

Jurisdiction	The Hashemite Kingdom of Jordan
Date	11 th of April 2022
Law Firm	Aljazy & Co . (Advocates and Legal Consultants)
Title, Name	Associate, Osama K. Khraisat
Contact Information	o.khraisat@aljazy.com

Questionnaire

I. Law concerning protection of personal information

- i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future?

Personal information protection in the private sector is not regulated in Jordan under a specific law at the present time. Jordan is taking serious steps to bring legislation aimed at the protection of personal data in the near future. There is a circulated draft of the Data Protection Law and the estimated time for it to be officially enacted is around 12-18 months from now as this law has not been presented to the Jordanian Parliament as of yet. The Data Protection law will be in force after 6 months of the Parliament's approval in accordance with the latest circulated draft.

As for now, all communications that may contain personal information are protected and private under article 18 of the Jordanian constitution which states that "All postal and telegraphic correspondence, telephonic communications, and other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law".

- ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future?

Personal information protection in the public sector is not regulated in Jordan under a specific law at the present time. Article 18 of the Jordanian Constitution in addition to the proposed Data Protection law are applicable to both private and public sector.

- iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.)

Yes.

The Financial and Banking sectors:

The Banking Law No. (28) of 2000 article 72 stipulates that "The bank must observe the complete confidentiality of all customers' accounts, deposits, trusts and safes with it, and it is prohibited to share any data about them directly or indirectly, except

with the written consent of the account holder, the depositor, the settlor of trust, or the user of treasury, or one of his heirs, or by a decision of a competent judicial authority in an existing judicial litigation or because of one of the cases permitted under the provisions of this law, and the ban remains in place even if the relationship between the customer and the bank ends for any reason”

The protection of personal information is also applicable on all financial services that banks and financial institutions provide, including money transfer and digital services.

The Telecommunications Sector:

The Telecommunications Law No. (13) of 1995 considers phone calls and private communications as private in accordance with Article 56: “telephone calls and private communications are considered confidential matters that may not be violated, under penalty of legal responsibility.”

The Cyberspace and Digital Communications sectors:

The Cybercrime Law No. (27) of 2015 indicates that unauthorized and unlawful access to websites or information systems to cancel, delete, add, destroy, disclose, damage, withhold, modify, change, transfer or copy data or information is a crime and punishable by law .

Where all of the answers to the question of I.(i), (ii) and (iii) is “no”, please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

- i. Please fill in the blanks below about all the law concerning personal information mentioned at I.. (please add a reply column as necessary,)

The title of the law : Data protection Law (still a draft and its provisions are subject to



Data Protection Law (Draft).pdf

change) Scanned Pdf file is available.

① The definition of “Personal Information”	Personal Information: Any data or information relating to a natural person that would identify him directly or indirectly, regardless of its source or form, including data relating to person identity, family status or whereabouts. Sensitive Personal Information: Any data or
--------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	information related to a natural person that directly or indirectly indicates his or her origin, race, opinions, political affiliations, religious beliefs, or any data related to his financial status, health, physical, mental or genetic condition, or his vital fingerprint. (Biometrics) or his criminal record, or any information or any data that the Council decides to consider sensitive, and of which the disclosure or misuse harms the person.
② The scope in which the law applies	A- The provisions of this law shall apply to all data, even if it was collected or processed prior to its entry into force. B - The provisions of this law do not apply to natural persons who process their data for their personal purposes.
③ The territorial scope	Jordan, and outside of Jordan if the data holder for the information is overseas.
④ URL	Not yet decided
⑤ The effective date	Not yet decided

The title of the law : The Banking Law No. (28) of 2000

<https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/2f75d7af-5465-4e1f-90dd-8b825037edbd.pdf>

① The definition of "Personal Information"	There is no definition of Personal Information
② The scope in which the law applies	The provisions of this law shall apply to all those who engage in the banking business
③ The territorial scope	Jordan
④ URL	https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/2f75d7af-5465-4e1f-90dd-8b825037edbd.pdf
⑤ The effective date	August 1 2000
⑥ Institutions subject to the law	All licensed financial institutions
⑦ Information subject to the law	The financial history of a person, or any personal information required to be disclosed to receive a service from a financial institution.

The title of the law : The Telecommunications Law No. (13) of 1995

<https://trc.gov.jo/EchoBusV3.0/SystemAssets/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA%20%D9%88%D8%AA%D8%B9%D8%AF%D9%8A%D9%84%D8%A7%D8%AA%D9%87.pdf>

① The definition of "Personal Information"	There is no definition of Personal Information
② The scope in which the law applies	This law is applicable to all Transmission, broadcast, reception, or transmission of symbols, signals, sounds, images, or data, of whatever nature, by wire, radio, or optical means, or by any other means of electronic systems.
③ The territorial scope	Jordan
④ URL	No official English translation is available.
⑤ The effective date	1/10/1995
⑥ Institutions subject to the law	Entities that hold a license to operate or manage a telecommunication network in Jordan.
⑦ Information subject to the law	information required to be disclosed to receive a service from a telecommunications provider, and Information subscribers share using a licensed telecommunication network.

The title of the law : The Cybercrime Law No. (27) of 2015

<http://www.mc.gov.jo/echobusv3.0/SystemAssets/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9%20%D8%B1%D9%82%D9%85%2027%20%D9%84%D8%B3%D9%86%D8%A9%202015.pdf>

① The definition of "Personal Information"	There is no definition of Personal Information
② The scope in which the law applies	This law is applicable to information systems and information networks, digital programs and websites.
③ The territorial scope	Jordan
④ URL	No official English translation is available.
⑤ The effective date	1/6/2015
⑥ Institutions subject to the law	Institutions that own or operate a website or an information network.
⑦ Information subject to the law	The information on a website or an information system of an institution.

ii. If there are any special instructions about the laws, please describe them.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your

country, please describe the outlines.

<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>

(a) Collection Limitation Principle

The draft of the Data Protection Law include the Collection Limitation Principle as per article 7(a) and 7(c) which states that purpose of processing the data must be legitimate, specific and clear and to be carried out by legal and legitimate means.

(b) Data Quality Principle

Article 7 (b) of the Law stipulates that the data processing shall be consistent with the purposes for which the data was collected. The data must be based on true, accurate and up-to-date data in accordance with article 7(d) of the Law.

(c) Purpose Specification Principle

Articles 9 (b) and 9(c) of the Law stipulate that the person must be informed about the purpose for which the data is processed and the period of time during which the data will be processed, provided that this period is not extended except with the consent of the person and in accordance with the provisions of the law.

(d) Use Limitation Principle

Article 4 (a) of the Law states the following: "Every natural person has the right to protect his data, and it may not be processed except after obtaining the prior consent of the concerned person or in the cases authorized by law."

(e) Security Safeguards Principle

Article 8(b) of the Law states that the entity responsible for the Data must take security, technical and organizational measures that ensure the protection of data from any breach of its security and integrity or any disclosure or any change, addition, destruction or unauthorized action

(f) Openness Principle

By virtue of the Law, a Data Protection Council shall be established and responsible for:

a- Approval of policies, strategies, plans and programs related to data protection

and monitor their implementation.

b- Adopting standards and measures for data protection, including codes of conduct related to the proper performance of the official and processor of its work.

c- Determining the mechanism for deciding on complaints and requests submitted by the person concerned against the official or by the responsible applicant against any other official and taking the necessary measures in this regard in accordance with instructions issued for this purpose.

d- Expressing an opinion on treaties, agreements, legislation and instructions related to data.

e- Issuing a periodically updated list of countries, international or regional bodies or organizations accredited to the Kingdom, which have an adequate level of data protection, and publishing it by any means it deems appropriate.

f- Suggesting international cooperation plans in the field of data protection and exchanging experiences with international bodies and organizations, coordinating and cooperating with governmental and non-governmental bodies and agencies to ensure the integrity of data protection procedures.

(g) Individual Participation Principle

Article 4 of the Law states that :

A- Every natural person has the right to protect his data, and it may not be processed except after obtaining the prior consent of the person concerned or in the cases authorized by law.

b- A person shall enjoy the following rights:

1- Knowing, accessing and obtaining the data held by the official.

2- Withdrawal of prior consent.

3- Correcting, modifying, erasing, hiding, adding or updating data.

4- Allocating treatment to a specific scope.

5- Object to processing and diagnosis if they are not necessary to achieve the purposes for which the data was collected, or if they are in excess of their requirements, discriminatory, unfair or in violation of the law.

6- Transferring a copy of his data from the official to another official.

7- Awareness and knowledge of any violation or breach of the security and integrity of his data.

C- The exercise of the rights stipulated in Paragraph (B) of this Article shall not entail any financial or contractual consequences for the person.

(h) Accountability Principle

In the event of a gross negligence or infringement, the data holder is obligated to compensate the person as per article 19 (b) of the Law.

- ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.
- iii. The below OECD Privacy Principles are included in the draft of the Data Protection Law. Currently, due to the absence of a legal frame work of such law the main data protection procedures and rules do not exist under Jordanian law. The matter of privacy is merely covered in the Jordanian Laws and regulations. The current laws broadly cover the general rule of protecting the personal information only with no specific procedures on how to process, store and protect personal information. Hence, these principles are not fully covered under the Jordanian laws at the present time.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If

yes, please describe them.

No. There is no system that has an impact on the rights of data subjects. Also, the right of privacy is protected under the Jordanian Constitution and generally the government does not access the personal data retained by private sector organizations. However, in accordance with the draft of the Data Protection Law, a public authority may process personal data without prior consent or notifying the person if the processing is carried out directly by a competent public authority to the extent required to carry out the tasks entrusted to it by law or through other contracted parties, provided that the contract (in case a governmental entity assigns its duties to another party to provide it services by signing a contract, then this contract must adhere to the provisions of the Data Protection Law.) includes observance of all obligations and conditions stipulated in this law and the regulations and instructions issued pursuant thereto.

As for Data Localization the Ministry of Digital Economy & Entrepreneurship issued Cloud (Platforms & Services) Policy 2020. In this Policy, the private entity may store their information outside of Jordan and must ensure that the data is protected. The cloud service provider is also obligated to protect the data from unauthorized access. Governmental entities in accordance with the Policy must classify their assets which include data, equipment, and software that will be transferred to cloud.

The first level (**Secret**): then the place of preservation and processing is limited within the Kingdom to the secure data centers in the government with the possibility of restrictions, and the authority can benefit from all the cloud services. • The second level (**Sensitive**): The place of preservation and processing is limited within the Kingdom, with the possibility of utilizing the secure data centers in the government with all different cloud services, and the secure data centers in the private sector with the possibility of restrictions. Thus, Government entities can take advantage of SaaS cloud services only.

The third level (**Private**): The place of preservation and processing can be inside or outside the Kingdom, with the possibility of taking advantage of secure data centers in the government and the private sector with all the different cloud services, with the possibility of restrictions on data centers in the private sector and / or outside of Jordan.

The fourth level (**Ordinary**): The place of preservation and processing can be inside or outside the Kingdom, with the possibility of benefiting from the secure data centers in the government and the private sector, and all different cloud services

can be used. Additional restrictions in the above classification such as encryption, tokenization, anonymization, data decomposition, and implementing cyber deception defense solutions shall ensure that data is not seen, accessed and replicated in the cloud by local or global cloud service providers.

Cloud (Platforms & Services) Policy 2020

https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/cloudpolicy-2020-english.pdf

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Currently there is no data protection authority in Jordan. However, in accordance with the draft of the Data Protection Law the relevant authority is the Ministry of Digital Economy And Entrepreneurship.

Address: 8th Circle Bayader Wadi Al Seer P.O.Box 9903 Amman 11191 Jordan