articles 20 and 21 of the personal data protection draft decree provide for potential restriction of data processing, enveloping aspects of retracting processing consent. However, when juxtaposed with the provisions of GDPR, an international benchmark for personal data protection legislation, a discernible opportunity emerges to augment this right's essence. It can be achieved by detailing constraints not solely emanating from consent revocation and by rendering the right more comprehensive, aligning it with Article 18 of GDPR. When this right is put into action, it warrants an immediate cessation of data processing and use. The data then can only be reutilized with new consent from its data subject and strictly for defined purposes, such as drafting legal contentions or exercising legal defense, defending the rights of other persons, or accomplishing the common good.

5. **Right to data portability:** The data subject has the right to receive the personal data concerning them in a structured, commonly used and machine-readable format and may transmit those data to another controller without hindrance from the controller to which the personal data have been provided. While chapter 4 of the personal data protection draft decree addresses the subject of personal exchange and transfer, setting the conditions and limitations of transfer, it completely omits any reference to the right of data subjects to request the transfer of data from one controller to another. This might unleash a myriad of risks tied to the data and their subjects, involving a threat to their control over their data. Individuals might find themselves constrained by the controller even if the users' satisfaction diminishes concerning the controller's services or the automatic processing. This could restrict their choice and their ability to move to a different controller that aligns better with their needs. Plus, there is the potential for entities in control to monopolize the collection and storage of data with no avenue for change. This could negatively affect the competitive landscape among those controlling the data, thus lessening the opportunities for performance improvement in protecting the rights of those whose personal data are collected.

6. **Right to object:** The right to object allows individuals to oppose processing their personal data for reasons tied to their specific situation. The law should detail these reasons and identify the solid legal grounds that would allow the processing entity to continue processing despite the objection. While Article 23 of the draft decree on data protection recognizes this right, it confines it to three specific areas, overruling the individual's entitlement to contest the use of their personal data for the purposes of direct marketing. Theoretically, individuals are entitled to voice opposition at

19 Procedural Guide to Palestinian Personal Data: Protection in the Digital Space, op. cit.

any juncture where their personal data is processed for such advertising purposes, potentially involving profiling to the extent that it correlates with the data subject through this direct marketing.[20]

7. **Automated individual decision-making, including profiling:** The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. The omission of this crucial right in the conclusive draft of the data protection law is glaring; it is an aspect that merits thoughtful reflection and advocacy among concerned authorities, necessitating a proactive stance in urging the decision-makers to make the necessary amendments. On this matter, insights can be drawn from Article 22 of the GDPR.

8. **Right to consent to data processing:** While Article 20 requires the data subject's consent, it overlooks the prerequisites for legitimate consent. It is imperative to revise it to incorporate provisions that ensure the data subject's rights, making it clear that consent is a freely given, specific, informed and unambiguous indication of the data subject's wishes by which they agree to the processing of their personal data for a specific purpose or set of purposes. Moreover, a clear provision that the burden of demonstrating the legality of consent rests with the controller is crucial, including proving methods.

9. **Right to an effective judicial remedy:** Article 5(5) of the personal data protection draft decree sets forth the responsibilities and specialties of the National Personal Data Protection Committee, indicating its jurisdiction to adjudicate complaints lodged by data subjects against controllers, the recipient of personal data, or the processor, along with complaints filed by the controllers against any party, following guidelines formulated by the authority for these ends. However, while the draft assigns the complaint oversight role to the National Personal Data Protection Committee, Chapter Five concurrently prescribes sanctions aligned with this draft or other statutory frameworks that penalize privacy breaches, e.g., Law by Decree No. 10 of 2018 on Cybercrime. This accentuates the potential recourse to judicial bodies in instances of privacy violations, specifically regarding personal data.

10. **Right to compensation and liability:** The inherent right to obtain equitable compensation for any individual who has incurred material or nonmaterial damage due to processing the personal data of the data subject: The fifth chapter of the draft does allocate criminal penalties for law breaches by entities but fails to specify and assert the right to claim and receive fair compensation when the damage is substantiated.

20 EU GDPR. Article 21. Available at: https://gdpr-info.eu/

Based on the draft decision of the personal data protection law, chiefly regarding the rights of data subjects, it is evident that it lacks a provision that safeguards every right of data subjects. It simply delineates the right to access, object, limit processing, and refer complaints to the relevant authorities without thoroughly addressing all dimensions of these rights. While it provides for the rights to access, object, and restrict processing and the entitlement to file complaints to relevant authorities, it does not address data subjects' rights concerning data portability. The draft also leaves out certain rights and does not mention them at all, like the right to erasure and the right not to be subject to automated individual decision-making, including profiling. The absence of these crucial elements renders the draft potentially flawed if it is ratified and enacted as legislation purposed for personal data protection.

It is perhaps critical to highlight that although the draft legislation on personal data protection does make allowances for certain key rights, the disarrayed and segregated exposition of these rights across different sections notably attenuates the structural solidity and legal congruity of this draft. In this situation, the draft does not provide a clear and seamless pathway for understanding the rights and limitations of data subjects. With this approach, the draft decree fails to provide an effortless scope for grasping the rights and boundaries of data subjects with clarity and smoothness. For instance, while some rights of the data subjects are integrated within the draft, Article 25 restricts these rights to: "the data subject has the right to 1) Seek rectification of their data. 2. Request a copy of their data," seemingly implying these are the entirety of the rights afforded to data subjects. In the subsequent progression, Article 25(2) is intricately explained within varying sections, notably Article 27(3), related to data security. Here, it covertly delves into facets correlated with the right to retrieve personal data, synonymous with the right of access, allowing for a comprehensive understanding of individual data rights in keeping with the GDPR principles. This complexity shrouds the understanding of the draft decree and the enveloped rights, potentially impeding the practical construe of its articles once approved. In this context, 7amleh underscores the imperative to word and present the draft coherently in harmony with the tenets of legislative drafting, advocating reference to the EU GDPR as an international benchmark in this domain.

- **The National Personal Data Protection Committee**

National personal data protection committees play a crucial role in safeguarding personal data and privacy and implementing the relevant personal data protection legislation. To have the mission of these bodies accomplished in the sui generis Palestinian landscape, their absolute independence is crucial, including a resilient shield against any form of

influence from governmental or private entities.[21] These regulatory bodies should also exemplify an advanced degree of professional acumen and specialized technical insight. They must ensure their capability to guide and counsel individuals and institutions on compliance with data protection standards, whether found in the foundational legislation dedicated to safeguarding personal data or in ancillary statutes. The latter may encompass provisions that intertwine with personal data protection or stipulate protective measures in various sectors.

National authorities should be vested with the executive powers to implement laws and provide pivotal advice and instructions. They are also to be mandated to supervise compliance with a relevant corpus of legislation, carrying frequent inspections to ascertain compliance with data protection directives. When laws are breached, these bodies should have the power to enforce appropriate sanctions. In concerted efforts with relevant bodies, they should raise awareness about data protection legislation and exchange of information with international data protection watchdogs, thereby strengthening transborder data protection initiatives. In essence, the raison d›être of these national entities is to safeguard personal data and ensure the rigorous and effective implementation of laws.

While the personal data protection draft decree provides an elaborate discourse on the formation and specifics of a National Personal Data Protection Committee in Articles 3 to 17, a clear breach of the independence principle is evident in Article 2(3). This article brings the national authority under the aegis of the cabinet, implicating a tether to the executive power. Such a structural configuration may impinge on its autonomy, casting shadows on its impartiality and resilience against potential transgressions or infringements by executive apparatuses. Beyond that, Article 2(8) mandates that “the chair and board directors shall be appointed by a cabinet’s decision,” implying a stand-alone and independent decision purely by the executive authority.

Despite the fact that Article 2(3) of the draft decree dedicates a specific item in the general budget for this authority. Article 6(2) and (3) vests in the cabinet the power to decide on the financial accountability of this national entity. In a similar vein, Article 15 provides that “the cabinet shall, by regulation, set the compensation and allowances allotted to the president, and the remuneration and allowances assigned to the members of the board, of the [Personal Data Protection National] committee.” This unequivocally illustrates the authority’s absolute dependence on the cabinet.

The imperative for establishing the National Personal Data Protection Committee for, along with its board, inherently warrants members with higher qualifications and track record of experience in the same field. Notwithstanding, Article 1(8) lends the draft decree further

21 EU GDPR. Chapter 6. Available at: https://gdpr-info.eu/

ambiguity, "The authority is governed by a board of directors that consists of a chair and six members. Each member must be qualified and experienced in their fields." In layman's terms the draft decree does not specify the required experience or qualification to be exclusively in privacy, digital data, and the legal background, consequently compromising the board's credibility and reliability in supervising personal data protection and upholding the rights of data subjects.

A comprehensive examination of the draft's articles related to the National Personal Data Protection Committee reveals an explicit blueprint devoid of any semblance of professional and financial independence. It also substantially deviates from the customary norms associated with specialized fields. This context amplifies grave concerns regarding the authority's effective performance in protecting personal information. The potential to enforce unswerving accountability for every breach, unauthorized access, and any manifest bias affecting such delicate data is questionable, irrespective of the presence or influence of the concerned entities. This inherently establishes an ambiance of distrust concerning data protection, undermining public confidence in the actions and decisions of this authority.

Conclusion

With a stroke of critical acuity, 7amleh advocates for well-thought-out Palestinian legislation that enshrines and protects personal data, an urgent international obligation since 2014. An in-depth examination of the Palestinian personal data protection draft decree reveals a slew of problems. These span a spectrum of concerns, from questions of transparency in its formulation to its autonomy and to defects associated with articles pertaining to the rights of those whose data are at stake. This demands the urgent obligation to disclose this draft decree, propelling it into profound public comment and discussion, all while being anchored in international standards and core legal tenets at each step, with an aspiration to perfect a comprehensive personal data protection law that lives up to the anticipation and conforms with the legislative sanctuary called for by 69 percent of Palestinians, according to 7amleh's surveys.[22]

Beyond the substantive and formal issues explored in the analysis of the personal data protection draft decree, it is crucial to canvass any Palestinian legislation on personal data protection as a conduit to raise awareness about the rights it enshrines and protects. It should not be leveraged solely as a punitive instrument but as a reference guiding public, private, and civil entities to attain deeper adherence to and reverence for personal

22 "Perceptions of Privacy and Personal Data Protection in the Occupied Palestinian Territory." 7amleh. June 27, 2022. Available at: https://7amleh.org/202269-/27/06/of-palestinians-in-the-west-bank-and-gaza-strip-support-privacy-and-data-protection-legislation

data protection. The laws in question should encapsulate overarching safeguards for data protection. This incorporation obliges all related bodies to disclose clear privacy policies, allowing for clear insight into these bodies' compliance with the established personal data indicators. In the final analysis, the anticipated Palestinian personal data protection legislation ought to be all-encompassing, obligatory, and steeped in solid legal foundations, boosting awareness, protection, development, and just, equal, and lawful accountability for the rights and obligations of all.

Recommendations

1. Transparent, inclusive general elections—both legislative and presidential—should be held in a transparent and inclusive manner, with an unwavering commitment to honoring the results. The Legislative Council's cardinal role in legislating—including the expeditious promulgation of personal data protection and information access laws—should be invigorated.

2. The personal data protection draft decree should be released for public comment and consultation. Similarly, consultations should be held with civil society organizations, experts, and other stakeholders, offering accessible avenues for all to share their insights and observations. There should be firm compliance with the directives and standards set forth in the legislative drafting guide and the public consultation guide approved by the cabinet.

3. All concerned and relevant agencies should review the draft decree to develop a rendition rooted in human rights and viable for pragmatic implementation. This penultimate should consider the substantive and formal issues by integrating the rights of data subjects and phrasing to ensure accuracy and coherent progression of the content, chiefly about rights, facilitating comprehension, application, and guidance.

4. The establishment of the National Personal Data Protection Committee, including its board and functions, should be grounded in the principle of the separation of powers, upholding operational financial independence, transparency, and impartiality. The formation and composition of this authority should be based on specialization. It also needs to be allocated adequate financial and human resources and mandate to access all public and governmental privacy and data protection procedures and information.

5. Last but not least, government agencies should devote concerted efforts to raise the awareness of all sections of Palestinian society about the multifaceted right to privacy, including personal data protection. To this end, a budget needs to be designated, and plans and programs should be tailor-made to bring these endeavors to fruition, all while ensuring optimal accountability for each action and step taken on this path.