DATA PROTECTION LAWS OF THE WORLD

Jordan

JORDAN

Last modified 11 January 2024

LAW

Personal data protection is regulated in Jordan under the Law of Personal Data Protection No. (24) of the Year 2023 (the “Law”). Jordan took a serious steps to enact this legislation aimed at the protection of personal data. The Data Protection law was published in the Official Gazette no. 5881 page 4338 on 17 September 2023.

Details on the law

Within this Law, numerous restrictions are placed on the processing of personal data, the most important and notable one being the requirement for prior consent being “explicit and documented in writing or electronically, it should also be specific in terms of duration and purpose.” The Law also stipulates that citizens should be informed in advance of their data’s date and reasons for collection. It also criminalizes the processing of data for reasons other than the purpose intended.

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”. Additionally, Article (7) states that personal freedom shall be protected, and that any infringement of the rights and public freedoms or sanctity of private life of Jordanians is a crime punishable by law.

Personal information protection in the public sector is regulated in Jordan under a specific law. Article 18 of the Jordanian Constitution in addition to the Data Protection law are applicable to both private and public sector.

The right of privacy is protected under the Jordanian Constitution and Law of Personal Data Protection. In accordance with 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). This includes observance of all obligations and conditions stipulated in this law and the regulations and instructions issued pursuant thereto.

Article (6) of the same provides for exceptions to the requirement of prior consent, as follows:

1. Processing carried out directly by a competent Public entity to the extent required to carry out the tasks entrusted to it in accordance with the provisions of the legislation in force or through other contracting parties provided that the contract includes compliance with all obligations and conditions stipulated in this Law and the regulations and instructions issued pursuant thereto.
2. If necessary to preventine medical purpose medical diagnosis or provision of health care by a licensee licensed to practice any of the medical professions.

3. If necessary to protect the life of the concerned person or his vital interests.
4. If necessary for the prevention of a crime or for its detection by a competent authority for the prosecution of crimes committed in violation of the provisions of the Law.
5. If required or authorized by virtue of any legislation or in implementation thereof or by virtue of a decision of the competent court.
6. If required for the purposes of the entities subject to the control and supervision of the Central Bank of Jordan to carry out their activities as determined by the Central Bank of Jordan including the transfer and exchange of data inside or outside the Kingdom.
7. The treatment carried out in accordance with the provisions of the Regulations issued pursuant to the provisions of this Law.
8. If necessary for the purposes of scientific or historical research if they are not intended to take any decision or action with respect to a specific person.
9. If necessary for statistical purposes or national security requirements or achieve the public interest.
10. If the subject of the processing is publicly available data from the Person concerned.

Article (15) of the law, relating to the cross-border transfer of personal data outside of the Hashemite Kingdom of Jordan, states that:

1. Regional or international judicial cooperation under international conventions or treaties in force in the Kingdom.
2. Regional or international cooperation between the Kingdom and international or regional bodies, organizations or agencies working in the field of combating crime of all kinds or prosecuting the perpetrators.
3. Exchange of personal medical data of the person concerned with processing when necessary for processing and exchange of data related to epidemics or health disasters or what affects public health in the Kingdom.
4. Exchange of data related to epidemics or health disasters or what affects public health in the Kingdom.
5. Transfer my occur if the concerned individual provides explicit consent after being informed that an adequate level of protection is unavailable.
6. Transactions involving banking operations and money transfers outside the Kingdom.

Before initiating the Data transfer, the Official is obligated to verify the level of protection guaranteed by the Recipient outside the Kingdom, ensuring the safety and security of the Data.

Article (7) of the Law, carries on specifying the Special conditions for the processing (which includes transferring or sharing) of personal datalt is prohibited to process personal data without the consent (standard of consent is set out above).

It is impermissible to conduct processing of personal data for anyone whom is incapacitated, without the prior written or electronic consent of one of his parents, and in the absence of a parent for any reason, the consent of the legally appointed guardian is taken to follow up on his affairs.

As for the processing of sensitive personal data, the following conditions apply: As per Article (6) of the Law, It is prohibited to process sensitive personal data without the prior approval of the concerned person, except in the following cases:

1. Processing carried out directly by a competent Public entity to the extent required to carry out the tasks entrusted to it in accordance with the provisions of the legislation in force or through other contracting parties provided that the contract includes compliance with all obligations and conditions stipulated in this Law and the regulations and instructions issued pursuant thereto.
2. If necessary to preventine medical purpose medical diagnosis or provision of health care by a licensee licensed to practice any of the medical professions.
3. If necessary to protect the life of the concerned person or his vital interests.
4. If necessary for the prevention of a crime or for its detection by a competent authority for the prosecution of crimes committed in violation of the provisions of the Law.
5. If required or authorized by virtue of any legislation or in implementation thereof or by virtue of a decision of the competent court.

6. If required for the purposes of the entities subject to the control and supervision of the Central Bank of Jordan to carry out their activities as determined by the Central Bank of Jordan including the transfer and exchange of data inside or outside the Kingdom.
7. The treatment carried out in accordance with the provisions of the Regulations issued pursuant to the provisions of this Law.
8. If necessary for the purposes of scientific or historical research if they are not intended to take any decision or action with respect to a specific person.
9. If necessary for statistical purposes or national security requirements or achieve the public interest.
10. If the subject of the processing is publicly available data from the Person concerned.

The protection officer, personal data processor and recipient of personal data are committed to ensuring the integrity and security of personal data and tracking cases of abuse of personal data security. The personal data must be handled and processed in such a way that ensures confidentiality, safety, and non-modification.

DEFINITIONS

Definition of Personal Data

There is no specific definition in the laws or the regulations.

Definition of Sensitive Personal Data

There is no specific definition in the laws or the regulations.

NATIONAL DATA PROTECTION AUTHORITY

Not applicable.

REGISTRATION

No registration required.

DATA PROTECTION OFFICERS

Not applicable at present, but see details on the draft law.

COLLECTION & PROCESSING

The legislations in Jordan are silent in this regard, however see details on the draft law.

TRANSFER

The Cybercrime Law No. (27) of 2015 (‘**Cybercrime Law**’) generally acts to criminalise unlawful access to websites or information systems such as access without authorisation, permission or in a manner that breaches the said authorisation or permission.

Anyone who intentionally enters a computer network or an information system by any means without authorisation, or in violation of or exceeding the authorisation, shall be punished by imprisonment for a period of no less than a week and not exceeding three months, or by a fine of no less than (100) one hundred dinars and not more than (200) two hundred dinars, or both of these penalties.

If the entry stipulated above is accompanied with the intention to cancel, delete, add, destroy, disclose, damage, withhold, modify, change, transfer or copy data or information, or stop or disrupt the work of the information network or the information network information system, then the offender shall be imprisoned for a period of not less than three months and not exceeding one year and a fine of no less than (200) two hundred dinars and not more than (1,000) one thousand dinars.

SECURITY

Anyone who intentionally enters the information network or information system by any means without permission, or in violation of or exceeding authorisation with the aim of accessing data or information not available to the public and that affects national security, foreign relations of the Kingdom, public safety or the national economy shall be punished with imprisonment for a period of no less than four months and a fine of no less than (500) five hundred dinars and not more than (5000) five thousand dinars.

If the entry referred to above is accompanied with the intention of cancelling, destroying, modifying, changing, transferring, copying or disclosing such data or information, the perpetrator shall be punished with temporary labour and a fine of no less than (1,000) thousand dinars and not more than (5000) five thousand dinars.

Anyone who intentionally accesses a website to view data on information not available to the public that affects national security, the Kingdom’s foreign relations, public safety, or the national economy shall be punished by imprisonment for a period of no less than four months and a fine of no less than (500) five hundred dinars.

If the entry referred to in the paragraph directly above is accompanied with the intention to cancel, destroy, modify, change, move or copy such data or information, the perpetrator shall be punished with temporary labour and a fine of no less than (1,000) one thousand dinars and not more than (5,000) five Thousands of dinars.

BREACH NOTIFICATION

In the relation to the Cybercrimes, the injured party shall have the right to submit a complaint before the Cybercrime Unit and the latter shall review the complaint and transfer it to the court.

Mandatory breach notification

It is stated in the aforementioned draft Personal Data Protection law, under Article (6), that a unit will be established within the Ministry of Digital Economy and Entrepreneurship, which will be responsible for preparing a regulation that controls the process of receiving notifications and complaints regarding any violations that may affect personal data.

The second law is “Cyber Security Law No. 16 of 2019” as it has established a National Center for Cyber Security, which receives complaints and reports related to cyber security and cyber security incidents. The law opened the door for further collaboration with different official entities according to its sphere of specialty.

The Cybersecurity Framework for Jordan Financial Sector – V. 1 – July, 2021, states that organizational-level severity rating is performed by the entity to define the point at which the incident should be treated as a disaster, in addition to determine escalation procedures, as well as human resources and time durations to recover. The entity has to notify the Central Bank of Jordan / Financial Cyber Emergency Response Team about the incident according to the following timelines:

- Initial notification within 2 hours from confirming time.
- After the closure of the incident for “Low” incidents.
- Within 8 hours from confirming the incident and one time every two business days for “Medium” incidents.
- Within 4 hours from confirming the incident and once a day for “High” incidents.

Additionally, Article (49) of the Instructions for Handling Cyber Risks No. (26/1/1/1984) for the Year 2018 stipulates that *“ the company shall notify the Central Bank in the event of discovering that it has been exposed to any cyber incident or any attempt of cyber-attack characterised by a high degree of danger to its systems or networks, no later than 72 hours from the moment of discovery of the cyber-event and according to the mechanism that will be adopted by the Central Bank, and inform the relevant security services of any case of embezzlement, forgery, theft or fraud resulting from the cyber event as soon as it is discovered and in accordance with the relevant laws and instructions.”*

ENFORCEMENT

The Cybercrime Unit is the body responsible to deal with any complaints and to assign it to the court.

In general, the court shall enforce the sanctions that are stated in the Cybercrime Law, and any other applicable laws and regulations.

ELECTRONIC MARKETING

The e-Procurement Instructions of 2018 mandates the use of JONEPS (Jordan Online E-Procurement System) in the implementation of public procurement.

The user of the system means the government entity, government unit, or interested party that submitted an application for registration on the electronic system and was approved by the electronic system manager.

The instructions explicitly state that the user of the system shall maintain the confidentiality of the information available in the system and take all necessary precautions and measures that would prevent the leakage of any information to any person, including the following:

- Prevent the disclosure of information to persons who are not authorised to view or disclose it, and apply the highest levels of privacy, confidentiality, security and transparency of information.
- Maintaining the security and integrity of data from alteration or modification by any party that does not have the authority to do so.

Additionally, the tenderer shall provide security controls to protect the system and devices, such as using anti-virus programs, using strong and modern programs and programs to detect intrusions from people or programs, and constantly updating information security programs.

Finally, the user of the system must use the system in a safe and sound manner, and it bears responsibility for any wrong use by it or by its users.

ONLINE PRIVACY

The legislations in Jordan are silent in this regard.

KEY CONTACTS

Aljazy& Co.
www.aljazylaw.com/

Omar M.H. Aljazy
Managing Partner
Aljazy& Co.
T + (962 6) 5654477
oaljazy@aljazylaw.com

Sewar Smierat
Head of Corporate Department
Aljazy& Co.
T + (962 6) 5654477
ssmierat@aljazylaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.