April 2022

Policy brief: How to strengthen Jordan's data protection law

Introduction

On December 29, 2021, Jordan's Council of Ministers endorsed a new data protection draft law and passed it to parliament for debate and consideration. The new law aims to protect individuals' personal data, in line with the rights and freedoms enshrined in Jordan's constitution, as well as to "foster the trust necessary to engage in the digital economy and to contribute to encouraging e-commerce and online services in Jordan."

Legislative context: four iterations of the data protection bill

Currently there is no data protection law in Jordan. In 2014, the Ministry of Information and Communications Technology (now Ministry of Digital Economy and Entrepreneurship) proposed a new draft law for the protection of personal data. It launched the first public consultation in November 2016, and formed a committee to discuss the draft bill composed of the Ministries of Interior and Labor, the Telecommunications Regulatory Commission, the Central Bank, and Information and Communications Association of Jordan.

Civil society groups raised significant concerns over the bill, particularly with regard to the proposed structure of the future data protection authority. The draft law of 2017, for instance, proposed that the new Data Protection Council, mandated to investigate complaints on privacy violations among other duties, be chaired by the ICT minister.

As Jordanian civil society groups flagged, there is a conflict of interest attaching the Council to the ICT Ministry, since the latter "has a great interest in developing the tech sector, representing companies whose interests are to collect the largest amount of personal data and not necessarily protect the rights of the data owners." The Council would also include members of security agencies which would further undermine its independence and autonomy as an oversight body.

A second major concern was that the bill allowed the disclosure or sharing of data by order of a public prosecutor rather than a court order as stipulated in Article 18 of the Jordanian Constitution. Furthermore, the bill did not include mention of biometric data or sensitive personal data as a category that requires a higher threshold of protection.

In September 2018, the ICT Ministry issued a third amended draft, this time modeled on the European Union's General Data Protection Regulation (GDPR), and introduced obligations on data collectors and processors as well as advancing rights for data subjects.

After a few years of stalemate, Jordan's Council of Ministers endorsed a new draft bill on December 29, 2021, and passed it to parliament for debate and consideration. The bill requires approval by both the lower and upper houses of parliament to become law. The new draft recognizes biometric data as sensitive personal data. It also maintains the previous problematic structure of the data protection authority.

Jordan's draft data protection bill vs. E.U.'s GDPR

In order to analyze the robustness of the proposed data protection regulatory framework, Access Now conducted a comparative analysis of the draft bill against the principles of the European Data Protection Regulation (GDPR). The GDPR sets one of the highest standards for data protection globally. Alignment of the legislation with the GDPR may positively impact the European Union's decision to grant Jordan an adequacy decision to allow for data flows and transfer between the E.U. and Jordan.

The draft law adopts a number of basic principles of the GDPR **in 15 of its 24 articles,** such as the rights granted for data subjects as well as obligations on data controllers. There are, however, significant differences and loopholes that undermine the robustness of the law as a data protection framework. These are: *data transfer, the structure of the Personal Data Protection Board (the equivalent of the Data Protection Authority or DPA) and the Personal Data Protection Competent Organizational Unit within the Ministry ("the Unit"), the measures to deal with leaks, errors, and infringements, and the compulsory authorization requirement to process data.*

1. Compatibility with GDPR

Many of the legal definitions and provisions proposed in the new bill are modeled on the GDPR. Despite being a different bill from the third amended draft issued in September 2018, this text has Article 2, which defines "personal data" very similarly to the GDPR. Other legal definitions, such as "sensitive personal data" and "data processing," are either verbatim or improved versions of the E.U. regulation. Moreover, the exemption for processing data made in Article 3(b), which stipulates that "the provisions of this law shall not be applicable to natural persons who process their data for their own purposes," is identical to the household exemption of the GDPR. Similarly, the draft law's provisions regarding legitimate processing of data (Article 6(a)) and retention (Article 6(b)) are in line with the GDPR.

The mandate and different functions of the future DPA are also compatible with the European standard, except for a missing part on sanctions and whether the annual report of the DPA mandated by the law will be made public. Some of these roles and responsibilities include "the establishment and monitoring of the implementation of policies, strategies, plans, and programs relating to data protection" and "the adoption of prior consent, consent revocation, objection, and request forms to be submitted by the concerned person in accordance with the provisions of the present law."

Additionally, measures and sanctions taken in case of errors or infringements on data protection as mentioned in Article 19 have some resemblance with the GDPR in terms of the delay to inform the Unit. In fact, the Jordanian draft law scores better in terms of duration required to inform data subjects in case of infringements, with a period of 24 hours instead of 72.

Finally, Article 22 stipulates that "Prior to the provisions of this law entering into force, all entities that handle data shall commit to get regularized in accordance with the present law within a maximum of one year following its enforcement," which is very similar to the GDPR, with a shorter period of time for the legislation to be implemented (one year instead of two).

More of these similarities are detailed in the comparative table joint to this document (linked at the end).

2. Differences and loopholes:

In spite of the positive points detailed in the section above, there are significant concerns differentiating the bill with the E.U. regulation, falling under four key areas:

I. Data transfer:

Data transfer is an important issue addressed in the bill that has some differences with the European framework. For instance, Article 14 does not specify whether it applies to data transfer within Jordan only, even though Article 15 addresses international data transfer. Article 14 is problematic if this is not clarified, especially with its paragraph (a) which allows data transfer if it "serves legitimate interests for the official and the recipient." This stands at odds with the GDPR since data transfer cannot be justified on the basis of legitimate interest. Article 44 of the GDPR stipulates that *"any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization."* The underlying principle of the GDPR's rule on data transfer is to ensure that the recipient and the country where data is sent will protect the data, and that it will not be unlawfully transferred/accepted, so that the right to privacy, data protection, and access to remedy are ensured.

Article 15 is also problematic because it puts too much responsibility on the data subject (paragraph a(5)). Article 15(b) should also mandate keeping a documentation of the procedure to check whether the recipient outside Jordan can guarantee data security and protection as a condition to authorize data transfer to a foreign country.

II. *Problematic structure of the DPA and the Unit:*

According to the GDPR principles, the DPA must be independent to fulfill its duties. This is not the case in this bill: the DPA is not independent. The board is chaired by the ICT minister and representatives of the executive branch and security agencies are sitting members. The authority is attached to the executive branch, and has representatives from the security services on board, which is not acceptable for an independent oversight body.

It is acceptable, however, that nominations to sit on the DPA board come from the government or the executive branch in general, but they must be confirmed by the parliament after audition, and the ministry cannot be part of the DPA or decide who can and cannot sit in the authority board. The same principle of independence should apply to the Unit.

In addition, the annual report mentioned in Article 17(j) should be made publicly available.

III. *Measures to be undertaken in case of leaks, errors, and infringements:*

More specifications should be made to identify what constitutes a "serious error or infringement,"mentioned in Article 2 (the definition) and Article 19. It should also specify what compensations shall be made to the concerned person in case of harm (Article 19(b)). Moreover, the Unit and the affected person(s) should be simultaneously notified in case of infringement since the Unit can investigate the incident quickly and help provide immediate security tips to the affected data subject.

The 24-hour notification period to inform the concerned person(s) in case of error or infringement, even though it is shorter than the 72 hours period of the GDPR, should take into consideration the capacity of small companies which may not be able to comply with such a short notice rule. It can be raised to, for example, 48 hours.

In addition, the maximum amount of fine to be imposed on entities or companies for data protection violations (Article 20) should be equal to 5% of the global revenue of a company and not the local one. Otherwise, the fine could be insignificant for big or multinational companies, which may not incentivize them to comply with the law.

The affected data subject should also be granted the right to bring a case to the Unit (Article 20), which is the only unit mandated to conduct an investigation per the draft law.

IV. Compulsory authorization to process data:

As mentioned in Articles 20 and 23, an authorization to process data stands at odds with the GDPR, and gives too much control to the state. The GDPR is based on the principle of accountability, where a public institution or a private company can collect and process personal data as long as it is compliant with the law and can prove it through adequate documentation, in addition to agreeing on being overseen by a regulatory body.

A prior authorization or a license does not help in ensuring compliance with the law. In some countries, such as Egypt, the licensing requirement is introduced as a governmental tool to raise money. Most dangerously, such a requirement would grant the government full control of the overall data collection and processing ecosystem.

For more details, we outline here the full provisions that are either similar or incompatible with the GDPR:

Similar to GDPR - Advantages	**Different from GDPR - Loopholes**
2: Personal data: Any data or information relating to a natural person, regardless of their source or form, that may identify them directly or indirectly, including data on their person, family situation, or whereabouts. Definition similar to the GDPR. Very short definition, similar to the GDPR but with less details. It does not for instance include references to online identifiers as a link to personal data.	**2: Sensitive personal data:** Any data or information relating to a natural person, which directly or indirectly reveal their origin, race, opinions, political affiliations, or religious beliefs or any data relating to their financial situation or their health, physical, mental, or genetic condition, or their biometric fingerprint, criminal record, or any other information or data the Board deems sensitive if their disclosure or abuse harms the concerned person. Goes a bit beyond the GDPR (with the board being able to expand on it — not a bad idea). We would recommend adding communications to this point. We would recommend adding communications to this point.
2: Data: Personal data and sensitive personal data. Not different from GDPR per se, but different from EU law where data can be personal or	**2: Processing:** One or more processes conducted in any way, form, or means to collect, view, record, copy, save, store, organize, revise, exploit, use, send, distribute, publish, link to other data, make available, transfer, display, hide the identity, reconstitute, or destroy data.

non-personal (this distinction is also quite unclear in the EU).	A copy of the GDPR.
2: Official: Any natural or moral person whether within Jordan or abroad, who is in charge of the data. The meaning is unclear: does it refer to the data collectors/processors even though they are defined in other articles? Is it a new notion specific to Jordan?	**2: Diagnosis:** Automatic processing of data to identify the concerned person's tendencies, orientations, choices, or attitudes. Similar to "profiling" in the GDPR. If it has to be automated, so as soon as a human is involved, can we consider that there is no profiling? This is a potential loophole.
3: paragraph "a": The provisions of this law shall be applicable to all data, even those collected or processed prior to the law taking effect. Difficulties to have a retroactive effect of the law.	**3: paragraph "b":** The provisions of this law shall not be applicable to natural persons who process their data for their own purposes. Similar to the GDPR household exemption.
4: paragraph "b": Every concerned person shall enjoy the following rights: • Be aware of and able to view, access, and acquire data kept by the official. • Revoke their prior consent. • Validate, amend, erase, hide, add, or update their data. • Restrict processing to a specific scope. • Object to processing and diagnosis if they are unnecessary to achieve purposes for which data was collected, if they exceed the requirements, or if they are discriminatory, abusive, or illegal. • Transfer a copy of their data from one official to another. • Be Aware and informed about any breach, violation, or infringement to the security and integrity of their data.	**4: paragraph "c":** No financial or contractual implications shall be incurred by the concerned person for exercising their rights stipulated in paragraph (b) of this article. The GDPR also says that the exercise should be free of charge, but the contractual implications are not mentioned in the European framework and this is a great addition.

Very similar to the data protection rights guaranteed under the GDPR.	
5: paragraph "b": Prior consent shall be disregarded in the two following cases: If it was given based on invalid information or deceptive or misleading practices that led the concerned person to the decision of giving their consent. If the nature, type, or objectives of processing change without obtaining approval. Very good.	**6: paragraph "a": 1 - 3 - 4 - 5 - 6 - 7:** Processing shall be deemed lawful and legitimate and may be undertaken without prior consent or notification of the concerned person in the following cases: Processing conducted directly by a competent public entity to the extent required to carry out its statutory functions or through other contractual entities provided that the contract includes the respect of all obligations and conditions stipulated in the present law as well as in the regulations and instructions issued thereunder. If it is necessary to protect the concerned person's life or vital interests. If it is necessary to prevent or detect a crime by a competent entity or to prosecute crimes committed in contravention of the provisions of the law. If it is required, authorized under, or as part of enforcing any legislation or by decision of the competent court. If it is necessary for scientific or historical research purposes, provided that their purpose is not related to taking any decision or action regarding a specific person. If it is necessary for statistical purposes, national security requirements, or in favor of public interest. Similar to the GDPR.

6: paragraph "a": 2: If it was necessary for preventive medical purposes or for medical diagnosis or to assess health care by any person licensed to practise any medical profession. This is not exactly similar to the GDPR but it can be understood, although it should be limited to health care professionals and not include apps and similar solutions.	**6: paragraph "a": 8:** If data being processed are made available to the public by the concerned person. Different from the GDPR and that also depends on what "made available to the public" means. Is the data publicly posted on social media like Twitter or Facebook concerned, even if it is a private platform? Can people reuse it? This could lead to abuse or fraud if people can reuse other people's photos for example.
6: paragraph "b": Processed data may not be kept following the completion of the intended purpose, unless otherwise prescribed by legislation. Similar to the GDPR retention principle.	**7:** Processing shall meet the following requirements: ● Shall have a legitimate, specific, and clear purpose. ● Shall be consistent with purposes for which data has been collected. ● Shall be conducted by lawful and legitimate means. ● Shall be based on valid, accurate, and updated data. ● Shall not lead to the identification of the concerned person following the exhaustion of its purpose. ● Shall not lead to harm to the concerned person or undermine their rights, either directly or indirectly. ● Shall be undertaken in a manner that ensures information confidentiality and integrity and without making any changes to them. Very similar to the GDPR.
8: The official shall commit to the following: Take the necessary actions to protect data they keep and those received from another person. Take the security, technical, and organizational measures that guarantee the protection of data	**9:** Subject to Article (6) of the present law, the official, before processing begins, shall notify the concerned person either in writing or electronically about: ● Data to be processed and processing start date.

from any breach to their security and integrity as well as any unauthorized disclosure, modification, addition, damage, or action, as prescribed in the instructions issued by the Board for this purpose. Establish mechanisms and procedures that govern processing and receive and respond to complaints regarding processing in accordance with the provisions of the present law as well as with the regulations and instructions issued thereunder, in addition to the publication of such complaints on the official website and through available media outlets. Provide means to enable the concerned person to exercise their rights in accordance with the provisions of the present law. Correct incomplete and inaccurate data if found incorrect or inconsistent with reality before processing begins, except for data collected for the prevention, detection, or prosecution of a crime. Enable the concerned person to object to processing and to revoke their prior consent as well as to access and update their data. The official shall provide means they deem appropriate to enable such actions in a secure manner. The role of the controller under the GDPR. The nomenclature used is different from the GDPR, does the term "المسؤول" refers to "the controller" or "the official"? If it does not refer to "the controller", then what is its role under this bill?	• The purpose behind processing their data. • Period of data processing, provided that such period shall not be extended unless with the concerned person's approval and in accordance with the provisions of this law. • The processor who will be collaborating with the official to execute processing. • Security and safety controls to protect data as well as information about the diagnosis. Very similar to the GDPR, only missing information about transfer (or not) of data, and the rights that the concerned person has. Missing information about transfer (or not) of data, and the rights that the concerned person has.
10: Data shall be deleted or hidden, and the official shall take the necessary measures in this regard based on the concerned person or unit's request in any of the following cases:	**11: paragraph "b":** The controller shall have the following functions and responsibilities: • Monitor the official's actions regarding the protection of data and document their

• If processing is conducted for a purpose other than what data were collected for or in a way other than the one subject to prior consent. • If the concerned person revokes their prior consent upon which processing was based. • If data were processed in contravention to the provisions of the present law as well as to the regulations and instructions issued thereunder. • If data were related to the implementation of a legal or contractual obligation. If the data is no longer needed, we delete it and do not keep it even in a "hidden" state.	compliance with the provisions of the present law and relevant legislations. • Conduct periodic assessment and inspection on database systems, data processing systems, and systems ensuring data security, integrity, and protection. The controller shall document the outcome of the assessment and issue any required recommendations to protect data and then follow-up on the implementation of these recommendations. • Function as a direct liaison officer with the Unit as well as security and judicial entities with regards to compliance with the provisions of the present law. • Establish internal instructions to receive and examine complaints, data access requests, and requests to correct, delete, hide, or transfer data while enabling the relevant concerned person to carry out such actions in accordance with the provisions of the law. • Enable the concerned person to exercise their rights prescribed in this law. • Organize necessary training programs for the processing and official's staff members to prepare them to handle data in line with the requirements of the present law as well as with the regulations and instructions issued thereunder. • Any other entrusted functions or responsibilities in virtue of the present law as well as the regulations and instructions issued thereunder. The controller is called "the data protection officer" in the GDPR. The criteria to appoint a controller should also include: *"if the entity's main activity involves processing of data, in addition to all that is listed."* Basically, all tech companies should have a controller.
13: Data subject to processing is considered confidential. The official and processor shall bear the responsibility of keeping such data confidential. It perhaps misses an obligation to ensure data security as well.	14: It seems that this article is about data transfer within Jordan. This should be clarified.

14: paragraph "a": 1: Data may not be transferred and exchanged between the official and any other person, including the recipient, except with the approval of the concerned person and according to the following conditions: The transfer serves legitimate interests for the official and the recipient. This is very different from GDPR. Data transfer cannot be justified on the basis of "legitimate interests".	**14: paragraph "a": 2 - 3:** Data may not be transferred and exchanged between the official and any other person, including the recipient, except with the approval of the concerned person and according to the following conditions: The concerned person is sufficiently informed about the recipient and the purposes for which their data will be used. The purpose of transfer shall not be for product or service marketing, unless the concerned person agrees. These are all odd reasons to allow or not allow transfer — none similar to the GDPR. If a concerned person knows about the transfer but cannot do anything about it, how does it help? Transparency is not enough. And then saying that data cannot be transferred for marketing? Why not? It could be if data is sufficiently protected. **The whole point of transfer rules is to ensure that the recipient (and the country where the data is sent to) will protect the data and that the data will not be unlawfully accepted.**
14: paragraphs "b", "c", "d" & "e": The official shall commit to keeping records documenting transferred or exchanged data with the recipient and their purpose along with documenting the concerned persons' approval regarding transfers. Notwithstanding paragraphs (a) and (b) of this article, data may be transferred and exchanged between competent public entities to the extent required to carry out their statutory functions. The recipient shall be subject to the same legal responsibilities and duties established for the official. The official, processor, and recipient shall commit to ensure the security and integrity of data and to establish the appropriate means to help in detecting and tracking violations to their security and integrity.	**15: paragraph "a": 1:** Data may not be transferred to any person outside Jordan, including the recipient, in case the level of protection available to such data is less that what is stipulated in the present law, except for the following cases: Regional or international judicial cooperation under international agreements or treaties in force in Jordan. Different from the GDPR that has a specific mechanism for data transfers. **Suggestion:** trade agreements could be excluded from this scope to ensure that data and privacy rights are not lowered for commercial gains.

This is positive.	
15: paragraph "a": 2 - 3 - 4: Data may not be transferred to any person outside Jordan, including the recipient, in case the level of protection available to such data is less that what is stipulated in the present law, except for the following cases: • Regional or international cooperation with regional or international bodies, organizations, or agencies working on combatting or prosecuting crimes of all kinds. • Exchange of the concerned person's medical data when it is necessary to treat them. • Exchange of data relating to pandemics, health disasters, or anything that affects public health in Jordan. Even though the language is different, this makes sense.	**15: paragraph "a": 5:** Concerned person's approval to transfer after being informed about the lack of sufficient protection level. Not allowed under the GDPR: this puts too much responsibility on the concerned person, how can we be sure that the data is protected?
15: paragraph "b": Before beginning data transfer, the official shall check the protection level provided by the recipient outside Jordan to guarantee data security and protection. A documentation of the checking procedure should be kept.	**16: paragraph "a":** A Board named as "The Personal Data Protection Board" shall be formed and chaired by the Minister and shall include the following members: • Information Commissioner as Vice-Chairman • Commissioner-General for Human Rights. • Representatives of security services designated by their respective Directors and based on the Minister's request. • Four people with the relevant expertise and specialization, designated by the Minister. **This board is very different from GDPR, in a problematic way: it is not independent from the state** **The data protection authority must be independent to fulfill its duties; The chair of the board can be nominated by the state, and then confirmed by the parliament after audition, etc. but the ministry cannot be the head or seat there or decide alone who seats in the authority.**
16: paragraphs "b &"c": The Board membership	**17:** The Board shall have the following functions and

term shall be four years, renewable once. The Board shall issue instructions regulating meetings, decision-making mechanisms, and other matters related to the Board. Good overall. The board should also be able to issue fines and sanctions to ensure compliance with the law.	prerogatives: • Establish and monitor the implementation of policies, strategies, plans, and programs relating to data protection. • Adopt data protection standards and measures, including the code of conduct related to the official and processor's proper performance in their functions. • Issue permits and authorizations to keep, process, diagnose, and transfer data. • Adopt prior consent, consent revocation, objection, and request forms submitted by the concerned person in accordance with the provisions of the present law. • Specify the mechanism used to resolve complaints and requests submitted by the concerned person against the official, or those submitted by the official against any other official. The Board shall take the required resolving actions pursuant to instructions issued for this purpose. • Express views on treaties, agreements, legislations, and instructions related to data. • Represent Jordan in local, regional, and international events related to data protection. • Issue a periodically updated list of countries or international or regional bodies or organizations certified by the Jordan of having a sufficient level of data protection. This list shall be published in any manner the Board deems fit. • Propose international cooperation plans on data protection, exchange experiences with international bodies and organizations, and coordinate and cooperate with governmental and non-governmental entities and agencies to ensure the integrity of data protection procedures. • Establish the annual report on data protection, which shall be drafted by the Unit and submitted to the Ministerial Cabinet. • Any other functions related to data protection. Good overall. Missing part on sanctions.
17: paragraph "j": Establish the annual report on	**18:** The Unit shall have the following functions and

data protection, which shall be drafted by the Unit and submitted to the Ministerial Cabinet. The report should be made publicly available.	prerogatives: • Prepare and submit to the Board draft legislations and instructions related to data. • Receive and investigate reports and complaints relating to the infringement of the present law as well as the regulations and instructions issued thereunder. The Unit shall, thereafter, submit recommendations to the Board to take the appropriate decision. • Monitor adherence to the present law as well as to the regulations and instructions issued thereunder. • Establish, oversee, and organize a record of data protection officials, processors, and controllers in accordance with instructions issued by the Board for this purpose. • Draft the annual report on the work of the Unit and submit it to the Board to be adopted. The Unit shall conduct any other missions assigned by the Minister or the Board. The Unit has an important role: who decides who is a member of it? The Unit should be independent, too.
19: paragraph "a": 1: When a breach to the security and integrity of data that would cause significant harm to the concerned person occurs, the official shall undertake the following actions: Notify concerned persons whose data have been compromised, within 24 hours of discovering the breach, and provide them with the necessary procedures to avoid any consequences that would stem from such breach. Much better than the GDPR: it is within 72 hours and only if there is a risk. 24 hours could be a very short period and it might be hard for some small companies to comply. Maybe raise it to 48 hours?	**19: paragraph "a": 2:** Notify the Unit, within 72 hours of discovering the breach, about the origin and mechanism of the breach as well as the concerned persons whose data have been compromised. The official shall also notify the Unit about any other information available regarding the breach. Similar delay with the GDPR. A bit odd that the Unit would be notified after the affected data subjects. They should both know at the same time as the Unit can investigate the incident and help provide immediate security tips.
19: paragraph "b": In case of serious error or	**20: paragraph "a":** In case of any violation of the

infringement, the official shall be committed to compensate the concerned person. Even though this does not exist in the GDPR, it is for sure a deterrent risk that would incentivize companies to be careful. The GDPR does not have this. What constitutes a "serious error or infringement"? This should be specified as well as the compensation.	provisions of the present law as well as of the regulations and instructions issued thereunder, the Unit shall warn the violator to cease their action and remove its causes and impacts within a period specified in the warning. If that period has elapsed without abiding by the warning, the Board shall decide on any of the following penalties, based on the Unit's recommendation: As a lesson learned from the GDPR, the warning issued by the Unit to the violator should have a deadline. We recommend a period of one month.
20: paragraph "a": 1: Give a warning about the partial or full suspension of the permit or authorization. People/entities should not have to apply for an authorization or a permit to process data.	**20: paragraph "a": 4:** Impose a financial penalty not exceeding 500 Dinars for every day the violation continues, with a maximum imposed fine of 5% of the violating official's total annual revenues for the previous financial year. The maximum amount of the fine should be equal to 5% of the global revenue of a company and not the local one. Otherwise, the fines could be too small and some entities would engage in unlawful activities.
20: paragraph "c": Taking any of the actions stipulated in paragraph (a) of this article shall not preclude the aggrieved person's right to civil damages incurred due to the violation of the provisions of the present law as well as of the regulations and instructions issued thereunder. The concerned person should also be able to bring a case to the Unit. According to this version, it is only the Unit who has the right to investigate without the possibility for a citizen/entity to request an investigation.	**22:** Prior to the provisions of this law entering into force, all entities that handle data shall commit to get regularized in accordance with the present law within a maximum of one year following its enforcement. Similar principle with the GDPR, even though the period is two years for the GDPR. Different period: two years for the GDPR instead of one year.
23: paragraph "a": The Ministerial Cabinet shall issue the necessary regulations to implement the provisions of the present law, including: Types, conditions, requirements, and suspension or annulment cases of permits and authorizations issued in accordance with the provisions of this law as well as entities exempted from acquiring permits and	

authorizations along with allowances required for their issuance and renewal.

An authorization to process data is odd and gives too much control to the state.

The GDPR does have accountability principles instead, where you can operate and use data as long as you comply with the law, show documentation that proves compliance and agree to be overseen by a regulator (the Unit).

A prior authorization/license will not help to ensure compliance, it is only a tool for the government to potentially raise money and at the same time, give it control over the infrastructure.

Recommendations:

1. **Specify if Article 14 concerns the data transfer within Jordan only or not: amend Article 14.**

---

2. **Ensure that the data transfer as mentioned in the law abides by the principles of the right to privacy, data protection, and access to remedy, by ensuring that the recipient and the country where data is sent meet these requirements, and by keeping a documentation of the transfer: amend Articles 14 and 15.**

---

3. **Ensure the independence of the Data Protection Authority and the Unit from the executive branch to fulfill their role of oversight: amend Articles 16 and 18.**

---

4. **Make the annual report of the DPA available to the public: amend Article 17(j).**

---

5. **Provide a clear and exhaustive definition of what constitutes a "serious error or infringement": amend Articles 2 and 19.**

---

6. **Take into consideration the capacity of small and medium companies to inform the concerned person(s) in case of error or infringement by raising the 24 hours notification period to 48 hours: amend Article 19(a).**

---

7. **Notify the concerned person and the Unit simultaneously in case of infringement, allowing the Unit to investigate the incident quickly and help provide immediate security tips to the affected data subject: amend Article 19(a).**

---

8. **Specify what compensations shall be made to the concerned person in case of harm: amend Article 19(b).**

9. **Fix the maximum amount of the fine to be imposed on entities or companies for data protection violations to 5% of the global revenue and not the local one: amend Article 20(a).**

10. **Grant the right to bring a case to the Unit for the affected data subject since it is the only unit mandated to conduct an investigation per the draft law: amend Article 20(b).**

11. **Remove the compulsory authorization to process data and replace it with the principle of accountability through adequate documentation and oversight: amend Articles 20 and 23.**

In addition to our recommendations, policymakers should consult our guide to comprehensive data protection legislation as they continue to debate the 2022 Data Protection bill in the Jordanian parliament. The guide was developed based on learnings from our work on the European Union General Data Protection Regulation and related global legal frameworks.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

This policy brief is an Access Now publication. It is written by Chérif El Kadhi and Marwa Fatafta. We would like to thank Access Now's Data Protection Lead, Estelle Massé, for providing support.

For more information, please contact:

Marwa Fatafta | MENA Policy and Advocacy Manager | marwa@accessnow.org
Chérif El Kadhi | MENA Policy Analyst | cherif@accessnow.org