Jurisdiction	*The state of Libya*
Date	*18/09/2022*
Law Firm	*Zahaf & Partners Law Firm*
Name and Position of the person in charge	*Dr. Saleh Zahaf – Partner* *Mahmud Zahaf - Partner*
Contact Information	*Tel: 00218 21 3334636 | 00218 21 3345761 | Fax: 00218 21 3343515* *Email: mahmud.zahaf@zahaflaw.com* *Email: Saleh@zahaflaw.com*

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

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?

There is no comprehensive statute. Although the Libyan Parliament enacted the the Electronic Transactions Law in 2021, this law has not been published or made available to public. The provisions of this law remain unknown to this date.

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?

National Information Security and Safety Policies.

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.)

Libya does not have a law specifically addressing protection of personal information which apply in individual (specific) sectors.

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 ： National Information Security and Safety Policies

① The definition of "Personal Information"	Although "Personal Information" is not defined, it is described as personally identifiable information, *such as social security or National ID numbers, passport numbers, credit card numbers, driver's license numbers, and medical records.*
② The scope in which the law applies	*This policy is binding to the work of all ministries, public sectors, government departments and their affiliated entities*
③ The territorial scope	*The policy is enforced on a local and global scale.*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*https://nissa.gov.ly/wp-content/uploads/NISSA_Policy_Manual_v1.0-1.pdf*
⑤ The **effective** date *	*This information is not available*

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：

① The definition of "Personal Information"	
② The scope in which the law applies	
③ The territorial scope	
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	
⑤ The **effective** date*	

* If the law has been amended, please fill in the effective date of the amended law.

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/oecdguidelinesontheprotectionofprivacyandtran

sborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

The relevant provision is inapplicable.

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

The relevant provision is inapplicable.

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

The relevant provision is inapplicable.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (c) Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

Partially stipulated in the National Information Security and Safety Policies under:

- Data Protection Policy section 2 titled Information Protection Policy

paragraph 2.4.3 titled Disclosure of Information.

- Data Protection Policy section 4 titled Information Dissemination Policy.

- Data Protection Policy section 5 titled Access to Information Policy.

- Under these stipulations, the Policy restricts sharing personal information to those who are granted permission by management. Additionally, under this Policy, where personal information is shared/disclosed, it should only be done so in accordance with a documented Information Sharing Protocol or a Data Exchange Agreement.

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Stipulated in the National Information Security and Safety Policies under the Network Security Policy.

This Policy instructs public entities on the procedures and protection which they must apply to protect any personal information which they obtain.

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

The relevant provision is inapplicable.

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

The relevant provision is inapplicable.

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.

The relevant provision is inapplicable.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(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 (e.g., limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the attorney-client privilege)** to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

There is no system for data localization, but for government access, the following regulations exist:

Libyan Banking Law No 1 of 2005 Article 116

Employees of the Central Bank of Libya so designated as investigation officers with respect to crimes that occur in violation of the provisions of the law and regulations and decrees issued pursuant to it may examine records, debit accounts, other documents and records, and electronic systems.

https://www.almontaser.com/Laws/Law%20No.%20(1)%202005%20regarding%20banks.pdf

Law No 2 of 2005 (on Anti Money Laundering) Article 14

All entities getting information or data in accordance with the provisions of this law must maintain their confidentiality and not to disclose them unless necessary for use in investigations, prosecutions and cases concerning money laundering crime and other crimes stipulated.

https://security-legislation.ly/en/law/31549

Libyan Penal Code - Article 469

Whoever, without a legitimate excuse, refuses to provide assistance or to do what a public official asks of him during the performance of his duties in the event of a disturbance or any other disaster or in flagrante delicto, or refrains from providing the information or data required of him in the aforementioned cases, shall be punished with detention for a period not exceeding one month or a fine.

https://security-legislation.ly/sites/default/files/lois/290-Penal%20Code_EN.pdf

Communications Law No 22 of 2010 - Article 15
Entities providing communication services must take all steps to ensure the confidentiality of the beneficiaries' communications, and the entities may not that provide services intercept, monitor, change or modify the communications of service beneficiaries.
For the purposes of following up, locating or responding to harassment, aggressive or illegal calls, or as the law permits the following:

a. The beneficiary may request the service provider to monitor calls related to his phone.

b. The legally competent judicial authority may issue its instructions to the entity that provides services to intercept or monitor incoming or outgoing calls to the individual's phone, and it must abide by those instructions.
The service provider must provide this body with information derived from its monitoring of the individual's phone, including the phone numbers called and the dates of their occurrence.

c. The competent authority may take any action to protect people from harassing, hostile or illegal calls, and refer the matter to the competent authorities to take the necessary measures.

https://security-legislation.ly/en/law/34009#:~:text=No%20telecommunications%20networks%20may%20be,and%20the%20implementing%20regulations%20thereof.

Anti-Cybercrime Law No. 5 of 2022 - Article 7

The National Authority for Security and Information Safety may monitor what is published and displayed through the international information network or any other technical system, and block everything that spreads prejudices or ideas that would destabilize the security and stability of society or prejudice its social peace. E-mails or conversations may not be monitored except by a judicial order issued by the Competent District Judge.

Article (18)

Anyone who illegally obtains identification and identification tools belonging to another person which is used in an information system shall be punished by imprisonment and a fine of no less than 1,000 thousand dinars and not more than 3,000 three thousand dinars.
Anyone who knowingly and illegally uses identification and identification tools belonging to another person in an information system shall be punished by imprisonment for a period of no less than one year and a fine of no less than 1,000 thousand dinars and not more than 10,000 ten thousand dinars.

https://lawsociety.ly/legislation/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-5-%D9%84%D8%B3%D9%86%D8%A9-2022-%D9%85-%D8%A8%D8%B4%D8%A3%D9%86-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7/
Available only in Arabic.

V. The Data Protection Authority

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

Name: The National Information Security & Safety Authority
Address: V5FR+33W, Sharia al-Jala'a, Tripoli
Telephone: +218 21 361 41 15
Website: https://nissa.gov.ly/

Other information if any: