



CyberSouth
Cooperation on cybercrime
in the Southern Neighbourhood

version 21 July 2020

Report of a study
on the conformity of personal data provisions with
Convention 108+ in Algeria, Jordan, Lebanon,
Morocco and Tunisia

Prepared within the framework of the
CyberSouth Project

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Introduction	3
Lebanon- law n°81-2018	4
Object and purpose (Article 1 of Convention 108+)	4
Definitions (Article 2 of Convention 108+)	4
Scope (Article 3 of Convention 108+).....	4
Legitimacy of data processing and quality of data (Article 5 of Convention 108+)	4
Special categories of data (Article 6 of Convention 108+)	5
Data security (Article 7.1 of Convention108+).....	5
Data breach notification (Article 7.2 of Convention108+)	5
Transparency of processing (Article 8 of Convention108+)	5
Rights of the data subject (Article 9 of Convention 108+)	6
Additional obligations (Article 10 of Convention108+).....	6
Sanctions and remedies (Article 12 of Convention108+)	7
Trans-border flows of personal data (Article 14 of Convention 108+)	7
Supervisory authorities (Article 15 of Convention 108+)	7
Conclusion & Recommendations	7

Introduction

CyberSouth program is a joint project of the European Union and the Council of Europe that aims to help Southern Neighbourhood countries to strengthen their legislation and institutional capacities on cybercrime.

Given the strong relationship between cybercrime and the use of personal data, the Council of Europe decided to conduct this study on the conformity of personal data provisions with the modernized Convention 108 (the Convention) in Algeria, Jordan, Lebanon, Morocco and Tunisia.

Apart from Jordan, which has prepared a draft bill, all other countries concerned by this study have enacted domestic laws on personal data processing. Tunisia and Morocco are a step ahead in this field, since they both have operational supervisory authorities and are parties to Convention 108 and its additional protocol, respectively, since November 2017 and September 2019.

For the purpose of this study and due to the deadline set for it (two weeks), the following texts were examined in light of the provisions of Convention 108+:

- **Algeria**: the Constitution of 2016 and the law n°18-07 of 10 June 2018 on the protection of individuals with regard to the processing of personal data (***French versions***).
- **Jordan**: the Constitution of 2011 and the 2020 Personal Data Protection draft Bill, which was submitted for public consultation on 23 January, 2020, on the website of the Jordanian Bureau of Legislation and Opinion (***Arabic versions***).
- **Lebanon**: Book V of law No. 81 of 10 October 2018 on Electronic Transactions and Personal Data (***Arabic version***).
- **Morocco**: the Constitution of 2011, law n°09-08 on the protection of individuals with regard to the processing of personal data and its implementing decree (***French versions***).
- **Tunisia**: the Constitution of 2014, the organic law n° 63 of 27 July 2004 on the protection of personal data and the decree n° 3003 of 27 November 2007, fixing the operating procedures of the national personal data protection authority (***French versions***).

Lebanon- law n°81-2018

Object and purpose (Article 1 of Convention 108+)

1. Article 2 of the law provides that "information technology is at the service of all people, provided it does not affect their individual identity, rights, privacy or individual and public freedoms". It will be useful to include an article that explains the purpose of the fifth section of the law relating to personal data processing and ideally align it with that of the Convention.

Definitions (Article 2 of Convention 108+)

2. The first article of the law uses definitions equivalent to those of the Convention for the concepts: "**Personal data**", "**Data processing**", "**Data subject**", "**Controller**"," **Recipient** ". The law did not define, however, the terms "**Processor**" and "**non-automated processing**".

Scope (Article 3 of Convention 108+)

3. Provisions of section V of the Lebanese law, relating to the protection of personal data, concerns automated and non-automated processing (art.85). Since the term "**non-automated processing**" has not been defined, like in the Convention, as processing carried out on structured data, the scope of the law covers all manual processing and is therefore broader than that of the Convention.
4. Like the convention, the law excludes from its scope all processing relating to personal activities, operated for the exclusive needs of individuals.
5. Article 85 is silent concerning the application of the law's provisions to public bodies. Article 104 specifies, though, that personal data processing carried out by these entities, outside of their attributions, fall within the scope of the law. It can be inferred consequently that processing performed by public bodies to perform their habitual functions is excluded from the Scope of the law!

Legitimacy of data processing and quality of data (Article 5 of Convention 108+)

- Proportionality and Data minimization (art 5.1 et 5.4.c)
6. The law does not contain any explicit provision regarding the proportionality of personal data processing. Its Article 85 establishes, though, that data collected must be "adequate and not excessive with regard to the declared purposes", which establishes the data minimization principal.
- Consent (art 5.2)
7. There is no provision in the law stating that data subject's consent is a prerequisite to the processing of his data. Article 92, for its part, prevents data subjects from objecting to processing carried out on the basis of their consent. This may infer that Controllers can collect and process personal data without obtaining data subject's consent, which is contrary to the spirit of the Convention (Articles 5.2 and 5.3).
- Transparency and fairness (art. 5.4.a)
8. Fairness of processing is mentioned explicitly in Article 87 of the law "data is collected fairly ..."; while the transparency of processing is ensured by the right to information, enshrined in Article 88, as well as by the list of processing of personal data that the Ministry of Economy and Commerce must publish on its website (art.98).
- Purpose limitation (art. 5.4.b)
9. The purpose limitation principal is explicitly cited in Article 87 of the law "data is collected fairly for legitimate, determined and explicit purposes. It is not possible to process them subsequently for

purposes incompatible with those declared, except for statistical, historical or scientific research purposes”.

- Data accuracy (art 5.4.d)

10. Data accuracy is provided for in Article 87 of the law, which states that "Data must be (...) accurate, complete and properly updated”.

- Storage limitation (art 5.4.e)

11. Storage limitation is ensured by Article 90 of the law, which stipulates, "Personal data can only be legitimately stored during the period indicated in the declaration or the decision authorizing the processing". Yet, to be conform to international standards, data retention period should not exceed that necessary to achieve the processing’s purposes.

Special categories of data (Article 6 of Convention 108+)

12. Article 6 of the Convention enumerates specific categories of data whose processing requires appropriate guarantees. Among them, biometric data and that revealing racial or ethnic origin, political opinions, union membership and religious beliefs are not cited in the Lebanese law.

13. Article 91 of the law specifies the cases where the processing of personal data revealing health status, genetic identity or sexual life is allowed. One of these cases is when "the data subject made this information public", which raises some questions, because making data public shouldn’t be considered as a valid consent to all the processing they may undergo.

14. The processing of personal data relating to "criminal offenses and legal proceedings" is subject to the authorization of the Minister of Justice, whereas that revealing "health status, genetic identity or sexual life" requires the authorization of the Minister of Health (Article 97 of the law).

Data security (Article 7.1 of Convention 108+)

15. Article 93 provides that "The controller must take all measures, depending on the nature of the data and the risks associated with their processing, to guarantee data security and avoid their distortion, damage or that they are accessible to unauthorized persons. "

Data breach notification (Article 7.2 of Convention 108+)

16. There is no provision in the Lebanese law regarding data breach notification.

Transparency of processing (Article 8 of Convention 108+)

17. Transparency of processing is ensured by Articles 88 and 89 of the law, which establishes the right to information to data subjects. However, it does not explicitly state that the controller must communicate this information, as required by Article 8 of the Convention:

- habitual residence or establishment of the controller,
- the legal basis for the processing,
- the categories of personal data processed and
- other data subject’s rights, apart from rights to access and rectify data, and the means to facilitate them.

18. Provisions of Article 89 regarding right to information when data is not collected directly from the data subject are conform to those of Articles 8.2 and 8.3 of the Convention "Art 89. When the information is not collected directly from the data subject, the controller must inform the latter personally and clearly of the content of this information, the purposes of the processing and his right to object to the processing.

This obligation doesn’t apply when the data subject is informed thereof, or his information proves to be impossible or requires disproportionate effort with regard to the processing’s benefits”.

Rights of the data subject (Article 9 of Convention 108+)

- Protection against automated decision-making (art 9.a & 9.c)

19. The second paragraph of Article 86 protects data subjects against judicial or administrative automated decisions "Art 86. No judicial or administrative decision, requiring the evaluation of human behavior, can be based exclusively on automated processing of personal data aimed at determining the characteristics of the person or evaluating certain aspects of his personality." On the same subject, Article 99 specifies that the data subject, or one of his heirs, may request additional information about the "nature of the processing". Article 86, for its part, grants to the data subject the right to object to "analysis, concerning him, used in automated processing". This protection should be extended to other automated decisions that may have significant effect on data subjects, as requested by Article 9.a of the Convention.

- Right to access (art 9.b)

20. Articles 86, 99, 100 and 104 of the law establish the right to access for data subjects. There is, though, a derogation to this right concerning health data or when the controller is a public body that processes data to perform its mission. Such exceptions are not conforming to the Convention, especially its Article 11 that specifies exceptions to certain provisions that apply under specific conditions.

21. The Convention requires that the controller meets data subjects' requests to access their data, without excessive delays or expenses. The law has remained silent regarding the delays and allowed controllers to collect fees not exceeding the cost of the photocopies issued.

- Right to object (art 9.d)

22. Right to object is enshrined in Articles 86 and 92 of the law. Nevertheless, the second exception of Article 86, discarding this right if the data subject had already given his consent to the processing, deprives this important right from its essence.

- Right to rectification (art 9.e)

23. Right to rectification is provided for in Article 101, for both data subjects and their heirs. According to the same article, the controller must meet the corresponding requests, free of charge and within ten days after having received them. This period may be considered as not excessive, in accordance with the Convention, except when the prejudice suffered by the data subject requires a shorter response time.

- Remedies (art 9.f) and access to the assistance of a supervisory authority (art 9.g)

24. Article 102 establishes remedies to the benefit of the data subject "art 102. Data subject, or his heirs, has the right to seize the competent courts, to guarantee the rights of access, rectification or to report the obligation to apply the provisions of this section with regard to personal data".

25. Data subjects do not have, nevertheless, access to the assistance of a supervisory authority, as provided for in Article 9.g of the Convention.

Additional obligations (Article 10 of Convention 108+)

26. The controller must either obtain the authorization of the competent ministry or file a declaration stating that personal data will be processed in compliance with the law's provisions (art.96). There isn't, however, any explicit provision obliging the controller or the processor to demonstrate that the processing carried out complies with the law (art.10.1 of the Convention), nor to take additional measures to protect data under their control, such as privacy impact assessment or privacy by design, as suggested by Articles 10.2 and 10.3 of the Convention.

Sanctions and remedies (Article 12 of Convention 108+)

27. According to Article 102 of the law, any grievant can seize the competent court. For its part, chapter V, relating to sanctions, establishes that offenders risk a fine of up to 30 million LBP (18 000 €; 1€ = 1,691.9223 LBP on 03 June 2020) and a maximum 3 years imprisonment. These sanctions may be increased by a third or half, in case of recurrence (art 108. of the law).

Trans-border flows of personal data (Article 14 of Convention 108+)

28. Apart from Article 96 that states that the processing's declaration filed to the Ministry of Economy and Finance must include "If necessary, the transfer of personal data to another country", there is no provision in the law regulating data transfers, as required by Article 14 of the Convention.

Supervisory authorities (Article 15 of Convention 108+)

29. Contrary to the provisions of Article 15 of the Convention, the Lebanese law does not provide for the creation of a supervisory authority that is responsible for the enforcement of its provisions. Instead, it entrusts the Ministry of Economy and Finance to centralize and maintain the list of declarations and authorizations relating to the processing of personal data and each Ministry to authorize processing associated with its activity.

Conclusion & Recommendations

The Lebanese law n° 81 of October 10, 2018, relating to electronic transactions and personal data, has provided for important provisions, such as those establishing the conditions of legitimacy of processing and data subject's rights. Nonetheless, it lacks some fundamental pillars that are essential to any efficient system regulating personal data processing.

Therefore, it is highly recommended to consider the following adjustments:

- Suppress derogations granted to public bodies regarding the processing of personal data and ensure that they do respect the same rules as the private entities.
- Provide for an independent authority that is responsible for ensuring compliance with the law's provisions and empower it with the missions enumerated in Article 15 of the Convention.
- Establish appropriate safeguards to trans-border data flow in order to facilitate free movement of personal data, without compromising data subject's fundamental rights.
- Increase the amounts of the fines to make them deterrent, for example by indexing them to the annual turnover of the controller.
- Establish additional obligations to controllers and processors, such as, conducting privacy impact assessment, taking measures to protect personal data at all stages of the processing, notifying serious data breaches and being able to demonstrate, at any time, that processing of personal data under their control is compliant to the law's provisions.
- Provide for appropriate protection to all special categories of data, enumerated in Article 6 of the Convention, by requiring additional guarantees, complementing those of the Convention when processing these categories of information.
- Review exceptions to data subject's rights to align them with those provided for in Article 11 of the Convention.