



TOWARDS A MODERN PERSONAL DATA PROTECTION LAW IN LEBANON

February 2024

Prepared
by



With the
support of



THE SAMIR KASSIR FOUNDATION

SIGRID RAUSING TRUST

TABLE OF CONTENTS

INTRODUCTION	3
SECTION ONE - COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS	6
SECTION TWO - PROPOSED COMPREHENSIVE INDEX FOR PERSONAL DATA PROTECTION LAW	21
CONCLUSION	29
ANNEXES	30

INTRODUCTION

The ongoing debate regarding privacy and personal data protection is intensifying, driven by potential violations on both privacy rights and personal data protection in the rapidly advancing technological landscape of the current digital age.

The distinction between the right to privacy and the right to personal data protection is crucial, although they are often intertwined. Privacy concerns an individual's control over the accessibility and use of their information by others, while personal data protection involves implementing tools and policies to secure and safeguard such data from unauthorized access, loss, tampering, or misuse by those processing it.

Recognizing the paramount importance of upholding these rights, it has become imperative to counter their violation through the enactment of laws that strengthen their protection. Numerous countries have taken significant steps in this direction, with the European Union notably passing the General Data Protection Regulation (GDPR) on April 14, 2016, and implementing it as of May 25, 2018.

The significance of personal data protection law is underscored by the principle of "individual autonomy," emphasizing an individual's independence in decision-making regarding their personal life. This principle ensures that individuals retain control over their personal information and protects against arbitrary or illegal intrusions into their privacy without informed consent. Informed consent entails the right to understand why personal data is being collected, the purpose behind its collection, and the consequences of sharing this data with other parties.

Responsibility for safeguarding personal data against leaks or harm lies with those processing the data, aligning with the principle of protecting the right to privacy and private life. This protection extends beyond initial consent, granting individuals the right to object to processing and revoke their consent.

The principle of "individual autonomy" extends beyond privacy and personal data protection to encompass a range of democratic values, including freedom of opinion, expression, and assembly.

In addition to safeguarding these rights and values, personal data protection laws also counter cyber threats stemming from digital transactions and global network interconnectivity. These laws set procedures to protect against fraudulent activities, unauthorized access to personal information, and data breaches, strengthening digital infrastructure and defenses.

Furthermore, this law serves to highlight the efforts exerted by the state and its institutions to adhere to best standards in this field, fostering trust between the state and society, especially personal data subjects. Moreover, it enhances the state's credibility in its interactions with the international community, attracting foreign investments, stimulating economic growth, and strengthening diplomatic relations. These elements pave the path for international collaboration in an interconnected world facilitated by globalization, communication networks, and the internet.

The absence of a dedicated personal data protection law in Lebanon underscores the urgent need for comprehensive legislation aligned with international standards, particularly the GDPR. By comparing the GDPR with laws in Oman, Qatar, and Tunisia, this report aims to identify effective practices and rectify shortcomings within Lebanon's legal framework. Notable examples include Tunisia's Law No. 63 on the Protection of Personal Data, Qatar's Law No. 13 on the Protection of Personal Data, and Oman's Sultani Decree No. 6/2022 on the Protection of Personal Data.

The Lebanese Parliament has yet to pass a law specifically dedicated to addressing the protection of personal data. Instead, such protection is regulated within Law No. 81, "Electronic Transactions and Personal Data," enacted on October 10, 2018. However, the provisions pertaining to this protection are outdated and prove ineffective in ensuring the safeguarding of private data for the moment. Moreover, they fall short of fully considering this law's core principle which is "individual autonomy," as the current legislation does not explicitly mandate obtaining the data subjects' consent for the processing of their data. Therefore, there is an urgent need for the enactment of a comprehensive law solely focused on protecting personal data, one that protects data from any breaches, in accordance with this principle and international best standards in this field.

The Lebanese Parliament has yet to pass a law specifically dedicated to addressing the protection of personal data. Instead, such protection is regulated within Law No. 81, "Electronic Transactions and Personal Data Protection," enacted on October 10, 2018. However, the provisions pertaining to this protection are outdated and prove ineffective in ensuring the safeguarding of private data at present. Moreover, they fall short of fully considering this law's core principle of "individual autonomy" since the current legislation does not explicitly mandate obtaining data subjects' consent for the processing of their data. Therefore, there is an urgent need for the enactment of a comprehensive law solely focused on protecting personal data, one that safeguards data from any breaches, in accordance with this principle and international best standards in this field.

This report aims to establish a comprehensive index of a much needed personal data protection law in Lebanon, drawing heavily from the General Data Protection Regulation (GDPR) issued by the European Union. Effective since May 25, 2018, this regulation stands out as one of the most important legislations safeguarding personal data, given its extensive scope, procedures, and mechanisms imposed on data processors, in addition to its focus on the rights of data subjects. The regulation also emphasizes the importance of privacy, accountability, and transparency and imposes severe sanctions on violators. Furthermore, it has contributed, both within and beyond the

EU, to disseminating the culture of personal data protection within institutions and raising awareness among individuals about their rights in this domain.

The GDPR set forth by the European Union was compared with the laws of Lebanon, the Sultanate of Oman, Qatar, and Tunisia. The aim is to discern the diverse approaches taken by these countries in protecting personal data, adopting the most effective practices in this field, and rectifying the loopholes and shortcomings within the Lebanese legal system. The Tunisian Law No. 63 on the Protection of Personal Data, issued on July 27, 2004, was selected because the rights to privacy and the protection of personal data are enshrined in the Tunisian Constitution.¹ Qatar was chosen for its pioneering role as the first Gulf Cooperation Council member state to adopt dedicated legislation for personal data protection,² as embodied in Law No. 13 on the Protection of Personal Data, issued on November 3, 2016. Additionally, the Sultanate of Oman's Sultani Decree No. 6/2022 on the Protection of Personal Data, issued on February 9, 2022, was selected because it is relatively recent compared to other legislations in the region.

Based on the study of aforementioned laws and their comparison with the GDPR issued by the EU, we have strived to set the best standards that Lebanon's personal data protection law must align with, should there be a political will to enact such a law. This report comprises two main sections:

Section one – Comparing EU General Data Protection Regulation with Data Protection Laws in Lebanon, the Sultanate of Oman, Qatar, and Tunisia.

Section two – Suggesting a Comprehensive Index for the Provisions Relating to Personal Data Protection Law in Lebanon.

1 Data Protection Laws of the World, Tunisia, DLA PIPER, <https://www.dlapiperdataprotection.com/index.html?t=law&c=TN&c2=>

2 Data Protection Laws of the World, Qatar, DLA PIPER, <https://www.dlapiperdataprotection.com/index.html?t=law&c=QA>

SECTION ONE - COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS

In this section of the report, we will showcase the procedures protecting personal data and the best related practices. These measures have been selected after examining the personal data protection laws in Lebanon, the European Union, the Sultanate of Oman, Qatar, and Tunisia, along with the comparison and analysis of these laws' common provisions.

1 - DEFINITION OF TERMS IN LAW

The laws in Lebanon, Oman, Qatar, Tunisia, and the EU have defined the concept of "personal data." These jurisdictions agree that such data refers to information allowing the identification of a natural person. The EU and Oman elaborated on this definition, citing examples such as name, identification number, location data, electronic identifiers, or other specific individual factors like genetic, physical, mental, psychological, social, cultural, or economic identity.

Additionally, these laws define terms such as "personal data processing," "responsible for personal data processing," "controller," or "supervisor," with each country adding additional terms aligned with its relevant legal framework. For example, Lebanon's Law defines the term "recipient of personal data" in Article 1. Similarly, the GDPR outlines terms like "restriction of processing," "processor," "third party," "consent," "personal data breach," "representative," "establishment," "monitoring authority," and "international organization." Oman's law adds terms such as "genetic data," "biometric data," and "health data," while Qatar's law includes terms like "legitimate purpose," "acceptable practices," "direct marketing," and "website operator." Tunisia's law includes definitions like "referral" and "beneficiary" in Article 1.

Terminology regarding personal data protection laws varies among countries, emphasizing **the need for clear, detailed, and accurate definitions within the legal framework to prevent confusion or misuse**. The GDPR is widely recognized for providing the most detailed and clear definitions of these terms.

2 - UPHOLDING THE RIGHT TO PERSONAL DATA PROTECTION

Lebanese law falls short in upholding the right to personal data protection whereas the GDPR firmly did so in Article 1, paragraph two, stating: "This regulation safeguards fundamental rights and freedoms of natural persons, particularly the right to personal data protection." Similarly, this right has been enshrined in Qatar's law, Article 3: "Every individual has the right to safeguard the privacy of their personal data." Likewise, Tunisian law, in Article 1, guarantees: "Every person holds the right to protect personal data concerning their private life as a fundamental right guaranteed by the Constitution." However, the Sultanate of Oman's law, while stipulating in Article 3 that "personal data is protected under the provisions of this law," refrains from using the term "right."

Upholding the right to personal data protection is crucial as it protects individuals' privacy, independence, and dignity from potential breaches of their personal data. This principle aligns with the Lebanese Constitution, which recognizes international treaties protecting privacy rights and ensuring personal data protection.

3 - SCOPE OF LAW APPLICATION AND EXCEPTIONS

Scope of Law Application:

The provisions of laws in Lebanon (Article 85), the Sultanate of Oman (Article 2), Qatar (Article 2), Tunisia (Article 2), and the GDPR (Article 2, paragraph 1) encompass automated and non-automated data processing, including manual processes. This inclusive legislation guarantees the protection of all data, irrespective of the processing method employed.

Additionally, the GDPR extends its scope to include data processing concerning individuals within the EU, regardless of their nationality or residency status. The regulation also applies to institutions processing data outside the EU under certain conditions, such as offering goods or services to EU individuals or targeting the EU market. This extended scope ensures comprehensive protection even if data storage is outside the EU (Article 3).

Defining the scope of the law thoroughly and accurately, as demonstrated by the GDPR, **ensures the safeguarding of personal data for both citizens and residents, irrespective of the nationality of the data processor or the location of data storage.**

Exceptions:

The laws in Lebanon (Article 85), Oman (Article 3), Qatar (Article 2), Tunisia (Article 3), and the GDPR (Paragraph 2 of Article 2 and Paragraph 5 of Article 30) each exclude certain processing activities from their protective scope. All countries agree on excluding processing related to personal or familial activities for personal purposes, given their non-commercial nature and minimal risk to privacy rights.

Notably, the law of Oman stands out for its extensive exceptions outlined in Article 3, which exclude various processing activities from legal protection. These encompass processing conducted by state entities to enforce legal authorities, protect economic interests, ensure national security or public interest, or fulfill legal obligations mandated by law, verdict, or court ruling.

4 - PRINCIPLES OF DATA PROCESSING

The lawful processing of personal data must adhere to specific principles outlined in the law. The GDPR, in Article 5, delineates seven fundamental principles for processing personal data:

- **Lawfulness, fairness, and transparency:** Ensuring lawful and transparent data processing.
- **Purpose specification:** Clearly defining the legitimate and explicitly determined purpose of processing at the time of data collection.
- **Data minimization:** Collecting only necessary data and processing it solely for specified purposes.
- **Accuracy:** Maintaining data accuracy and updating it in a timely manner.
- **Storage limitation:** Storing personal data for the **necessary duration** to achieve the specified purpose.
- **Integrity and confidentiality:** Processing data safely, and ensuring confidentiality and appropriate security measures such as encryption.
- **Accountability:** Holding data processors accountable for compliance with personal data protection laws.

Other laws, such as those of Oman, Qatar, and Tunisia, incorporate most of these principles to varying degrees. **Lebanese law includes all principles outlined in the GDPR except for the principle of integrity, which does not mandate notifying data subjects of data breaches or violations and the corresponding actions taken. This gap underscores the need for specific legislation in Lebanon to protect personal data comprehensively.**

5 - DATA NOT TO BE PROCESSED

Personal data protection laws may prohibit processing sensitive data that could harm individuals. However, all laws under review include exceptions to this prohibition.

In Lebanon, Article 91 prohibits processing personal data revealing health status, genetic identity, or sexual life unless explicitly consented, legally required, or necessary for medical diagnosis or treatment, or to assert rights before courts.

Similarly, Oman and Qatar's laws prohibit processing a child's personal data without guardian consent, except in the child's best interest. Tunisia's law prohibits processing certain sensitive data unless consented, publicly available, necessary for historical/scientific purposes, or vital for the data subject's interests.

The GDPR unequivocally bans processing data revealing racial or ethnic origin, political opinions, religious beliefs, genetic/biometric data, health information, or sexual orientation, with exceptions for specific purposes outlined in Article 9. Key exceptions outlined in the GDPR include explicit consent of the concerned person for processing, necessary processing to protect the vital interests of data subjects or another natural person when data subjects are physically or legally unable to provide consent, processing related to non-profit organizations or data publicly disclosed by the data subjects, necessary processing for establishing, exercising, or defending legal rights, necessary processing for reasons of interest to public opinion, preventive or occupational medical objectives, assessing employee capacity to work, medical diagnosis, provision of health, social care, or treatment, management of healthcare systems and services, archival purposes in the public interest, or for scientific, historical, or statistical research purposes (Article 9).

When exceptions are granted to the prohibition on processing specific data, Lebanese law must ensure that these exceptions adhere to the principle of proportionality and respect the rights to personal data protection, privacy, and data subjects' interests.

6 - PERSONAL DATA SUBJECTS' CONSENT TO THE PROCESSING OF THEIR PERSONAL DATA

Lebanese law did not explicitly stipulate the data subjects' right to provide explicit and independent consent for the processing of their data. Instead, this matter is addressed in Article 91 of the law, which allows for the collection or processing of personal data revealing the health situation, genetic identity, or sexual life of the individual concerned, provided that explicit consent from the latter is obtained for such processing.

While other laws prohibit processing personal data without the data subjects' consent, exceptions have been introduced to this principle, acknowledging that certain interests or circumstances may justify data processing without obtaining explicit consent from the data subjects. The GDPR excludes from the consent requirement the processing of activities that are necessary for the preparation or execution of a contract involving the data subjects, fulfilling a legal obligation, saving someone's life, performing tasks in the public interest or official duties, or when the data processor has a legitimate interest in processing personal data of a particular individual (Article 6).

As for Tunisian law, exceptions to the consent requirement encompass processing activities that clearly benefit the data subjects but contacting them is impossible, or obtaining their consent requires significant efforts, as well as those mandated by law or agreements in which data subjects are a party (Article 28). In Qatari law, several exceptions are outlined to the consent requirement for data processing. These include situations where processing is necessary to fulfill a legitimate purpose for a third party to whom the data is transmitted (Article 14), if the processing aims to protect national security and public order, safeguard the state's international relations, economic or financial interests. Furthermore, exceptions apply when processing is essential to prevent any criminal offense, gather information about it, or investigate it (Article 18). Additionally, exceptions arise when processing is conducted to carry out missions related to the public interest in conformity with the law, fulfill a legal obligation or an order from a competent court, protect vital interests of individuals, pursue scientific research for the public good, and gather necessary information for investigating a criminal offense (Article 19).

The commitment to enshrining the data subjects' right to consent to the processing of their personal data is based on the principle of "individual autonomy" and serves as a cornerstone for upholding their right to privacy and control over their personal data. Moreover, this consent fosters transparency and accountability by requiring explicit consent from data processors before any processing takes place, thereby nurturing trust between data subjects and those responsible for data processing. As for exceptions to consent, they may be justified in specific circumstances, but they must be necessary and proportionate, as they curtail a fundamental right: the right to privacy and individual control over personal data.

7 - PROPERTIES OF CONSENT

Defining the properties of consent within the legal framework serves to delineate the boundaries of personal data usage and processing, ensuring data subjects are aware of their right to control such usage and safeguard their privacy.

While Tunisian law and the GDPR outline the properties of consent expressed by data subjects for data processing, Lebanese and Qatari laws do not. Tunisian law mandates that consent be explicit and written, without any conditions tied to providing a service or benefit in exchange for another

person's benefit (Article 17). Conversely, the GDPR elaborates on the conditions of consent, stipulating that it must be:

- **Freely given** consent
- **Specific**
- **Informed**
- **Clear** and unambiguous (Article 4, paragraph 11)
- **Documented** by the person responsible for the processing (Paragraph 1 of Article 7).

Lebanese law should clearly delineate the properties of this consent and the importance of documenting it, as stipulated in the GDPR.

Children's Consent for the Processing of their Data:

Tunisian law, the GDPR, and Qatari law outline provisions for obtaining children's consent to the processing of their data. Paragraph 1 of Article 8 of the GDPR stipulates the possibility for children under the age of 16 to express consent provided they have parental permission. Under Tunisian law, Article 28 specifies that processing personal data relating to a child is contingent upon obtaining consent from their guardian (parents) and permission from the family court judge. Similarly, Qatari law addresses children's consent to the processing of their data in Article 17, which prohibits it by owners or operators of any website targeting children unless explicit consent is obtained from the child's guardian (parents) via electronic communication or other suitable means.

Lebanese law must clearly stipulate parental consent for the processing of data pertaining to children under the age of 16, as outlined in the GDPR.

Revoking Consent:

The laws in Oman and Qatar, as well as the GDPR, stipulate the right of individuals to revoke their previous consent to data processing. Tunisian law specifies that consent for data processing cannot be applied in a particular way or for a specific purpose to other ways or purposes, as outlined in Article 30. However, Lebanese law lacks all the aforementioned. Therefore, **Lebanese legislation should explicitly acknowledge individuals' right to revoke consent at any time.**

8 - CONSENT FOR UTILIZING PERSONAL DATA FOR MARKETING PURPOSE

In Oman, Qatar, and Tunisia, laws require obtaining prior consent from data subjects before sending any advertising or marketing material for commercial purposes. Additionally, Qatari law stipulates the right for individuals to request the cessation of electronic communications for marketing purposes

or to revoke their consent for such communications (Article 22). Similarly, Tunisian law allows data subjects, their heirs, or their guardians to object to the portability of their personal data to third parties for advertising purposes, which immediately halts the processing (Article 42).

Both the GDPR and Lebanese law grant data subjects the right to object to the use of their data for commercial promotion. However, Lebanese law includes an exception to this right if data subjects had previously consented to such processing. This exception represents a violation of individuals' privacy rights and control over their personal data, exposing it to potential misuse and exploitation by business companies seeking profit.

In this context, it is best practice to abide by the principle of obtaining data subjects' explicit consent for the processing of their data under purposes, and to **seek separate consent from them when a processor intends to use data for commercial marketing**. This ensures that consent for processing personal data for non-commercial purposes does not automatically extend to commercial marketing endeavors without the explicit consent of the data subjects. Furthermore, **data subjects should be granted the right to revoke their consent**.

9 - RIGHTS OF PERSONAL DATA SUBJECTS

The law should unequivocally uphold the rights of individuals regarding their personal data, as exercising these rights is intrinsically linked to the principle of "individual autonomy." The GDPR includes all the rights of data subjects concerning their personal data, which are:

- The right to **be informed**,
- The right to **access**,
- The right to **rectify** data,
- The right to **erase** data,
- The right to **limit data processing**,
- The right to **data portability**,
- The right to **object to data processing**,
- The right **not to rely solely on automated processing for decision-making** regarding individuals, including decisions aimed at profiling data subjects or evaluating certain aspects of their personality.

The law in Oman, Qatar, and Tunisia stipulates most of these rights to varying extents. However, Lebanese law recognizes all the aforementioned rights except for the right to limit data processing and the right to data portability. Yet, certain rights stipulated in the law require other guarantees to ensure their good practice. For instance, **the right to obtaining a copy of one's data should be done at no cost**. Furthermore, frequent requests for data copies might be deemed an abuse of this right. Additionally, Lebanese law restricts individuals' right to object if they had previously consented to such processing.

Exceptions:

Each of the laws in Oman, Lebanon, Qatar, and Tunisia, along with the GDPR, incorporates various exceptions regarding the exercise of these rights. The GDPR stipulates that these exemptions must respect the essence of fundamental rights and freedoms, being necessary and proportionate in a democratic society for safeguarding national or public security, exercising the right to defense, prevention, investigation, detection, or prosecution of crimes, for the enforcement of sentences. These exemptions may also serve other purposes of interest to public opinion, protect judicial independence and proceedings, surveillance and inspection performed by public authorities, or safeguard the rights of data subjects or the rights and freedoms of others (Article 23).

Hence, it is crucial to guarantee that data subjects have the opportunity to fully exercise all the aforementioned rights stipulated for them. If restrictions were imposed on exercising these rights, they must be deemed necessary and proportionate to safeguard specific interests defined by the law.

10 - OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS

The individual responsible for managing personal data, whether referred to as the data controller, or supervisor, is the natural or legal person that defines the objectives and methods of data processing. Conversely, the processor, or the handler, is the natural or legal person who processes personal data on behalf of the individual responsible for data processing.

Each of the laws in Oman, Qatar, and Tunisia detailed the obligations of the individuals responsible for data processing and data processors, while the GDPR set comprehensive guidelines on this matter. These obligations focus on the proper application of the law protecting personal data and ensuring the rights of data subjects. This is done, for example, by compelling them to set controls and procedures to be adhered to while processing personal data, keep documentation relating to processing activities, and inform personal data subjects through written notifications before processing, including information about the processing and their personal rights. Furthermore, they must take all necessary measures to ensure data safety and security, prevent data distortion or damage, unauthorized access, and notify the authority and data subjects about personal data breaches leading to their destruction, change, disclosure, unauthorized access, or illegal processing. Additionally, they must provide the authority with required and necessary data and documents for the authority to exercise its competence defined by law.

On the flip side, Lebanese law did not specify the obligations of the person responsible for personal data processing but merely included the text informing data subjects of the following: The identity of the individual responsible for data processing or that of the representative, the purposes of data processing, whether responses to queries are mandatory or optional, the repercussions of non-

response, the recipients of the data, and the right to access and rectify information, along with the available means to do so. Moreover, the law stipulated that the responsible for data processing take measures ensuring data safety, security, and confidentiality. While Lebanese law did not explicitly mention a “data processor,” it only referred to the “representative of data processing responsible” in Article 88 and the obligation of notifying persons from whom personal data is collected about the aforementioned information.

The lack of explicit and detailed provisions regarding the obligations of individuals responsible for data processing in Lebanese law undermines the necessary safeguards for protecting the data information. This also opens the door to non-compliance with laws and violations of data subjects’ rights and data confidentiality.

11 - AUTHORITY RESPONSIBLE FOR MONITORING LAW ENFORCEMENT

The laws in Lebanon, Oman, and Qatar assigned the responsibility of monitoring law enforcement to a relevant ministry: The Ministry of Economy and Trade (MoET) in Lebanon, the Ministry of Transport, Communications and Information Technology in Oman, and the Ministry of Transport and Communications in Qatar. The responsible authority for monitoring law enforcement in these countries operates under the executive power. As for Tunisian law, it has established an authority with legal personality and financial independence, comprising members representing the executive, legislative, and judicial branches. Additionally, the GDPR recommends establishing an independent authority while setting specific standards for organizing the latter and ensuring the efficiency of its members and the safeguard of their independence from any external influence. The regulation also guarantees a mechanism for monitoring, accountability, and proper enforcement of the law while protecting personal data.

Establishing an independent authority to monitor law enforcement is recommended, as such independence helps mitigate conflicts of interest, enhancing transparency at work, build public trust in the monitoring process, as well as strengthening monitoring and accountability mechanisms, as these independent bodies prioritize individual rights over political and governmental interests.

12 - TASKS AND PREROGATIVES OF THE LAW ENFORCEMENT AUTHORITY

The laws in the Sultanate of Oman (Article 7), Qatar (Article 27), Tunisia (Articles 76, 77, and 79), and the GDPR (Article 57, paragraph 4, and Article 58) extensively delineate the tasks and prerogatives of the authority responsible for law enforcement. However, these tasks may vary based on the legal and administrative structures of each country. In general, these laws mandate the authority to monitor

law enforcement, establish implementation procedures or directives, raise awareness, and provide guidance about the law, receive, accept, or object to certifications, receive data subjects' complaints, conduct investigations and decide on them, prepare and disseminate periodic reports on data protection activities, and collaborate with other monitoring authorities.

Unlike other laws, Lebanese law does not clearly specify the tasks and prerogatives of the MoET. Instead, it only mentions its role in receiving certifications for the collection and processing of personal data (Article 95) and in publishing a list of authorized processing that has met the licensing or certification requirements (Article 98). This lack of clarity negatively impacts proper law enforcement and leaves room for violations of rights within the scope of personal data protection.

Therefore, **it is important to clearly and explicitly detail the tasks of the independent authority in the law, which helps identify the scope of its competence and adhere to it.** The authority's tasks and prerogatives revolve around the proper and effective enforcement of data protection law and the safeguarding of data subjects' rights.

13 - DATA PROCESSING CERTIFICATIONS

The natural or legal person responsible for processing personal data submits certification to the competent authority to inform them of personal data processing.

In principle, Lebanese law (Article 95), Omani law (Article 5), Qatari law (Article 16), and Tunisian law (Article 7) required personal data processing certification. However, the GDPR did not explicitly stipulate the obligation to obtain certification for data processing, leaving the decision to each country.

Exceptions to this principle are found in both Lebanese and Tunisian laws, which exempt certain processing activities from the obligation to get certification, including those conducted by public authorities. As for other exceptions, Tunisian law exempted from getting a certification for personal data processing concerning an employee's professional situation by the employer when necessary for workflow and organization (Article 16). In contrast, Lebanese law, under Article 94, stipulated eight additional exceptions to this requirement, besides the exemption for public authorities, without providing specific justifications. These exceptions included:

- Prior consent for personal data processing is obtained unless there exists a legal prohibition.
- Non-profit associations maintaining records of their members and stakeholders within the scope of their normal and legal tasks.
- Processing involving the maintenance of special records, as stipulated by legal or regulatory provisions, intended for public disclosure and that may be accessible to persons with legitimate interests.

- Processing involving pupils and students from educational institutions for educational or administrative purposes related to the institution.
- Processing involving employees or members of institutions, business companies, unions, associations, and freelancers, within the limits and needs of the legal exercise of their activities.
- Processing activities involving customers and stakeholders of these institutions, business companies, unions, associations, and freelancers within the limits and needs of the legal exercise of their activities.
- Certain processing activities or some of their categories, if it turns out that they are in progress and do not pose any threats to private life or personal freedoms, pursuant to a decree issued by the Council of Ministers upon the recommendation of the Ministers of Justice and the MoET.
- Processing activities stipulated in Law No. 140/99, aimed at safeguarding the right to confidentiality of intelligence operations conducted through any means of communication (Wiretapping Law).

In general, certifications help in organizing the processing of these data and in ensuring compliance with law by those responsible for the processing. Therefore, **there is no hindrance to structuring this processing through the requirement of certification, even when involving public authorities.** However, if a requirement for processing certification is adopted, **the exceptions to this requirement should be limited and well justified, based on the principle of equality before the law**, and safeguarding the data protection right and privacy.

14 - DATA PROCESSING LICENSING

Licenses represent the consent from the relevant authority for some personal data processing undertaken by a natural or legal person. They constitute an additional guarantee to protect certain personal data categories. Breaching or disclosing such data could result in significant harm to the data subjects and their rights, or other protected interests.

Both Lebanese and Tunisian laws delineated the scenarios wherein obtaining a license is mandatory for personal data processing. In Lebanon, processing personal data pertaining to national internal and external security requires licensing from the minister of National Defense and the minister of Interior and Municipalities. Processing pertaining to criminal offenses and various legal proceedings necessitates licensing from the minister of Justice. Moreover, processing data concerning individuals' health conditions, genetic identity, or sexual life mandates licensing from the minister of Public Health (Article 97). Additionally, the law requires prior licensing from the Cabinet, based on the recommendation of the relevant minister, in case of processing personal data in ministries, administrations, and public institutions beyond the scope of their legal and regulatory texts (Article 104).

As for Tunisian law, obtaining a license is required for processing personal data related to racial or genetic origins, religious beliefs, political, philosophical, or trade union opinions (Article 14). Moreover, a license is necessary for referring personal data when written and explicit consent is not obtained from the concerned persons, their heirs, or their guardian, under specific conditions (Article 47), and for the portability of personal data abroad, as specified in (Article 52).

In general, **there is no objection to requiring licenses for processing sensitive categories of personal data. However, it is recommended that the independent authority monitoring law enforcement be empowered to grant these licenses.**

15 - PUBLICATION OF CERTIFICATIONS AND LICENSES

Both Lebanese law (Article 98) and Omani law (Article 7) mandated the publication of certifications and licenses. This publication is considered a key tool for promoting transparency in personal data processing.



16 - FILING COMPLAINTS

Laws in the Sultanate of Oman, Qatar, Tunisia, as well as the GDPR, grant personal data subjects the right to file complaints if harmed due to violations of personal data protection laws. Lebanese law stipulates, under Article 102, the right of data subjects to refer to competent courts, particularly judges of urgent matters, to ensure access and rectification rights and compel the defendant to apply law provisions. Similarly, Omani law, under Article 12, empowers data subjects to file complaints before the Ministry of Transport, Communications and Information Technology if they believe and consider their personal data processing breaches the law. Qatari law, according to Article 26, allows data subjects to lodge complaints with the competent administrative unit at the Ministry of Transport and Communications for contravening the provisions of this law and the decisions issued in implementation thereof. Tunisian law, as outlined in Article 76, grants data subjects the right to lay charges with the National Authority for the Protection of Personal Data. Finally, the GDPR stipulates in Article 57 the right of individuals to file complaints with the authority monitoring law enforcement.

It is preferable for Lebanese law to stipulate the establishment of an independent authority responsible for monitoring the enforcement of data protection law, and capable to receive complaints in cases of law violations.

17 - SANCTIONS

In Lebanese law (Articles 106 to 109), Omani law (Articles 24 to 32), Qatari law (Articles 23 to 25), and Tunisian law (Articles 86 to 103), as well as the GDPR, sanctions are delineated for certain breaches. They uniformly stipulated fines, with Lebanese and Tunisian laws also imposing incarceration in certain instances.

The preferable approach is to enforce fines as sanctions for breaching personal data protection laws.

18 - MEASURES

The GDPR (Article 58) and Omani law (Article 8) have established the measures to be taken to ensure effective law enforcement. Omani law granted the Ministry of Transport, Communications and Information Technology the authority to take various actions, including warning controllers or processors violating this law provisions, mandating the rectification or deletion of improperly processed personal data, suspending the processing temporarily or permanently, and halting the portability of personal data to another country or international organization. As for the measures outlined by the GDPR, which the monitoring authority may undertake, they are as follows:

- Warnings and reprimands,
- Ensuring that the individuals responsible for processing, or processors, honor data subjects' requests to exercise their rights and comply with laws,
- Instructing the responsible for data processing to communicate with affected data subjects in case of data breaches,
- Imposing temporary or permanent restrictions, including processing bans,
- Ordering the rectification or deletion of personal data, or limiting processing, and ensuring that these measures are communicated to the recipients who have been provided with the personal data,
- Withdrawing or prohibiting certifications, and imposing administrative fines,
- Ordering suspension of data flows to recipients in third countries or international organizations.

Empowering the independent authority to impose various measures is preferable for ensuring proper law enforcement.

19 – SPECIAL PROVISIONS FOR PROCESSING SPECIFIC DATA CATEGORIES

Special provisions are allocated to certain categories of data deemed sensitive, thus requiring additional safeguards to protect them and the rights of data subjects.

Lebanese and Omani laws did not specifically address the processing of certain categories of data, unlike Qatari, Tunisian laws, and the GDPR. The Qatari law dedicated a section to personal data of special nature such as racial origin, children, health, physical or psychological conditions, religious beliefs, marital relationships, and criminal offenses. It also allocated some articles concerning data processing of children by websites targeting them. Meanwhile, Tunisian law outlined provisions for processing data of public figures (from Article 53 to Article 61), health-related data (from Article 62 to Article 65), scientific research data (from Article 66 to Article 68), and data processing for visual surveillance purposes (Article 69 to Article 74).

The GDPR included provisions relating to various sensitive data categories such as:

- Processing related to freedom of expression and access to information (Article 85)
- Processing and public access to official documents (Article 86)
- Processing of national identification numbers (Article 87)
- Processing in the employment context (Article 88)
- Safeguards and exceptions about processing archiving in the public interest, or scientific, historical, or statistical researches (Article 89)
- Confidentiality obligations (Article 90)
- Existing rules for the protection of churches and religious associations' data (Article 91)

The GDPR included data requiring further protection due to its sensitive nature. Therefore, adopting the categories outlined in the GDPR ensures the protection of a wide array of data.

After delineating the preferred provisions and best practices for personal data protection laws in section one of the report, we accordingly propose a detailed index tailored for such law in Lebanon.

SECTION TWO - PROPOSED COMPREHENSIVE INDEX FOR PERSONAL DATA PROTECTION LAW

CHAPTER 1: GENERAL PROVISIONS

Article 1: Definitions³

Clear definition of legal terminology used in the law is essential for its proper understanding and application.

Key legal terms in this context include:

- Personal data
- Personal data processing
- Personal data subjects
- Persons responsible for data processing or controllers
- Processors
- Personal data recipients
- Third parties
- Data subjects' consent
- Personal data breaches

Article 2: Upholding the Right to Personal Data Protection⁴

All individuals have the right to protect their personal data

3 For more information on definitions, see annex 1

4 For more information on upholding the right to personal data protection, see annex 2.

Article 3: Scope of the Law⁵

The law applies to both automated and non-automated processing of personal data and extends to processing data of citizens and residents of Lebanon regardless of the nationality of the person performing the processing or the location where the data is stored.

However, the law does not cover processing related to personal activities exclusively conducted for one's own needs, or to household activities.

CHAPTER 2: PERSONAL DATA PROCESSING⁶

Article 4: Principles of Processing

Personal data processing is governed by seven fundamental principles to ensure its protection:

- Lawfulness, fairness, and transparency: Data processing must be lawful, fair, and transparent to data subjects.
- Purpose limitation: Clearly define the legitimate purpose for collecting data from data subjects, ensuring it is explicit and specific.
- Data minimization: Collect and process only the necessary amount of data for the specified purpose.
- Accuracy: Maintain the accuracy of personal data and update it when necessary to ensure it remains relevant.
- Storage limitation: Store personal data for the necessary period to achieve the specified purpose, avoiding unnecessary retention.
- Integrity and confidentiality: Process data in a manner that ensures appropriate security, safety, and confidentiality, using measures such as encryption.
- Accountability: Holding the person responsible for data processing accountable for compliance with personal data protection regulations.

Article 5: Lawful Processing

Personal data processing is deemed lawful in the following cases:

- When data subjects provide specific and unambiguous consent for data processing.
- When processing is necessary for drafting or executing a contract in which the data subjects are involved.

5 For more information on the scope of the law, see annex 3.

6 For more information about data processing, see annexes 4,5 and 6.

- When data processing is required to comply with legal obligations.
- When data processing is necessary to save someone's life.
- When data processing is necessary to perform a task in the public interest or to carry out official duties.
- When there is a legitimate interest in processing the personal data of an individual.

In all cases, the fundamental rights and freedoms of the individual concerned take precedence over the interests of the personal institution, especially if the personal data pertains to a child.

It is essential to specify the legal basis for processing personal data and to communicate with data subjects each time this basis is changed.

Article 6: Data Not to Be Processed

Processing sensitive data, which includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of solely identifying a natural person, and data related to health or sexuality, is prohibited.

However, processing of such data is authorized in specific cases underlined in the law.

CHAPTER 3: DATA SUBJECT CONSENT TO DATA PROCESSING⁷

Article 7: Properties of Processing Consent

Data subjects' consent to the processing of their personal data must comply with the following requirements:

- Consent must be clearly given, specific, informed, clear and explicit.
- Request for consent must be clearly distinguishable from other requests and should be presented in simple and clear language.
- Data subjects have the right to revoke consent at any time
- Children under the age of thirteen can only give consent with the permission of their parents.

⁷ For further information regarding consent, refer to annexes 7 and 8.

Article 8: Utilizing Personal Data for Commercial Marketing or Advertising Purposes

The person responsible for processing is committed to obtaining data subjects' consent before sending any advertising or marketing material for commercial purposes.

CHAPTER 4: RIGHTS OF PERSONAL DATA SUBJECTS⁸

Individuals whose personal data is being processed are entitled to various rights regarding the handling of their personal information.

Article 9: Right to Be Informed

Article 10: Right to Access

Article 11: Right to Rectification

Article 12: Right to Object

Article 13: Right to Restrict Processing

Article 14: Right to Deletion

Article 15: Right to Portability

Article 16: Right to Not Be Subjected to Solely Automated Processing of Data for Decision-making, Assessment, or Analysis of Human Behavior

Article 17: Exceptions to the Exercise of the Personal Data Subject's Rights

CHAPTER 5: OBLIGATIONS OF THE RESPONSIBLE FOR DATA PROCESSING OR THE PROCESSOR⁹

Article 18: The Responsible for Processing Obligations

- Establishing codes and procedures to be followed when processing personal data.
- Providing data subjects with written notice, prior to commencing processing, regarding the processing activities and their rights within the framework of data protection.

⁸ For more information about the rights of personal data subjects and exceptions, refer to annex 9.

⁹ To learn more about the obligations of the personal data subject's right.

- Taking all measures, considering the nature of the data and the risks associated with the processing, to ensure data safety and security and prevent its alteration, damage, or unauthorized access.
- Ensuring personal data confidentiality, and refraining from disclosing it without data subjects' prior consent.
- Notifying the monitoring authority and the data subjects in the event of a personal data breach that results in destruction, alteration, disclosure, unauthorized access, or unlawful processing.
- Keeping records of processing activities.
- Providing the data and documents requested by the monitoring authority that are deemed necessary for exercising its specific authority under the law.

Article 19: Processor's Obligations

The processor commits to adhering to the provisions of the law specifically by:

- Taking all measures to ensure data safety and security, preventing any tampering, damage, or unauthorized access.
- Refraining from engaging with another processor without obtaining data subjects' consent.
- Ensuring that the processing operation adheres to a contract defining the legal obligations.
- Providing the data and documents requested by the authority, as deemed necessary for the exercise of its specified jurisdiction under the law.

CHAPTER 6: THE AUTHORITY RESPONSIBLE FOR LAW ENFORCEMENT AND ITS TASKS

Article 20: Establishment of an Independent Monitoring Authority

The level of adherence to legal provisions is under the scrutiny of an independent regulatory body.

Article 21: Properties of the Independent Authority¹⁰.

The independent body should have the following properties:

- Its members must be independent from any direct or indirect external interference.
- Its members must be competent.
- It must establish and enforce stringent rules and procedures regarding recruitment mechanisms and employees' conduct.
- It should have the authority to choose its staff.

¹⁰ To access further information about the independent authority and its tasks, refer to annex No. 11

- All employees are bound by professional confidentiality during and after tenure.
- It must operate with transparency.

These properties ensure the smooth functioning of the authority and shield it from external interference and corruption.

Article 22: Tasks of the Independent Authority¹¹

The Independent Authority is entrusted with tasks aimed at ensuring the protection of individuals' personal data rights.

Its tasks are as follows:

- Establishing procedures or guidelines for law enforcement.
- Ensuring privacy protection.
- Reviewing and approving or objecting to certifications.
- Issuing and revoking licenses.
- Educating the responsible for data processing and processors about their legal obligations.
- Monitoring law enforcement and verifying compliance by data controllers.
- Handling complaints from personal data subjects, conducting investigations and rulings on them.
- Collaborating with authorities responsible for personal data protection in other countries.
- Providing advice, support and coordination to public administrations and individuals on personal data protection matters.
- Raising public awareness on personal data protection.
- Compiling and publishing periodic reports on its activities related to personal data protection.
- Maintaining a register of authorized controllers and processors.
- Keeping records of breaches committed and the actions taken regarding them.
- Monitoring developments related to personal data protection and proposing or providing input on issuing or amending relevant legislation, decrees and decisions.

CHAPTER 7: CERTIFICATIONS AND LICENSES¹²

Article 23: Providing Certifications for Processing

All processing operation of personal data requires prior certifications that must be deposited with the regulatory authority.

Authority non-objection for the personal data processing is deemed as acceptance.

¹¹ To learn more about the Independent Authority and its tasks, refer to annex number 12.

¹² To access more information about permits and licenses, refer to annex 13, 14, and 15.

Timely responses are provided to certification requests to ensure seamless data processing operations.

Certain processing activities may be exempt from the certification requirements.

Article 24: Obtaining Licenses for Processing

A license from the independent authority is required for personal data processing.

The decision to grant or reject the license is issued within a reasonable timeframe.

Article 24: Publication of Certifications and Licenses

The certifications and licenses issued by the authority are published on its official website.

CHAPTER 8: ACCOUNTABILITY¹³

Article 26: Personal Data Subjects' Complaints

Data subjects have the right to file a complaint before the independent authority if they believe that their personal data processing violates the law.

Article 27: Sanctions

Penalties shall be imposed for breaches of this law provisions, with the amount of the fine contingent upon the nature of the breach. Affected individuals have the right to seek compensation for damages incurred.

Article 28: Measures

Given the authority's oversight of law enforcement, it is entitled to:

- Warning the controller or processor about any breaches committed against this law provisions.
- Ordering the rectification and deletion of personal data processed contrary to the law provisions.
- Temporarily or permanently suspending the personal data processing.
- Ceasing personal data transfer to another country or international organizations.
- Taking any other action deemed necessary by the ministry to protect personal data.

¹³ For more information on accountability, refer to annexes 16, 17 and 18.

CHAPTER 9: SPECIAL PROVISIONS RELATED TO THE PROCESSING OF CERTAIN CATEGORIES OF DATA¹⁴

The law establishes special provisions related to the processing of certain categories of data.

14 For more information regarding the provisions concerning the processing of specific categories of data, refer to annex 19.



CONCLUSION

Given the shortcomings and gaps in the existing Lebanese law, specifically Law No. 81/2018 on “Electronic Transactions and Personal Data Protection,” as highlighted in the report, urgent action is required to introduce a dedicated and independent law focused on safeguarding personal data. This new legislation should align with international best practices and standards to address the pressing issues identified, especially concerning the acquisition and withdrawal of consent from data subjects.

An updated and robust legal framework is crucial to demonstrate Lebanon’s commitment to protecting human rights, particularly the fundamental right to privacy. It should prioritize the principle of individual autonomy, empowering individuals to exercise control over their data. Furthermore, the law should enhance protection measures, foster accountability among data processors, and bolster resilience against the evolving challenges posed by digital communication technologies.

The increasing volume of personal data processing and the complexities of digital transactions necessitate a comprehensive and forward-looking approach to data protection. By enacting such legislation, Lebanon can proactively respond to the dynamic landscape of digital privacy concerns, ensuring that its legal framework remains effective, relevant, and in line with global standards.

ANNEXES

ANNEX 1: DEFINITION OF TERMS IN LAW

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Personal data means: “Any information relating to an identified or identifiable natural person who can be identified directly or indirectly, in particular by reference to multiple sources of information or the cross-referencing of information” (Article 1).	Personal data means: “Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Article 4). The regulation also defines some data types: Genetic data, Biometric data and data concerning health (Article 4).	Personal data means: Any information relating to an identified or identifiable natural person who can be identified directly or indirectly, in particular by reference to one or more identifiers, such as name, civil number, electronic identifiers or location data, or to one or more factors specific to the genetic, physical, mental, psychological, social, cultural or economic identity of that natural person. The law also specifically defines different types of personal data: - Genetic data - Biometric data - Health data	Personal data means: “Data pertaining to an individual whose identity is determined, or can be reasonably determined, either through such data or by combining it with any other data.” (Article 1).	Personal data means: “All information, regardless of its source or format, that enables the identification of a natural person directly or indirectly, excluding information related to public life or deemed as such by law” (Article 4).

Lebanese law also defines other terms: - Personal data processing - Person responsible for personal data processing - Personal data addressee (Article 1).	The European Union also defines other terms: - Processing - Restriction of processing - Controller - Processor - Recipient - Third Party - Consent - Personal Data Breach (Article 4).	Omani law also defines other terms: - Processing - Personal Data Subjects - controller - Processor (Article 1).	The Qatari law also defines other terms, including: - Personal data processing - Individual - Controller - Processor - Legitimate purpose - Acceptable practices - Direct marketing - Website operator (Article 1).	The Tunisian law also defines other terms, including: - Processing of personal data - Data subjects - Data processor - Third party - Handler - Referral? - Beneficiary (Chapter 2)
---	--	---	---	---

ANNEX 2: UPHOLDING THE RIGHT TO PERSONAL DATA PROTECTION

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Did not ensure the right to personal data protection	Ensured the right to personal data protection: "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (Article 1(2)). The regulation also states that "Data protection" must be considered in the design of any new product or activity "by design and by default" (Article 25).	The right to protect personal data is enshrined in Article 4: "Personal data is protected under this law provisions."	The right to protect personal data is enshrined in Article 3: "Every individual has the right to protect their personal data privacy."	The right to protect personal data is enshrined in Article 1: "Every individual has the right to protect personal data pertaining to their private life, as it is one of the fundamental rights guaranteed by the Constitution."

ANNEX 3: SCOPE OF THE LAW AND EXCEPTIONS

Scope of the law:

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The law applies to both automated and non-automated personal data processing (Article 85).	1- Applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Article 2.1). 2- Applies if (Article 3) personal data of EU citizens or residents is processed, or goods or services are offered to such people. 3- Applies the same outside of the EU (extra-territorial scope), if: a) The organization offers goods or services to people in the EU (Article 3.2.a) Does not account for occasional instances, but rather where the EU is actually a target market.	The law applies to personal data that is processed (Article 2).	The law applies to personal data when it is processed electronically, obtained, collected, or extracted in any other way for electronic processing, or processed through a combination of electronic and traditional processing methods (Article 2).	The law applies to both automated and non-automated processing of personal data, whether carried out by natural or legal persons (Section 2).

	b) The entity monitors their online behavior (Article 3.2.b) When the website uses tools to track cookies or the IP addresses of people who visit from EU countries. 4- Applies even if the data is being stored or used outside the EU (Article 3.1).			
--	---	--	--	--

Exceptions:

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The regulation does not apply to person activities processing carried out solely for personal needs (Article 85).	The regulation does not apply to: 1- Purely personal or household activity (Article 2.2.c). 2- Organizations with under 250 employees are usually freed from the record-keeping obligation (Article 30.5).	The regulation does not apply to processing of personal data: 1- If the processing is carried out on a personal or familial basis. 2- Execution of legal prerogatives by state bodies (state administrative units and other public legal entities). 3- Protecting the state's economic and financial interests.	The regulation does not apply to personal data processed by individuals for personal or family purposes, as well as personal data processed for the purpose of obtaining official statistical data in accordance with the provisions of Law No. 2 of 2011 (Article 2).	The regulation does not apply to processing of personal data for personal or family purposes, provided that it is not transferred to third parties (Article 3).

		4- Disclosure or prevention of any crime based on an official written request from investigating authorities. 5- Compliance with a legal obligation imposed on the data controller by any law, judgment, or court decision. 6- Protecting vital interests of the personal data subjects. 7- Execution of a contract where the personal data subjects are a party of it. 8- Protection of national security or public interest. 9- Conducting historical, statistical, scientific, literary or economic research by authorized entities, provided that no indication or reference pertaining to the data subjects is used in the published research and statistics, to ensure that personal data is not attributed to a known or identifiable natural person. 10- When the data is publicly available and does not violate the provisions of this law (Article 3).		
--	--	--	--	--

ANNEX 4: PROCESSING PRINCIPLES

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
1- Fairness, lawfulness and purpose specification: Personal data is collected in lawfulness, for legitimate, specific and explicit purposes. 2- Data minimization, validity and accuracy: Data must be relevant and not exceeding the stated objectives. Data must be correct and complete, and kept up-to-date to the extent necessary (Article 87). The data cannot be processed at a later stage for purposes incompatible with the stated purposes, <u>unless</u> the data is processed for statistical, historical or scientific research purposes (Article 87). 3- Storage limitation Data storage shall be lawful and limited to the period specified in the processing certification or the decision (Article 90).	1- Lawfulness, fairness and transparency (Article 5.1.a) Processing must be lawful, fair, and transparent to the data subject. 2- Purpose limitation (Article 5.1.b) Data must be processed for the legitimate purposes specified explicitly to the data subject when it is collected. 3- Data minimization (Article 5.1.c) Only as much data as absolutely necessary for the purposes specified should be collected and processed. 4- Accuracy (Article 5.1.d) Personal data must be kept accurate and up to date. 5- Storage limitation (Article 5.1.e) Personally identifying data must only be stored for as long as necessary for the specified purpose.	1- Transparency and fairness: Processing takes place with transparency and fairness, respecting human dignity and requiring explicit data subjects' consent (Article 10). 2- Integrity and confidentiality: Data subjects are informed of any breaches or violations of their data and the measures undertaken in response (Article 11). 3- Accountability: Sanctions for breaches are clearly outlined in the law.	1- Fairness, lawfulness and transparency Processing personal data with fairness and lawfulness, within the framework of transparency and fairness, respecting human dignity and acceptable practices, in accordance with the law provisions (Article 3). 2- Accuracy: Data minimization, storage limitations It is the responsibility of the controller to ensure that the personal data collected or processed on their behalf is relevant for legitimate purposes, accurate, complete, and up-to-date as necessary for the intended purposes. Data should not be retained for longer than necessary to fulfill those purposes (Article 10).	1- Fairness and transparency: Processing occurs within the framework of transparency, fairness, and respect for human dignity, in accordance with this law provisions (Chapter 1). Processing takes place with respect for human dignity, private life, public freedoms, and the rights of individuals protected by laws (Chapter 9). 3- Purpose specification: Data is collected for legitimate, specific, and clear purposes (Chapter 10). The law provided exceptions, including cases where consent is given by the data subjects or when collection is for established scientific purposes (Chapter 12). 4- Data Minimization: Data processing is limited to what is necessary for the purpose for which it was collected (Chapter 11).

4- Data fairness, security and confidentiality The person responsible for data processing should take all measures, considering the nature of the data and the risks resulting from processing, to ensure the data fairness and security and prevent tampering or damage, and unauthorized access to it (Article 93). 5- Accountability The law specified the sanctions for violating the law from Article 106 to Article 109,	6- Integrity and confidentiality (Article 5.1.f) Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption). In the event of a data breach, the affected persons must be informed within 71 hours. 7- Accountability (Article 5.2) The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.		3- Integrity and Confidentiality: Individuals are notified of any inaccurate disclosure of their personal data. 4- Accountability: The law specifies sanctions for breaches.	5- Accuracy: The person responsible for the processing ensures that the data is accurate, precise, and up-to-date (Chapter 11). 6- Personal data is only collected directly from the data subjects. Exceptions are provided for in the law (Chapter 44). 7- Storage Limitation: Personal data is disposed of once the specified period for its retention expires, or when the purpose for which it was collected has been achieved, or if it is no longer necessary for the person responsible for the processing's activities (Chapter 45). Exceptions are provided for, including personal data intended for referral to public authorities after obtaining the data subjects' consent and the National Authority for the Protection of Personal Data (Chapter 46). 8- Accountability: The law specified sanctions for breaches.
--	--	--	--	---

ANNEX 5: LAWFUL PROCESSING

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The law did not provide for the data subjects' independent and explicit consent to their personal data processing. Reference is made to the personal data subjects' consent in Article 91, which stipulates the possibility of collecting or processing personal data if it reveals, directly or indirectly, the health status, genetic identity, or sexual life of the person concerned, subject to the explicit consent of the individual concerned (Article 91). However, this consent prevents data subjects from exercising their right to object to the collection and processing of their data in this context (Article 92).	The processing of personal data is considered lawful if the data subject gave specific, unambiguous consent, pursuant to process the data. <u>Exceptions:</u> The processing of personal data is still lawful (even without having the consent of the data subject) in the following circumstances: 1- Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. 2- Processing is necessary to comply with a legal obligation of yours. 3- Processing is necessary to save somebody's life. 4- Processing is necessary to perform a task in the public interest or to carry out some official function.	Personal data may be processed only after obtaining this consent (Article 10).	The controller is not allowed to process personal data without the individual's consent. <u>Exceptions:</u> The law provided several exceptions: 1- When processing is necessary to achieve a legitimate purpose of the controller or a third party to whom the data is transferred (Article 4). 2- Safeguarding national security and public security. 3- Protection of the state's international relations. 4- Protection of the state's economic or financial interests. 5- Prevention of criminal offenses, including gathering information about them, or conducting investigations in that regard (Article 18).	Processing of personal data can only be carried out with the data subjects' explicit and written consent. <u>Exceptions:</u> 1- When personal data is evidently in the data subjects' interest, and obtaining consent is impracticable, or would require considerable effort. 2- When processing personal data is required by law or by an agreement in which data subjects are a party (Article 28). <u>Note:</u> Consent to the processing of personal data in a specific manner or for a particular purpose does not extend to other forms or purposes (Article 30).

	5- The organization has a legitimate interest in processing someone’s personal data. (Article 6).		6- Carrying out a task related to the public interest as defined by law. 7- Carrying out a legal obligation or an order from a competent court. 8- Protection of individuals’ vital interests. 9- Achieving scientific research purposes conducted in the public interest. 10- Collection of information necessary for investigating a criminal offense, upon official request from investigative authorities (Article 19).	
--	--	--	--	--

ANNEX 6: DATA NOT TO BE PROCESSED

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Personal data revealing, directly or indirectly, data subjects' health status, genetic identity, or sexual life. (Article 91). <u>Exception:</u> It becomes possible to collect such data if: 1- The data subjects make this information publicly available. 2- The data subjects explicitly consent to its processing, unless there is a legal impediment. 3- The collection and processing are necessary for medical diagnosis or treatment by a healthcare professional. 4- Establishing a right or defending against legal claims. 5- License is granted to process data:	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. <u>Exception:</u> 1- the data subject has given explicit consent. 2- processing is necessary in the field of employment and social security and social protection law. 3- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.	Personal data of a child is only permitted with the consent of their parent or guardian, unless such processing serves the child's best interests, as determined by the codes and procedures outlined in the law's enforcement regulation (Article 6).	The processing of personal data of children by the owner or operator of any website aimed at children is prohibited without obtaining explicit consent from the child's parent or guardian through electronic communication or any other suitable means (Article 17).	1- Personal data related to criminal offences, examination thereof, criminal proceedings, sanctions, precautionary measures, or criminal records (Article 13). 2- Personal data directly or indirectly related to racial or ethnic origin, genetic characteristics, religious beliefs, political opinions, philosophical beliefs, trade union membership, or health. <u>Exception:</u> Processing of the aforementioned personal data is permissible under the following conditions: - Data subjects' explicit written consent. - If the data becomes clearly public. - If processing is necessary for historical or scientific purposes.

- Related to the external and internal national security, by a joint decision issued by the Ministers of National Defense, Interior, and Municipalities. - Related to criminal offenses and legal proceedings by a decision issued by the Minister of Justice. - Related to health conditions, genetic identity, or sexual life of individuals by a decision issued by the Minister of Public Health (Article 97).	4- processing related to non-profit organization. 5- processing relates to personal data which are made public by the data subject. 6- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity. 7- processing is necessary for reasons of substantial public interest. 8- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. 9- processing is necessary for reasons of public interest in the area of public health,			- If processing is necessary to protect the data subjects' vital interests (Article 14). Such processing requires an license issued by the National Data Protection Authority (except for health data subject to other legal provisions). The Authority may approve the license while requiring the person responsible for the processing to take appropriate precautions or measures to protect the data subjects' interests (Article 15).
--	--	--	--	---

	10- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. <u>Note:</u> It was mentioned in many instances that processing of such data shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9).			
--	--	--	--	--

ANNEX 7: CONSENT PROPERTIES

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The law did not specify the consent properties, nor provide for the individual's right to revoke consent.	1- Consent must be "freely given, specific, informed and unambiguous." (Article 4.11) 2- Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language." (Article 7.2) 3- Possibility to always withdraw previously given consent (Article 7.3) 4- Children under 16 can only give consent with permission from their parents. Member States may lower this to 13 years of age. (Article 8.1) 5- The controller needs to keep documentary evidence of consent. (Article 7.1)	The request for processing personal data must be written clearly, explicitly, and in an understandable manner (Article 10). The data subjects have the right to withdraw or revoke their consent, provided that the processing carried out prior to the revocation is not compromised.	The law did not specify the consent properties but rather stated the possibility for the individual to withdraw or revoke their prior consent to processing.	1- The data subjects' consent to the processing of their data must be: - Explicit and written. 2- Consent cannot be contingent on receiving a service or benefit in return for the benefit of someone else (Chapter 17). 3- If the data subjects are minors, incapacitated or unable to sign, consent is subject to general legal rules (Article 27). Personal data relating to a child can only be processed with the consent of the child's guardian and the permission of the family judge (Article 28).

ANNEX 8: PERSONAL DATA UTILIZATION FOR COMMERCIAL MARKETING OR ADVERTISING PURPOSES

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Every natural person holds the right to object to the collection and processing of their personal data, including for marketing purposes, based on legitimate reasons, before the person responsible for the data processing. Exception to the right to object: - When the person responsible for the data processing is legally mandated to collect the data. - When the data subjects consented to the processing of their personal data (Article 92).	Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing (Article 21(2)). Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes (Article 21(3)).	The controller is required to obtain written consent from the data subjects before sending any advertising or marketing material with commercial purposes to them (Article 22).	Sending any electronic communication for direct marketing purposes to an individual is prohibited without obtaining their prior consent (Article 22).	The use of personal data for advertising purposes is prohibited without explicit and specific consent from the data subjects, their heirs, or legal guardian (Article 30). Additionally, these parties reserve the right to object to the transfer of their personal data to third parties for advertising purposes. Such objection shall promptly halt the processing of their data (Article 42).



ANNEX 9: RIGHTS OF PERSONAL DATA SUBJECTS

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
1- The right to access personal data: Unless the subject matter of the processing pertains to internal or external state security and disclosure jeopardizes its objectives or state security (Article 86 and Article 103). 2- The right to object: For legitimate reasons against the collection and personal data processing. Exceptions: - When the person responsible for the data processing is legally mandated to collect the data, or if the data subjects consented to the processing (Article 92). - If the data subjects consented to the data collection and processing, directly or indirectly revealing their health status, genetic identity, or sexual life (Article 92).	1- The right to be informed (Article 13 & 14) 2- The right of access (Article 15) 3- The right to rectification (Article 16) 4- The right to erasure (Article 17) 5- The right to restrict processing (Article 18) 6- The right to data portability (Article 20) 7- The right to object (Article 21) 8- Rights in relation to automated decision making and profiling (Article 22) Exceptions on all rights mentioned above: Such a restriction respects the essence of the fundamental rights and freedoms, is necessary, and proportionate in a democratic society to safeguard: 1- national security; 2- defense;	- The right to request that personal data be amended, updated or withheld. 2- The right to obtain a copy of processed personal data. 3- The right to transfer personal data to another controller. 4- The right to request the erasure of personal data, unless the processing is necessary for national archiving and documentation purposes	1- The right to object to the processing of personal data in certain cases specified by the law, such as situations where the processing is unnecessary for the intended purposes. 2- The right to request the erasure or deletion of personal data in specific situations, including when the processing is discriminatory, unfair, unlawful, or when consent has been withdrawn, or completion of the data's original purpose (Article 5). 3- The right to request the rectification of personal data with accompanying evidence supporting the request (Article 5). 4- The right of access to personal data and to request its review (Article 6). 5- The right to be informed Individuals shall be notified of the processing of their personal data and the purposes of the processing.	1- The Right to information: Individuals have the right to prior and comprehensive information regarding the processing of their personal data, provided through any means that leaves a written record, ensuring their awareness of the processing and their associated rights (Article 31). 2- Right of access: The data subject, their heirs, or legal guardian possess the right to access all personal data pertaining to them and to request rectifications, completions, amendments, updates, alterations, clarifications, or deletions if any information is found to be inaccurate, ambiguous, for which the processing is prohibited. This right also encompasses the receipt of a clear and identical copy of the data, particularly when processed automatically (Article 32).

3- The right to ascertain whether personal data is subject to processing or not (Article 99). 4- The right to receive a clear and understandable copy of their personal data along with additional information (Article 99). The person responsible for the data processing may provide the copy for a fee, and may object to arbitrary requests, especially in terms of quantity, frequency, or systematic nature (Article 100). 5- The right to rectify, supplement, update, or erase data (Article 107). This includes data that is inaccurate, incomplete, misleading, expired, incompatible with processing purposes, or prohibited from processing, collection, usage, storage, or portability (Article 101).	3- public security; 4- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; 5- other important objectives of general public interest; 6- the protection of judicial independence and judicial proceedings; 7- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority; 8- the protection of the data subject or the rights and freedoms of others; 9- the enforcement of civil law claims (Article 23).		6- The right to obtain a copy of their personal data upon payment of a fee not exceeding the cost of the service (Article 6). The law provided exceptions to this right, such as cases where exercising this right would disclose personal data concerning another individual without his consent, resulting in tangible or moral harm (Article 21). Additionally, the controller may refuse to provide data copies in situations involving national security and public order protection, safeguarding international relations, protecting the economic or financial interests of the state, and preventing any criminal offense, collecting of information or investigation (Article 20). Lastly, the law outlined <u>common exceptions for both the right to erase personal data and the right to obtain a copy of them</u>, including performing tasks related to the public interest as per legal requirements.	Exceptions: Limitations on the right of access may apply in cases where the processing serves scientific purposes, provided it does not excessively intrude upon the individual's private life. Additionally, access rights may be curtailed to protect the data subjects or others (Article 35). Furthermore, the data subjects, their heirs, or legal guardian may demand the deletion of personal data if its collection or use breaches the provisions of this law (Article 40). 3- Right to object: The data subjects, their heirs, or legal guardian have the right to object to the processing of their personal data at any time for legitimate and substantial reasons that concern them directly. <u>Exception:</u> This right may not apply if the processing is mandated by law or arises from the nature of the obligation at hand (Article 42).
--	---	--	---	---

Exceptions: These rights do not extend to processing solely for artistic expression, professional journalism, within the constraints of relevant laws. 6- The right not to rely solely on automated processes to make a judicial or administrative decision that necessitates an assessment of human behavior (Article 86).			Fulfilling legal obligations or competent court orders, safeguarding the individual's vital interests, conducting scientific researches for public benefit, and gathering information for criminal investigation upon official requests from investigative authorities (Article 19)	
---	--	--	---	--

ANNEX 10: OBLIGATIONS OF THE PERSON RESPONSIBLE FOR PROCESSING (THE CONTROLLER OR THE SUPERVISOR) AND THE PROCESSOR OR HANDLER

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Obligations of the person responsible for the processing 1- Notification to individuals: he must provide individuals from whom personal data is collected with specific information outlined by law, including disclosing the identity of the person responsible for processing or their representative, detailing the purposes of data processing, specifying whether responses to inquiries are mandatory or voluntary, explaining the consequences of non-response, identifying recipients of the data, and informing individuals of their right to access and rectify the information, along with the available means to do so (Article 88).	Responsibilities of the Controller: 1. Implement technical and organizational measures to ensure and to be able to demonstrate that processing is performed lawfully. 2- Use processors providing sufficient guarantees (Article 28(1)). 3- Maintain a record of processing activities under their responsibility (Article 24). Responsibilities of the Processor (Article 28): 2- Processor shall not engage another processor without prior specific or general written certification of the controller. 3- Processing shall be governed by a contract which must include certain provisions including confidentiality.	Responsibilities of the data controller: 1- Establishment of the necessary codes and procedures: The data controller is responsible for establishing necessary codes and procedures for processing personal data (Article 13), and must also adhere to the codes and procedures specified by the Ministry of Transport, Communications, and Information Technology to ensure legal compliance (Article 15). 2- Prior notification of data subjects: Before initiating any data processing, the data controller must provide the data subjects with written notification detailing essential aspects such as the contact details of the person	Responsibilities of the Controller: 1- Adherence to specific controls governing design, alteration, or development of products, systems, and services related to personal data processing, along with taking appropriate measures to safeguard personal data. 2- Compliance with privacy protection policies (Article 8). 3- Identification and training of data protection persons responsible for safeguarding personal data, and raising their awareness on this matter. 4- Establishment of internal systems for receiving and handling complaints as well as receiving requests for data access, rectification, or deletion.	Responsibilities of the Data Controller: 1- Undertaking all necessary measures to preserve the security of personal data, preventing unauthorized alteration, damage, or access without the data subjects' consent (Article 18). 2- Entrusting some or all processing tasks to a third party under a data processing agreement after a thorough investigation of the selected person (Article 20). 3- Prior written notification to individuals from whom personal data will be collected, providing specific information such as the type of personal data to be processed, processing purposes, the mandatory or optional responses and the consequences of non-response, recipient identity or

2- Informing Data Subjects: The person responsible for processing must notify the data subjects about information not collected directly from them, explicitly stating the content of this data, the purposes of processing, and their right to object to the processing. <u>Exception:</u> This obligation is waived when the data subjects are aware of the information or when informing them is impossible or would require disproportionate effort compared to the benefits of processing (Article 89). 3- Considering the nature of the data and the associated risks, the responsible for the processing must take all necessary precautions to ensure the data security and safety. This involves preventing its alteration or damage and preventing unauthorized access (Article 93).	4- Where a processor engages another processor, the same data protection obligations as set out in the contract shall be imposed. Responsibilities of both Controller and Processor: They shall cooperate, on request, with the supervisory authority in the performance of its tasks (Article 31).	responsible for personal data protection, processing purposes, data source, a comprehensive and accurate description of processing procedures, disclosure extent, data subjects' rights, and any other pertinent information (Article 14). 3- Breaches notification: The data controller must notify the ministry and the data subject of any breaches compromising personal data including instances of destruction, alteration, disclosure, unauthorized access, or unlawful processing (Article 19). 4- The person responsible for data protection's appointment: The data controller is responsible for designating one. (Article 20). 5- Confidentiality of personal data: The data controller is obliged to maintain the confidentiality of personal data and refrain from disclosing it without the data subjects' prior consent (Article 21).	5- Utilization of proper technological means to facilitate individuals' exercise of their rights to access, review, and rectify their personal data directly. 6- Conducting comprehensive auditing and review operations to ensure compliance with personal data protection protocols (Article 11). 7- Prohibition of taking any decision or action that impedes the cross-border flow of personal data, except when data processing breaches the provisions of this law or poses significant harm to personal data or individual privacy (Article 15). 8- Notification of individuals with specific information, including the identity of the person responsible for the processing, legitimate processing purposes, comprehensive descriptions of processing activities and data disclosure practices, and any other pertinent information required for	access rights, data controller identity of the responsible for data processing and location, data subjects' rights, data retention period, summary of security measures, and potential data portability destinations (Article 31). Responsibilities of the handler: 1- Complying with legal mandates and abstaining from actions exceeding the scope authorized by the person responsible for the processing, while being equipped with the requisite and suitable technical resources for tasks completion (Article 20). 2- proactive rectifications, completions, modifications, updates, or deletions of cards in their possession upon discovering inaccuracies or deficiencies in included personal data, with notifications sent to the affected individuals and beneficiaries of the amendments made to personal data (Article 21).
---	--	---	--	--

		6- Prohibition of unlawful data portability: The data controller is prohibited from transferring unlawfully processed data or data harmful to data subjects (Article 23). Shared obligations of the controller and processor: 1- Compliance with specified codes and procedures: Both the data controller and processor must comply with the codes and procedures specified by the Ministry of Transport, Communications, and Information Technology to ensure legal compliance (Article 15). 2- Appointment of an external auditor to verify that personal data processing procedures comply with the law. The controller and processor are required to provide the ministry with a copy of the external auditor's report (Article 16). 3- Documentation retention: Both parties must retain documentation related	compliance with personal data processing regulations (Article 9). <u>Exception:</u> Provisions outlined in Article 9 and Article 15 are not binding in certain specified cases, such as those involving the protection of national security, public security, international relations, economic or financial interests of the state, and the prevention criminal activities or gathering of information related to them (Article 20). Shared responsibilities of the data controller and processor: 1- Implementing necessary precautions to protect personal data from loss, damage, alteration, disclosure, unauthorized access, or incidental or unlawful use. 2- The processor must notify the controller of any breaches of the aforementioned precautions or any risks threatening individuals'	3- Ensuring confidentiality of personal data and processed information by the person responsible for the processing, handler, their assistants, even after processing is completed or their status is terminated, except for data explicitly consented in writing by the data subject for disclosure or for cases stipulated by applicable laws (Article 23). 4- Notifying the authority upon the permanent cessation of processing activities (Article 24).
--	--	--	---	--

		to processing operations and provide with data and documents requested by the ministry deemed necessary for the exercise of its authority (Article 17 and Article 18).	personal data promptly upon becoming aware of them (Article 13). The controller then notifies the individual and the relevant authority of any breaches of previously established precautions if they could cause significant harm to the individuals and their data.	
--	--	--	---	--

ANNEX 11: THE AUTHORITY RESPONSIBLE FOR LAW ENFORCEMENT

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The Ministry of Economy and Trade	Independent Authority: 1- Each member state shall establish at least one authority to monitor the application of the regulation (Article 51(1)). 2- They shall be established by national law (Article 54(1)) 3- Requirement of independence (Article 52): Members of the authority shall be free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody (Article 52(2)). 4- The authority shall be able to choose its own staff (Article 52(5)). 5- Members are to be chosen with transparency (Article 53(1)). 6- The member state needs to ensure that each authority is equipped with the human, technical and financial resources, premises and infrastructure (Article 52(4)). 7- They are subject to financial control, but this cannot affect their independence (Article 52(6)). 8- Authority shall have the necessary competences to monitor the application of the regulation (Article 55(1)).	The Ministry of transportation, Communications and Information Technology	The Ministry of Transportation and Communication	The National Authority for Personal Data Protection is an entity established by law, endowed with legal personality and financial independence. The authority is composed of a president, selected among competent individuals in the field, and 14 members, including members from the House of Representatives and the Council of Advisors, along with delegates from ministries such as the Prime Minister's Office, Interior, National Defense, and the Ministry overseeing communication technologies. Additionally, it encompasses four judges, a researcher appointed by the Ministry of Scientific Researches, a physician from the Ministry of Public Health, a member from the High Authority for Human Rights and Fundamental Freedoms, and an expert in communication technologies. The president and members of the authority are appointed based on the recommendation of the Minister in charge of human rights (Chapter 79).

ANNEX 12: TASKS AND PREROGATIVES OF THE LAW ENFORCEMENT AUTHORITY

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The Ministry of Economy and Trade shall: 1- Receive certifications for the collection and processing of personal data (Article 95). 2- Publish a list of automated processing that have fulfilled licensing or certification procedures for processing (Article 98).	The independent authority shall: 1- Monitor and Enforce the application of the regulation. 2- Promote public awareness (especially among children). 3- Advise the national parliament, the government, and other institutions and bodies. 4- Promote the awareness of controllers and processors of their obligations. 5- Upon request, provide information to the data subject. 6- Handle complaints and investigate, and inform the complainant of the progress and the outcome. 7- Cooperate with other supervisory authorities. 8- Conduct investigations on the application of this Regulation.	The Ministry of Transport, Communications and Information Technology is responsible for: 1- Developing and endorsing codes and procedures related to the protection of personal data. 2- Issuing necessary codes and procedures for processing personal data and ensuring compliance by both controllers and processors. 3- Addressing and resolving notifications and complaints received. 4- Collaborating with relevant authorities responsible for personal data protection in other countries. 5- Offering guidance, assistance, and coordination to public administrations and individuals related to personal data protection matters.	The Ministry of Transport and Communications is tasked with the following duties: 1- Coordinating with relevant professional groups, associations, or other entities representing internet site monitors or operators to promote self-regulation, raise awareness regarding this law, and enhance training and educational programs. 2- Collaborating with organizations and associations focused on family affairs to bolster children's safety online. 3- Conducting researches, monitoring technology advancements relevant to the law's scope, and issuing reports or recommendations accordingly (Article 27).	The National Data Protection Authority is tasked with various responsibilities: 1- Granting licenses and receiving certifications for the processing or revoking personal data in accordance with the law. 2- Addressing complaints falling within its jurisdiction as defined by this law. 3- Establishing necessary guarantees and appropriate measures to protect personal data. 4- Accessing and inspecting personal data processing operations to verify them and gather necessary information for its tasks. 5- Providing opinions on all matters pertaining to the provisions of this law. 6- Developing code-of-conduct guidelines in the field of data protection.

	9- Monitor relevant developments, encourage, develop, and authorize the establishment of additional laws and regulations. 10- Accredited certification bodies. Issue certifications and approve criteria of certification (Article 58). 11- Where applicable, carry out a periodic review of certifications. 12- Keep internal records of infringements and of measures taken. 13- Fulfill any other tasks related to the protection of personal data (Article 57(4)).	6- Granting and revoking licenses of service providers entrusted with assessing and evaluating the compliance of controllers and processors with this law provisions. 7- Developing guidance models for the implementation of this data protection law. 8- Compiling periodic reports on its activities in the field of personal data protection and publishing them on its website. 9- Establishing a registry for controllers and processors who meet the legal requirements (Article 7).		7- Contributing to researches and studies related to its activities (Article 76). 8- Conducting necessary investigations, including hearing testimonies, inspecting processing sites (excluding residential premises), and informing the relevant public prosecutor of crimes discovered in the course of their work (Article 77). 9- The President and members of the authority are bounded to confidentiality obligations regarding personal data and information obtained during and beyond their tenure. 10- Submitting an annual report on its activities to the President of the Republic (Article 79).
--	--	---	--	---

ANNEX 13: PROCESSING DATA CERTIFICATION

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Anyone wishing to collect and process personal data is required to notify the Ministry of Economy and Trade under a duly authorized certification in return for a receipt (Article 95).	The GDPR specified the powers of the independent authority when it is decided to require a certificate to process data. These powers are: 1- To carry out a periodic review of certifications 2- To Accredit certification bodies. 3- To issue certifications and approve criteria of certification (Article 57 (4)). 4- To withdraw or withhold a certification (Article 58). 11- Where applicable, carry out a periodic review of certifications. 12- Keep internal records of infringements and of measures taken. 13- Fulfill any other tasks related to the protection of personal data (Article 57(4)).	A certification must be obtained from the Ministry of Transport, Communications and Information Technology for processing personal data related to genetic data, biometric data, health data, racial or ethnic origin, sexual life, political opinions, religious beliefs, criminal convictions, or security measures (Article 5).	Processing sensitive personal data is prohibited without obtaining prior certification from the relevant authority. Sensitive personal data encompasses information concerning racial origin, children, health or physical and mental condition, religious beliefs, marital relationships, and criminal offenses. The Minister may add other categories of sensitive personal data if their misuse or disclosure would cause serious harm to the individual (Article 16)	Each personal data processing operation is subject to prior certification deposited at the headquarters of the National Authority for Personal Data Protection. Failure of the authority to object to the processing of personal data within one month of the submission of the certification shall be deemed acceptance (Article 7).

Exceptions:

Lebanon	Tunisia
Exemptions from the requirement for processing certification include: 1- Processing conducted by public officials within the scope of their duties. 2- Non-profit associations holding records of their members and stakeholders within the scope of their natural and legal activities. 3- Processing related to maintaining specific records under legal or regulatory provisions for public disclosure, accessible to individuals with a legitimate interest. 4- Processing concerning students by educational institutions for educational or administrative purposes. 5- Processing concerning employees or members of commercial institutions, unions, associations, or freelancers, within the legal boundaries and needs of their respective activities. 6- Processing concerning customers and clients of commercial institutions, unions, associations, or freelancers, within the legal boundaries and needs of their activities. 7- Processing with the prior consent of the data subjects unless there is a legal impediment. 8- Certain processing activities or categories may be exempted from certification or licensing procedures if their implementation poses no risk to private life or personal freedoms, subject to a decree issued by the Council of Ministers upon the recommendation of the Ministers of Justice and Economy and Trade. 9- Processing activities specified in Law No. 140/99 aimed at safeguarding the confidentiality of communications carried out through any means of communication (Article 94).	Exemptions from processing certification are applicable in the following cases: 1- Processing of personal data related to the professional status of the employee by the employer, which is necessary for the proper work and organization (Article 16). 2- Processing conducted by public authorities (Article 54).

ANNEX 14: DATA PROCESSING LICENSING

Lebanon	Tunisia
1- License from the Ministers of National Defense, Interior and Municipalities, for processing personal data related to state's external and internal security. 2- License from the Minister of Justice for processing personal data related to criminal offenses and legal cases of all kinds. 3- License from the Minister of Health for processing personal data related to health conditions, genetic information, or sexual life of individuals (Article 97). 4- Processing, access, and rectification of personal data within ministries, public administrations, and institutions beyond their legal and regulatory framework are governed by this law and prior certification from the Council of Ministers, upon the recommendation of the relevant minister is mandatory (Article 104).	The National Data Protection Authority grants licenses for: 1- Processing personal data pertaining to racial or genetic origins, religious beliefs, political, philosophical, or trade union opinions (Article 14). 2- Transferring personal data in cases where explicit consent is not obtained from the data subjects, their heirs, or legal guardian: when such referral is essential for safeguarding their vital interests, conducting historical or scientific researches, or fulfilling contractual obligations in which the data subjects are involved. However, the referring entity must ensure adequate guarantees for safeguarding personal data and associated rights as specified by the Authority, and ensure that the data is not utilized for purposes beyond its intended scope (Article 47). 3- For personal data portability abroad (Article 52).

ANNEX 15: PUBLICATION OF CERTIFICATIONS AND LICENSES

Lebanon	Sultanate of Oman
The Ministry of Economy and Trade disseminates, notably on its website, a roster of automated processing that have met the necessary licensing or certification protocols as stipulated by law (Article 98).	The Ministry of Transport, Communications and Information Technology shall compile a registry of controllers and processors who meet the legal prerequisites (Article 7).

ANNEX 16: SUBMITTING COMPLAINTS

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
The data subjects have the right to appeal to the competent courts, in particular the judge of urgent matters, to ensure the exercise of their rights of access and rectification, and to compel the defendant to apply the provisions of the law (Article 102).	Complaints can be filed before the independent authority (Article 57 (4,1,f)). Individuals must be informed of their right to complain (Article 13.1.d).	The personal data subjects have the right to file a complaint with the Ministry of Transportation, Communications and Information Technology if they believe that the processing of their personal data breaches the law (Article 12).	The personal data subjects have the right to file a complaint with the competent administration. Individual may submit a complaint to the competent administrative unit at the Ministry of Transport and Communications in case of breaching the provisions of this Law and the regulation issued for its implementation (Article 26).	The National Authority for the Protection of Personal Data receives complaints submitted to it within the framework of the jurisdiction assigned to it under this law (Article 76).

ANNEX 17: SANCTIONS

Lebanon	European Union	Sultanate of Oman	Qatar	Tunisia
Incarceration and fines The sanction varies according to the severity and nature of the breach (Articles 106 to 109).	1- Up to 4% of their global annual revenue or €20 million, whichever is higher (Article 83.5). 2- Affected individuals can seek compensation for damages (Article 82).	- Fines - Seizure of tools utilized in the commission of the offense. The fines' amount varies according to the severity and nature of the breach (Article 24 to Article 32).	- Fines The fines' amount varies according to the severity and nature of the breach (Article 23 to Article 25).	Incarceration and fines The sanction varies according to the severity and nature of the breach - Revocation of license or processing suspension <u>as per court order</u> . - Reconciliation through penal mediation for certain committed crimes. (From Chapter 86 to 103).

ANNEX 18: MEASURES

European Union	Sultanate of Oman
The independent authority can: 1- issue warnings and reprimands. 2- order the controller or the processor to comply with the data subject's requests to exercise his or her rights and comply with the regulations. 3- order the controller to communicate a personal data breach to the data subject. 4- impose a temporary or definitive limitation including a ban on processing. 5- order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed. 6- withdraw or withhold a certification. 7- impose an administrative fine. 8- to order the suspension of data flows to a recipient in a third country or to an international organization (Article 58).	The Ministry of Transport, Communications and Information Technology may take any of the following actions: 1- Issuing warnings to the controller or processor found to be breaching this law. 2- Mandating the rectification and deletion of personal data processed in violation of the provisions of the law. 3- Temporarily or permanently suspending the processing of personal data. 4- Temporarily or permanently halting the portability of personal data to another country or international organization.

ANNEX 19: SPECIAL PROVISIONS FOR PROCESSING SPECIFIC DATA CATEGORIES

European Union	Qatar	Tunisia
The GRDP has underlined special provisions for processing specific data categories which include the following: 1- Processing and freedom of expression and information (Article 85). 2- Processing and public access to official documents (Article 86). 3- Processing of the national identification number (Article 87). 4- Processing in the context of employment (Article 88). 3- Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89). 4- Obligations of secrecy (Article 90). 5- Existing data protection rules of churches and religious associations (Article 91).	1- The law has introduced a special section to personal data of a sensitive nature, including data pertaining to racial origin, children, health or physical and mental condition, religious beliefs, marital relationships, and criminal offenses. Additionally, the minister may add other data categories if their misuse or disclosure could seriously harm individuals. The minister is also empowered to impose additional safeguards to protect sensitive personal data (Article 16). 2- The law has established special provisions regarding the processing of personal data of children by websites targeting them (Article 17).	The law has allocated different sections to regulate special data processing: 1- Processing of personal data of public officials (Chapter 53 to 61). 2- Processing of personal data related to health matters (Chapter 62 to 65). 3- Processing of personal data for scientific research purposes (Chapter 66 to 68). 4- Processing of personal data for visual surveillance activities (Chapter 69 to 74).

You are free to share, copy, distribute, and transmit this work under the conditions that you attribute the work to the Samir Kassir Foundation and SEEDS for Legal Initiatives but without suggesting in any way that the Samir Kassir Foundation and/or SEEDS for Legal Initiatives endorse(s) you or your use of the work. You may not use this work for commercial purposes.

In collaboration
with



UNDEF



The United Nations
Democracy Fund

SIGRID RAUSING TRUST

The contents of this report reflect the views of the Samir Kassir Foundation and SEEDS for Legal Initiatives and can in no way be taken to reflect the views of the United Nations Democracy Fund.

Design: Marc Rechdane

February 2024 – Samir Kassir Foundation

Address: Riverside Bloc C
6th floor, Charles Helou Street
Sin el-Fil, Metn – Lebanon

Tel: + 961 1 499012
info@skeyesmedia.org
skeyesmedia.org