DATA PROTECTION LAWS OF THE WORLD

Jordan

DLA PIPER

Downloaded: 7 December 2022

JORDAN

Last modified 16 February 2022

LAW

Jordan currently does not have a comprehensive data protection law in force.

As of yet, Data Protection is not regulated in Jordan under a specific law. However, the Personal Data Protection law No. (__) for the Year 2020 is still a draft at the Legislation and Opinion Bureau.

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.

COLLECTION & PROCESSING

The legislations in Jordan are silent in this regard.

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.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.