

Privacy Violated: Tunisian ISPs' Abuse of Personal User Information

JULY 2020






TABLE OF CONTENTS

I.	Executive Summary	4
II.	Introduction	5
III.	Study Methodology	7
IV.	Telecommunication and Internet Service Providers	8
V.	The Legal Framework in Tunisia	9
VI.	Privacy Policy	13
VII.	Findings	15
VIII.	Conclusions	21
IX.	Recommendations	23



I. Executive Summary

An analysis by [Access Now](#) and [ImpACT International for Human Rights Policies](#), in which 11 questions were posed to assess the privacy policies of seven internet service providers (ISP) in Tunisia, found that the vast majority fail to shield customers' personal information, violating basic principles of customer data protection.

The analysis showed that the main ISP companies in Tunisia, including Tunisie Telecom, Ooredoo, TopNet, GlobalNet, Hexabyte Tunisie, and BEE, are collecting often intrusive user information, without prominently disclosing that fact or explaining how the data will be used. Only one company, Orange Tunisia, complies with all requirements laid out in Article 4 of the Organic Law No. -2004 63. However, in practice, the company failed to comply with the legal text of the data protection law as seen on August 2018 ,31, when the company was accused of data exploitation through the misuse of its customers' data.

In response, Access Now and ImpACT International for Human Rights Policies call on the Tunisian government to adopt a new data protection law that prioritizes human rights in Tunisia and ensures the Council of Europe's Convention No. 108 on data protection—to which Tunisia is a 2007 signatory—is fully and effectively implemented. Existing domestic data-protection laws must be revised to adhere to the best practices outlined in the convention.

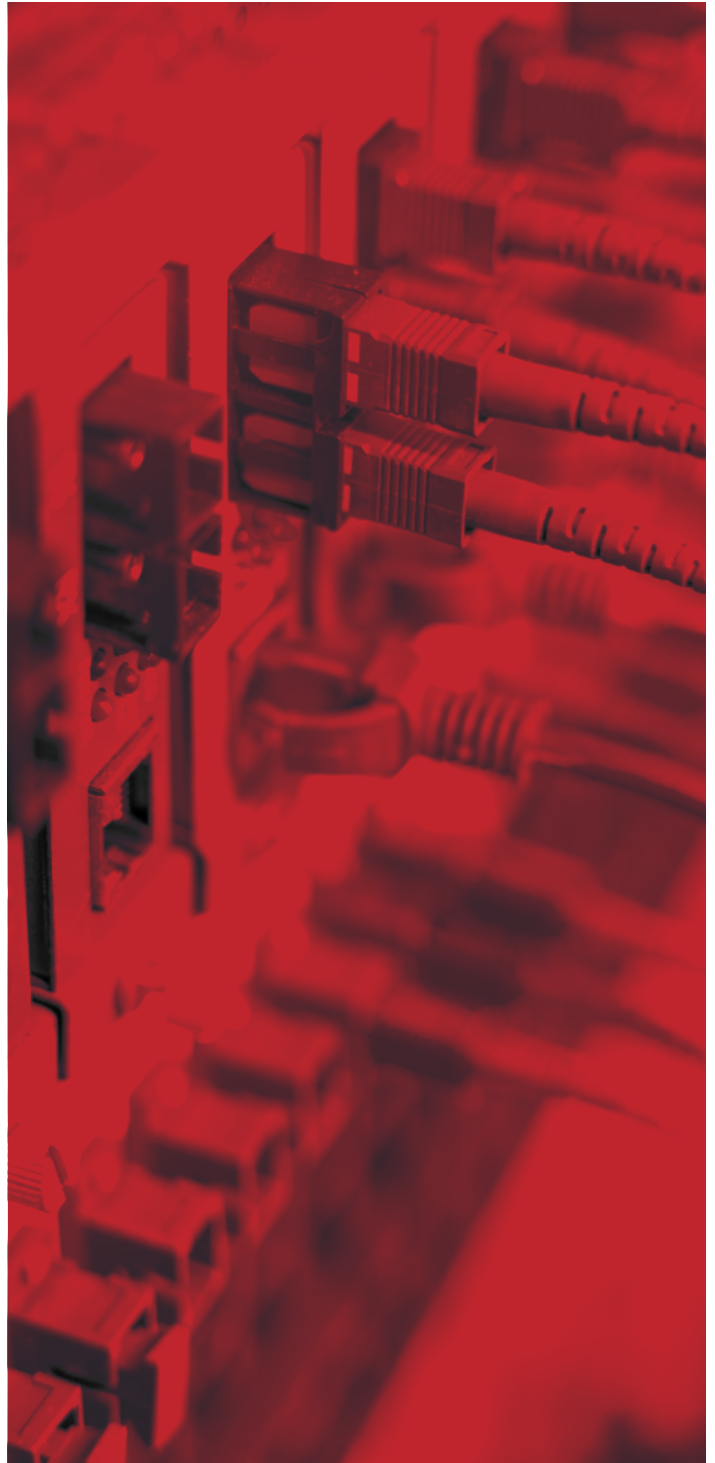
II. Introduction

This study looks into the practices of ISPs in Tunisia and their online privacy policies to evaluate how they protect the personal data of their users, hoping that it will lead to improved privacy policies and practices across local industries.

Tunisia has one of the most developed telecommunications infrastructures in North Africa, with broadband prices among the lowest on the continent. Internet access is available throughout the country via a fiber-optic backbone, with international service assured through submarine cables and both terrestrial and satellite links. Tunisia's international bandwidth reaches 430 Gbps. Its eight million internet users represent %67 of the population⁽¹⁾.

A brief description of each ISP in Tunisia is provided later in this report.

Tunisia has legislation in place designed to protect the personal information of its citizens through the Organic Law No. 63-2004. It defines personal data



1 Internetworldstats.com. 2020. Africa Internet Users, 2020 Population And Facebook Statistics. [online] Available at: <<https://www.internetworldstats.com/stats1.htm>> [Accessed 15 July 2020].

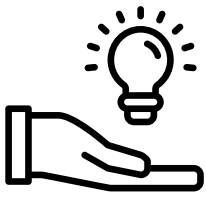
and outlines the responsibility of service providers and their partners towards customers in protecting this data. A 2013 analysis conducted by Article 19, however, concluded that the need for regulatory reform in Tunisia “is overwhelming. Indeed, the restrictions imposed on internet usage have gone backwards due to the deactivation of censoring mechanisms and the inability of the governing body exercising control over the internet.”⁽¹⁾ Many organizations are also calling for the country to urgently adopt a comprehensive data protection law to improve and complement existing laws and to be in line with international standards. ⁽²⁾



Access Now and ImpACT International for Human Rights Policies are conducting a series of analyses of ISP policies and practices in the Arab world. In this study, we examine seven ISPs and their privacy policies, as well as the legal framework in Tunisia, and propose recommendations on the key steps and measures that the Tunisian government and private companies have to consider to ensure that the right to privacy of Tunisian citizens is protected and respected.

1 2013. Tunisia: Background Paper On Internet Regulation. [online] Available at: <<https://www.refworld.org/pdfid/51dc0ef54.pdf>> [Accessed 15 July 2020].

2 Access Now. 2020. As Elections Approach, Tunisia Must Ensure Protection Of Personal Data - Access Now. [online] Available at: <<https://www.accessnow.org/tunisia-protecting-personal-data-during-elections-is-at-stake/>> [Accessed 25 June 2020].



III. Study Methodology

There are 11 ISPs operating in Tunisia – the seven ISPs we examined in this study are Tunisie Telecom, Ooredoo, TopNet, Orange Tunisia, GlobalNet, Hexabyte Tunisie, and BEE. These ISPs have the largest market share and are the main private operators in Tunisia. ImpACT International and Access Now reviewed and compared the privacy policies published on their websites, in light of the Organic Act No. -2004 63 of July 2004 ,27 on the protection of personal data, which states that “everyone has the right to the protection of personal data related to his privacy” and that “the processing of personal data shall respect transparency, fairness, and the respect of human dignity.”⁽¹⁾



1 Data Protection Act n°63-2004 of July 27th 2004 on the protection of personal data, Article 1: http://www.inpdp.nat.tn/Receuil_2019.pdf

IV. Telecommunication and Internet Service Providers

Tunisia is a well-developed market for telecom products and services. The penetration rate for telephones (both landlines and mobile) reached %138.8 in 2018. With over 14.8 million such lines, Tunisia enjoys one of the highest levels of mobile phone subscriptions in Africa. Of the estimated eight million internet subscribers, about %81 go online using a smartphone.⁽¹⁾

The cellular market opened to foreign competition in the early 2000s. Below are the main telecommunication and internet companies in Tunisia.

ISP	Year Opened	Parent Company	Other Notes
Tunisie Telecom	1995	n/a	Owns %60 of Go Malta, purchased from Emirati EIT in 2016
Ooredoo	2002	Ooredoo Group	Formerly known as Tunisiana
TOPNET	2001	Tunisie Telecom	n/a
Orange Tunisia	2003	Orange	n/a
GlobalNet	1997	Standard Sharing Software	n/a
Hexabyte Tunisie	2001	n/a	n/a
BEE	2019	n/a	n/a

¹ Export.gov. 2019. Tunisia – Telecommunications Equipment/Services. [online] Available at: <<https://www.export.gov/apex/article2?id=Tunisia-Telecommunications-Equipment-Services>> [Accessed 15 July 2020].

V. The Legal Framework in Tunisia



Tunisia was once a pioneering country in the Middle East and North Africa region in addressing privacy and personal data protection. Initially, these new rights were first recognized in the 2002 Constitution, when there were no privacy laws and regulations in any country across the region. Two years later, and prior to hosting the World Summit on the Information Society (WSIS) of 2005 in Tunisia, the Organic Act No. 63-2004 on data protection was born.

At first glance, the 2004 law appears to provide Tunisian citizens a basic level of protection; it grants rights to individuals whose data are collected by commercial enterprises and sets out the obligations of the responsible companies and institutions.

Nevertheless, the law contains numerous deficiencies. For instance, the law carves out exceptions for public entities such as the police, higher-education institutions, and courts from the obligations set forth in the law. Yet they process the largest

proportion of personal data, and, as a result, individuals' right to informed consent is severely limited. Moreover, statistics collected by the Independent Authority on Data Protection through 2017 show that the enforcement of the law differs significantly between actors.⁽¹⁾

The law also does not tackle key concepts such as “sensitive information,” for which different sets of rules should be applied when processing special categories of data. Data concerning a person's sex life or sexual orientation, for example, is not considered part of personal sensitive data.

The current law additionally puts the National Authority for the Protection of Personal Data (INPDP) in charge of oversight and enforcement. However, the independent authority began operation in 2009, more than six years after the institutionalization of the right to privacy and five years after the creation of the law. This, in turn, discloses the lack of political will to establish a decent and solid system for protecting personal data. What is even more worrisome is that, to date, no judicial rulings have been issued to prevent violations of personal data, which generates a sense of impunity and lack of accountability and mostly leads to a further invasion of privacy.

As a result, until 2015, data processors such as private companies were rarely engaging with the INPDP to declare their own processing in accordance with the law. Therefore, the application of the 2004 Organic Act has been more exceptional than systematic for years.

1 Activity Report Of The National Authority For The Protection Of Personal Data 2017-2009. [online] Available at: <http://www.inpdp.nat.tn/Rapport_2017-2009.pdf> [Accessed 23 June 2020].

Need for Urgent Privacy Reform

Following the 2011 fall of Ben Ali's regime and the establishment of the second republic three years later, a new constitution has been adopted. The Constitution of 2014 establishes human rights as a supreme guiding principle and codifies the right to privacy under Article 24, which stipulates that the state is responsible for "protect[ing] the right to privacy and inviolability of the home, and the confidentiality of correspondence, communications, and personal information."⁽¹⁾

Tunisia also ratified the International Covenant on Civil and Political Rights (ICCPR) in 1969. Article 17 of the ICCPR states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."⁽²⁾ The U.N. Human Rights Council has noted that states party to the ICCPR are obliged to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."⁽³⁾

On November 2017, Tunisia became the 51st member state to sign onto the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The country has also ratified the protocol amending the Convention.

A few months later, in March 2018, Tunisia introduced a new draft law on the protection of personal data. The modified bill is particularly designed to follow the lead of the European Union General Data Protection Regulation (GDPR) and would extend protection requirements to non-Tunisian processors of personal data in

1 2014. Tunisia's Constitution of 2014. [online] Available at: <https://www.constituteproject.org/constitution/Tunisia_2014.pdf> [Accessed 16 July 2020].

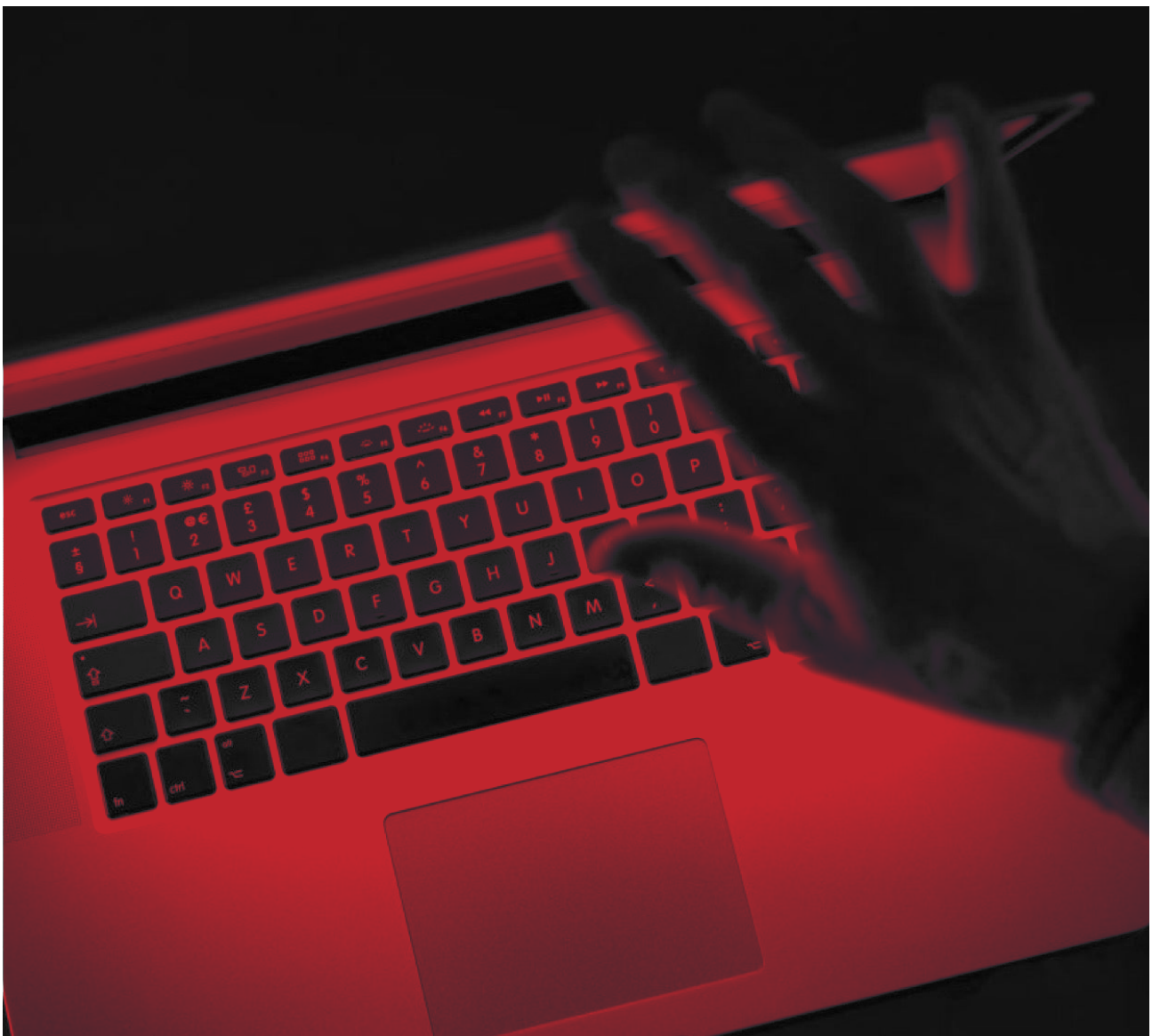
2 International Covenant on Civil and Political Rights (ICCPR): <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

3 Ibid. Article 2, ICCPR.

the country. In addition, it expands the concept of personal data to include email address, IP address, GPS coordinate, biometric, and genetic data. The amended bill also proposes the appointment of data protection officers within the various institutions charged with handling and protecting personal data.

Given that the current law in force has been adopted in the context of the authoritarian dictatorship of Ben Ali, it is critically important to reform and revisit the legal framework to bring it into line with the new Tunisian Constitution.

While Tunisia continues to aspire for political and legal reforms as a democratic state with a government both accountable and committed to the rule of law, it is crucial to remedy issues related to privacy and data protection.



VI. Privacy Policy

This study focuses on whether Tunisian ISPs have adopted and published explicit privacy policies that state the types of personal customer data collected, the use to which they are put, and the rights of customers to compensation if those provisions are violated. We also evaluated whether these policies are easily accessed by customers. Note that we relied on public disclosure via the company's websites for our information. Eleven questions were posed to explore 11 specific aspects of corporate privacy policies:

1. Is it easy to find on the company's website and written in terms easy for a layperson to understand?
2. Does the policy include an explicit and clear list of the types of personal information collected from customers?
3. Is there clear notice of any other parties that have access to this personal information and for what purpose?
4. Are users notified that by subscribing/purchasing, they agree to share the listed personal information with the disclosed parties?
5. Is there a clear statement regarding the extent to which the ISP is responsible for protecting customers' personal information?
6. Is there a disclosure of customers' rights to compensation if their personal information is stolen, leaked, or used for other purposes?
7. If any third parties are given access to customers' personal information, what is the extent of their liability in the case of any loss or misuse of personal information?
8. For how long does the ISP retain customers' personal information?

9. Does the ISP mention that the customer benefits from the Organic Act No. 63-2004 on the protection of personal data?

10. Is the legal liability of third parties clearly explained, in the case of loss, breach, or misuse of personal information?

11. Does the ISP mention that the customer benefits from the Organic Act No. 63-2004 on the protection of personal data?

8. For how long does the ISP retain customers' personal information?

9. Does the ISP mention that the customer benefits from the Organic Act No. 63-2004 on the protection of personal data?

10. Is the legal liability of third parties clearly explained, in the case of loss, breach, or misuse of personal information?

11. Does the ISP mention that the customer benefits from the Organic Act No. 63-2004 on the protection of personal data?

Links to the companies' websites and privacy policies are below:

Company Name	Company Website	Privacy Policy Link
Tunisie Telecom	https://www.tunisietelecom.tn/Fr	https://www.tunisietelecom.tn/Fr/acces-information/cadre-juridique
Ooredoo	http://www.ooredoo.tn/particuliers	http://www.ooredoo.tn/institutionnel/Donnees-Personnelles
Topnet	https://www.topnet.tn	https://www.topnet.tn/privacy-policy.pdf
Orange Tunisia	https://www.orange.tn	https://www.orange.tn/donnees-personnelles
Globalnet	https://www.gnet.tn	No privacy policy available
HexaByte Tunisie	http://www.made-in-tunisia.net/vitrine/index.php	No privacy policy available
BEE	https://bee.net.tn/	No privacy policy available

VII. Findings



Below are the specific questions and answers obtained from company websites.



Q1. Is it easy to find the privacy policy on the company's website?

Tunisie
Telecom

Ooredoo

Topnet

No.

Yes

Yes

There is a link to the legal framework but no clear statement that, "As a customer using a Tunisie Telecom service, you benefit from Organic Act No. 63-2004, dated 27 July 2004, which protects personal data."

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes

No privacy policy found.

No privacy policy found.

No privacy policy found.



Does the privacy policy include an explicit and clear description of the personal information collected?

Tunisie
Telecom

Ooredoo

Topnet

No

No

No.

It is only stated that, "We may require you to provide us with certain personally identifiable information."

Orange
Tunisia

Globalnet

HexaByte
Tunisie

Huawei
Tunisia

Yes.

as defined in Article
4 of Organic Act No.
63-2004.

No

No

No



Is there a clear definition or statement of where and when personal information is used and for what purposes?

Tunisie
Telecom

Ooredoo

Topnet

No

Yes

Yes

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes

as defined in Article 4 of Organic
Act No. 63-2004.

No

No

No



Is there a statement that notifies subscribers that they agree to share their personal information with other parties upon purchasing or subscribing to a product or service?

Tunisie
Telecom

Ooredoo

Topnet

No

Yes

Yes

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

as defined in Article
4 of Organic Act No.
63-2004.

No

No

No



Is there a clear statement of the ISP's responsibility for securing and protecting customers' personal information?

Tunisie
Telecom

Ooredoo

Topnet

No

Yes

Yes

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

as defined in Article
4 of Organic Act No.
63-2004.

No

No

No



Does the privacy policy provide a definition of customers' rights to compensation if their personal information is stolen, disseminated or used for purposes other than those mentioned?

Tunisie
Telecom

Ooredoo

Topnet

No

Yes

NO

It states: "Clients may apply to the national body for the protection of personal data for any dispute relating to the exercise of their rights in accordance with the provisions of the aforementioned law."

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

No

No

No

as defined in Article 4 of
Organic Act No. 63-2004.



Is there a clear definition of the other parties that may receive customers' personal information?

Tunisie
Telecom

Ooredoo

Topnet

No

No

Yes

It states: "We want to inform users of this service that these third parties have access to your personal information."

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

No

No

No

as defined in Article 4 of
Organic Act No. 63-2004.



Is there a clear definition or statement about the situations in which personal information is revealed to or shared with other parties?

Tunisie
Telecom

Ooredoo

Topnet

No

No

Yes

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

as defined in Article
4 of Organic Act No.
63-2004.

No

No

No



Is the legal liability of third parties clearly explained, in the case of loss, breach or misuse of personal information?

Tunisie
Telecom

Ooredoo

Topnet

No

No

No

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

as defined in Article
4 of Organic Act No.
63-2004.

No

No

No



For how long does the ISP retain customers' personal information?

Tunisie
Telecom

Ooredoo

Topnet

Not specified

Not specified

Not specified

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

Not specified

Not specified

Not specified

"The data controller and the subcontractor shall rectify, complete, modify, update or delete personal data from data files if they know of any inaccuracy or insufficiency in this data. In this case, the data controller and the subcontractor must inform the data subject and the data beneficiary of every modification made to personal data... Notification shall be done within two months from the date of modification, by registered letter with acknowledgement on receipt, or by any other means that leave a written trace."



Does the ISP mention that the customer benefits from the Organic Act No. 63-2004 on the protection of personal data?

Tunisie
Telecom

Ooredoo

Topnet

No

No

No

Orange
Tunisia

Globalnet

HexaByte
Tunisie

BEE

Yes.

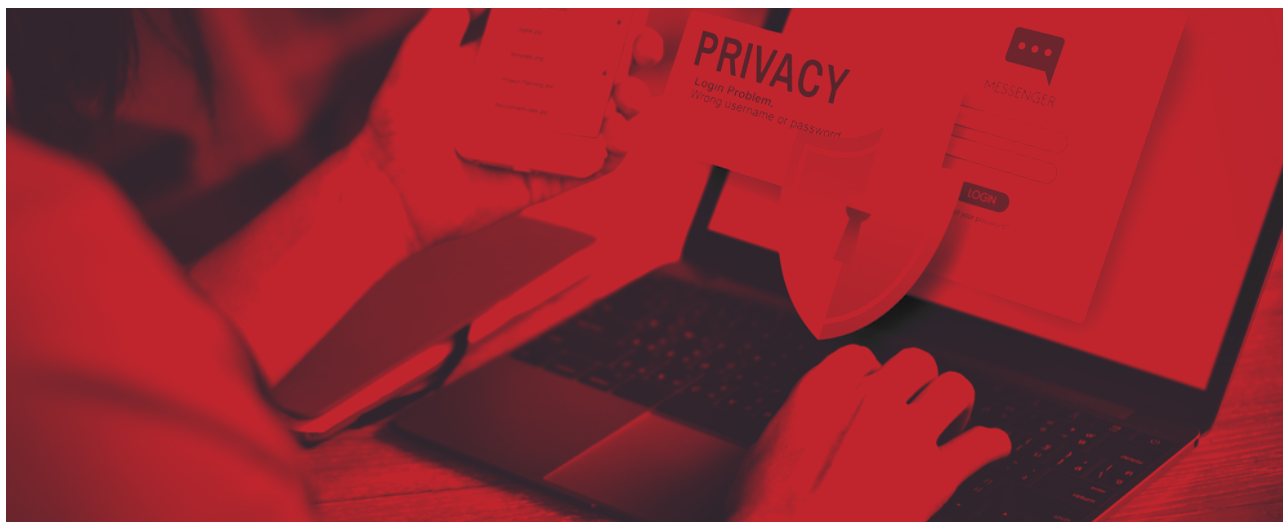
No

No

No

as defined in Article 4 of
Organic Act No. 63-2004.

VIII. Conclusions



Only one company, Orange Tunisia, complies with all requirements laid out in Article 4 of the Organic Act No. 63-2004. However, in practice, the company failed to comply with the legal text of the data protection law as seen on August 2018 ,31, when the company was accused of data exploitation through the misuse of its customers' data. Around 1,500 copies of ID cards and passports were thrown away in the streets, and, to date, the company has neither taken any legal action nor provided a clear justification or explanation regarding this incident. Access Now sent an official letter to the legal department of Orange Tunisia, and, to date, no clarifications have been received in response to our letter. ⁽¹⁾

Three companies—GlobalNet, BEE, and HexaByte Tunisie—do not publish a privacy policy on their websites; thus, they cannot be considered in compliance with the requirements for customer protection in any respect.

While the Tunisie Telecom website includes terms and conditions for using the service, it does not publish an explicit privacy policy. As a result, it is, in effect, noncompliant with Article 7 of the data protection law.

¹ Access Now. 2018. Orange Tunisie failed to protect personal data of its customers, [online] Available at: <<https://bit.ly/2Ow5hin>> [Accessed 23 June 2020].

	Characteristics of compliance	Tunisie Telecom	Ooredoo	Topnet	Orange Tunisie	Globalnet	HexaByte Tunisie	BEE
1.	Ease of accessing the privacy policy	No	Yes	Yes	Yes	No	No	No
2.	Disclosure of where and when personal information is used	No	Yes	Yes	Yes	No	No	No
3.	Disclosure that upon purchase, subscribers agree to share their personal information	No	Yes	Yes	Yes	No	No	No
4.	ISP responsibility for securing and protecting customers' personal information	No	Yes	No	Yes	No	No	No
5.	Disclosure of customers' right to compensation if personal information is stolen or used for purposes other than those mentioned by the privacy policy	No	Yes	No	Yes	No	No	No
6.	Disclosure of other parties that receive customer personal information	No	No	Yes	Yes	No	No	No
7.	Disclosure of the situations in which personal information is revealed to other parties	No	No	Yes	Yes	No	No	No
8.	Full disclosure of the requirements of the national law protecting personal data	No	No	No	Yes	No	No	No

IX. Recommendations

In an already-tense political landscape, Tunisia's inadequate legal framework has left the personal data of Tunisians vulnerable to misuse and abuse. This threat has been clearly manifested throughout the 2019 presidential elections.⁽¹⁾

Additionally, in mid-June 2020, Former Tunisian Prime Minister Elias El-Fakhfakh noted that, during the lockdown period, mobile phone chips were used in the "Operations Hall" to monitor and track citizens' gatherings and their adherence to the measures set by the government to control the spread of COVID19- and identify overcrowded areas.⁽²⁾

Although El-Fakhfakh said that this "initiative" was supervised by the INPDP, the INPDP denied its involvement and stated that «the authority is not aware of such a procedure and has not been consulted at all.»⁽³⁾ In short, the Tunisian government has not been forthcoming or transparent about its action plan to combat the coronavirus disease and has not clarified any specifics about the telcos engaged, the nature of the data collected, and whether it has been accessed or abused by different parties.

Based on the findings of our research, which demonstrates an urgent need for stronger data protection rules in Tunisia, we call on the country's executive branch and parliament to prioritize adoption of new regulations. Until today, serious substantial and enforcement problems remain with the data protection law. For

1 Dima Samaro & Emna Sayadi, Tunisia: Falsified Endorsements In The Presidential Elections. What Happens Next? – Access Now. [online] Available at: <<https://www.accessnow.org/tunisia-falsified-endorsements-in-the-presidential-elections-what-happens-next/>> [Accessed 25 June 2020].

2 Ultra Tunisia. 2020. Elias El-Fakhfakh: We Monitored Citizens' Adherence To Quarantine Through Their Phones. [online] Available at: <<https://bit.ly/2QF0qPb>> [Accessed 25 June 2020].

3 RT Arabic. 2020. The Personal Data Protection Authority In Tunisia: We Are Not Aware Of Monitoring Citizens' Sim Cards During The Quarantine. [online] Available at: <<https://bit.ly/3fBxJeI>> [Accessed 25 June 2020].

example, the law does not mandate ISPs to appoint a Data Protection Officer (DPO) to monitor the processing of data regularly and systematically. Furthermore, the current law also fails to address the right to compensation where affected consumers do not have the right to remedy and access to reporting mechanisms which might explain why there have been no judicial ruling concerning data breaches and violations since passing the law in 2004.

Those issues clearly need to be addressed. In the meantime, however, ISPs should adopt the following practices to protect their customers' privacy:

1. Provide and/or modify a clear, transparent, and accessible privacy policy.

It is crucial that ISPs include clear explanations on their official website of personal information collected, who uses or accesses it, where it's being stored, and for how long, as this would help in developing a bridge of trust between ISPs and consumers. Additionally, transparency further creates an environment based on accountability, in which consumers are constantly informed about their right to privacy.

2. Release regular transparency reports. These detail the extent and form of cooperation with law enforcement requests for user information and surveillance, provide information on the company's process for responding to those requests and notifying affected consumers, and help identify risks to privacy. Transparency reports also provide a picture of the regulatory landscape, helping civil society identify where there may be legal restrictions to reporting. Aggregated and anonymized statistics, publicized through regular reporting, may help bypass legal restrictions on disclosure.

3. Comply with national laws, in this case, with the Organic Act No. 63-2004, to protect against the misuse of consumers' personal data. While acknowledging the need for legal reform, ISPs should comply nevertheless with the existing law which provides basic guidelines on the use and processing of personal data in a lawful manner.

4. Provide grievance and remedial mechanisms. Affected consumers and users should be compensated if their personal information is being compromised, used for unclear purposes, or shared with an undefined third party in the privacy policy. The company should also provide a grievance mechanism for users to raise concerns about violations to their privacy. This, in turn, would generate a sense of public accountability, liability, and moral duty in case of data exploitation.

The current health crisis is further highlighting the urgent need for the Tunisian government to reform its data protection laws to ensure that the best practices outlined in Convention 108 are fully and effectively implemented.

The Tunisian government puts the country's fragile democratic process at risk by not enacting legislation to strengthen the protection and promotion of human rights recognized under the Constitution. What is needed now is a new data protection law informed by civil society input and public consultation. In addition to the threat posed to the democratic process, the lack of privacy and data protection safeguards has implications for Tunisia's unstable economy, as it impacts companies' decision-making on where they will headquarter and build a business. To date, there has been no serious effort by the government or parliament to adopt such a bill.



For more information please contact:

- **Dima Samaro**, MENA Policy Analyst – Access Now

dima@accessnow.org

- **Maha Hussaini**, Executive Director – ImpACT International for Human Rights Policies

maha@impactpolicies.org





Special Thanks to:

Dima Samaro

MENA Policy Analyst

Sami Zeno

IT Specialist

Lara Hamidi

Researcher

Pam Bailey

Editorial Adviser

Laura Hayek

Researcher

Sari Noah

Researcher

Khalil Agha

Digital Media Advisor

Muhammad Muzaffar

Designer

Mostfa Jihad

Designer

