TABLE OF CONTENTS

+ 1. THE LAW

1.1. Overview of the privacy/data protection situation

1.2. Constitutional provisions

1.3. Other applicable laws (e.g. cybercrime law, privacy of communications)

1.4. Case law

1.5. Mention of whether there are any public sector data protection laws

1.6. Possible amendments/draft data protection laws under discussion

2. SECTORAL LEGISLATION

+ 2.1 FINANCIAL SECTOR

2.1.1. Law: Scope of application/ Key provisions

2.1.2. Case law

2.1.3. Presence of a regulator, its role/powers

2.1.4. Key definitions

2.1.5. Data retention

2.1.6. Specific provisions on data breach and data breach notification

2.1.7. Specific provisions imposing limitations on data transfers

2.1.8. Sanctions and penalties

+ 2.2 HEALTH AND PHARMA SECTOR

2.2.1. Law: Scope of application/ Key provisions

2.2.2 Case law

2.2.3 Presence of a regulator, its role/powers

2.2.4. Key definitions

2.2.5. Data retention

2.2.6. Specific provisions on data breach and data breach notification

2.2.7. Specific provisions imposing limitations on data transfers

2.2.8. Sanctions and penalties

+ 2.3 TELECOMMUNICATIONS SECTOR

2.3.1. Law: Scope of application/ Key provisions

2.3.2. Case law

2.3.3. Presence of a regulator, its role/powers

2.3.4. Key definitions

2.3.5. Data retention

2.3.6. Specific provisions on data breach and data breach notification

2.3.7. Specific provisions imposing limitations on data transfers

2.3.8. Sanctions and penalties

3. OTHER JURISDICTIONAL ISSUES

July 2020

1. THE LAW

1.1. Overview of the privacy/data protection situation

As per the Constitution of the Democratic Republic of Timor-Leste ('the Constitution'), approved in 2002 following the formal declaration of the country's independence, Timor-Leste has established constitutional safeguards regarding the protection of personal data and privacy as a general right applicable to citizens.

Without prejudice to these rights, there is no general and comprehensive legislation on the protection of personal data; i.e. there is no national general law on the protection of privacy and data, cybercrime, cybersecurity, and other privacy-adjacent legislation.

In any event, there are some provisions on the processing of personal data and the protection of privacy included in different legislative instruments, aimed either at specific legal and regulatory obligations, or at the processing of information by public entities.

1.2. Constitutional provisions

The Constitution, enacted on 20 May 2002 provides that:

- every individual has the right to honour and privacy (Article 36); and
- the household, correspondence, and any private means of communication are inviolable, save in cases provided for by law (Article 37).

Additionally, in its Article 38, under the epigraph 'Personal Data Protection,' the Constitution provides for the following:

- every citizen has the right to access personal data which concerns them (if contained in either automated or non-automated records);
- every citizen may require the rectification and updating of their personal data, as well as the right to know the purpose for which their personal data is intended/was collected;
- the law defines the concept of personal data and the conditions applicable to processing; and
- automated processing of personal data relating to private life, political beliefs and philosophical, religious faith, party affiliation or trade union affiliation and ethnic origin it is expressly prohibited without the consent of the data subject.

1.3. Other applicable laws (e.g. cybercrime law, privacy of communications)

Law No. 17/2011 on Legal Regime Covering the Prevention of and Combat against Money Laundering and Financing of Terrorism (as amended by Law No. 5/2013 (only available in Portuguese here) ('the AML/CFT Framework') see section 2 for the relevant provisions and principles, from a data protection perspective.

Decree Law 19/2009 approving the Penal Code (as amended), in addition to sector-specific penalties (for further detail see section 2 below), provides for the following:

- **Privacy intrusion:** who by any means, even lawful ones, becomes aware of facts concerning another person's private or sexual life and without consent or just cause, discloses them publicly, shall be punished by imprisonment for up to one year or a fine (Article 183);
- **Violation of secrecy:** anyone who, without consent, discloses a secret of which he has become aware of, because of his condition, trade, employment, profession, or art shall be punished by imprisonment for up to one year or a fine (Article 184); and
- **Violation of correspondence or telecommunications:** any person who, without consent or outside of the cases admissible by law, opens a letter or any other writing addressed to another person, or becomes aware of its contents, or prevents it from being received by its addressee, shall be punished by imprisonment for up to two years or a fine. The same penalty shall apply to anyone who, under the same circumstances, interferes, or becomes

aware of the content of telephone, telegraph, or any other means of telecommunication. Anyone who discloses the contents of letters, closed writings, telephone calls, or other communications above referred shall be punished by imprisonment for up to one year or by a fine, even if he or she has lawfully known those facts. If the crimes referred to are committed by postal, telegraph, telephone, or telecommunications employees, the penalties shall be increased by one third in their limits (Article 187).

1.4. Case law

As far as we are aware, there is no relevant jurisprudence directly referring to procedures on privacy and data protection matters in Timor-Leste.

1.5. Mention of whether there are any public sector data protection laws

In Timor-Leste, most legislation covering the processing of personal data concerns the processing of personal data by the public sector. Below is provided an overview of the relevant public sector laws.

Data protection and civil identification

Decree-Law No. 2/2004 Of 4 February 2004 on Civil Identification ('the Framework for Civil Identification') determines, in relation to data protection matters, that civil identification shall comply with the principles of legality, authenticity, veracity, and security of a citizens' personal data and its purpose is to establish their civil identification. The Framework for Civil Identification provides for rules on the collection and updating of data and expressly forbids the interconnection of personal data contained in the database. Personal data may be communicated to police authorities and judicial entities upon reasoned request that may, or may not, be granted by the Director of the Registry and Notarial Services, the entity responsible for the civil identification database. The Framework for Civil Identification establishes that any person has the right to access and be informed about his or her registry and to correct or remove any information that does not correspond to the truth. In addition, it provides for cases in which third parties may access the personal data of their spouses, heirs and others. Personal data shall be retained in a database for up to five years after the data subject's death and in a historical/archive file for up to 20 years after the death. Finally, the Framework for Civil Identification establishes the security measures that must be in force to register the traceability of database research by the entities that are authorised to directly access the database.

Census data protection

Law No. 1/2015 on the Legal Framework of the General Census of the Population and of Housing (only available in Portuguese here) provides that, on data protection matters, that individual statistical data of natural persons shall be considered personal data.

Statistical data is confidential and cannot be included in any publications or provided to any persons or entities, nor may certificates be issued from it. Moreover, it shall not be disclosed without the written consent of the individuals concerned. Statistical data (which in and of its own, and even in the absence of a specific data protection law, may likely not be considered data protection information) is subject to professional secrecy for all professionals aware of this information; however, data relating to professional or business activity contained in public registers are not of a confidential nature. Questionnaires containing personal information should only be retained for the time needed to produce the statistical information and, in any case, should be deleted within five years later. Personal data is anonymised when it is transferred to an informatic medium.

Access to official documents

Decree-Law No. 43/2016 of 14 of October on Rules of Access to Official Documents (only avaliable in Portuguese here) ('the Framework for Access to Official Documents'), determines that access to officials documents shall comply with the principles of transparency, equality, fairness, and protection of privacy. Moreover, the Framework for Access to Official Documents establishes that the collection of personal data, including health data, must be expressly authorised by the data subject and that it must only be collected and accessed by professionals properly certified and authorised. Additionally, personal data cannot be disclosed without express consent in writing and the information is considered confidential.

The confidentiality duty binds all the parties intervening in the collection, processing, and storage of the personal data. Nevertheless, the Framework for Access to Official Documents also provides that a third party may access documents regarding an identified or identifiable natural person if such third party has written authorisation or demonstrates sufficient relevant personal and legitimate direct interest, in accordance with the principle of proportionality.

Confidential documentation can only be accessed by the public with the express permission of an member of the Government of Timor Leste ('the Governemnt') responsible for the entities and services integrated in the State Administration, and in the other entities as well as services, by the highest ranking official of the service or entity.

Passports

Decree-Law No. 52/2016 of 28 December on the New Passport Regime (only available in Portuguese here) determines that the concession of passports is subject to the principles of legality, authenticity, veracity, and security of the data contained in the passports. Furthermore, it establishes the use of an electronic information system that shall be governed by the principle of security and control of information, namely, by creating different levels of access permissions to prevent that personal data is distorted, damaged, or that unauthorised third parties have access to it. The Director of the Registry and Notarial Services is responsible for ensuring the right of information and access for data subjects, the correction of inaccuracies, and the deletion of unduly registered data, as well as ensuring that the consultation or communication of personal data complies with the law.

1.6. Possible amendments/draft data protection laws under discussion

Not applicable.

2. SECTORAL LEGISLATION

2.1 FINANCIAL SECTOR

2.1.1. Law: Scope of application/ Key provisions

Banking Regulation

Regulation No. 2000/8 on Bank Licensing and Supervision ('the Banking Regulation') establishes the framework for conducting banking activities in Timor-Leste and applies to banks as well as their shareholders, administrators, employees, agents, and affiliated entities.

While the Banking Regulation is aimed generally at the framework for banking licensing and supervision, its provisions on banking secrecy and confidentiality indirectly determines obligations on data protection.

Specifically, any non-public information provided in the course of their services to the bank may not be used or allowed to be accessed by third parties, for their own personal gain or for third-party gain, by past and present administrators, employees, and agents of a bank. Said information shall be kept secret. Such information includes, but is not limited to, customers' accounts balances, amounts, conditions, and use of proceeds of banks' loans, customers' business relationships, and recipients and amounts of payments made by the bank.

The information may be disclosed only to the Central Bank of Timor-Leste ('BCTL'), including its inspectors and the auditors appointed by it, to external auditors of the bank, to judicial authorities as the law shall provide, to foreign bank supervisory authorities, and when required for the protection of the bank's own interest in legal proceedings.

AML/CFT Framework

The AML/CFT Framework applies to financial and non-financial entities. Specifically, it applies to:

- credit institutions;
- insurance companies;
- finance companies and leasing companies;
- entities that issue credit cards;
- any natural or legal person professionally engaged in the activity of buying and selling or exchanging currency;
- any natural or legal person engaged professionally in the activity of transferring funds;
- any profession designated by the competent national authority;
- casinos, including online casinos;
- any person whose activity consists in providing financial services or intervening in financial or real estate transactions, on behalf of the client, without prejudice to professional secrecy; and
- accountants, auditors and consultants.

The AML/CFT Framework requires that the above mentioned entities verify the identity of its customers and beneficiaries in the cases stipulated by law. In order to comply with the law, those entities must verify the identity by virtue of assessing:

- the name and citizen card number of the person concerned when referring to natural persons; and
- the company name, head office, the board members' identity, company registration, corporate type and structure when concerning legal persons.

Entities must provide access to information or records in a timely manner when requested to do so by the competent authority and in accordance with the law, and shall communicate when they become aware of facts indicating that a crime has been or will be committed.

2.1.2. Case law

Please refer to section 1.4 above.

2.1.3. Presence of a regulator, its role/powers

There is no regulator or administrative authority specifically charged with monitoring and regulating the processing of personal data and the protection of privacy. We have indicated below sector-specific authorities which, in the context of their powers of monitoring, oversight and control, may issue decisions on acts or omissions with implications on personal data (as noted above).

The Banking Regulation

The BCTL is an independent and autonomous public entity that acts not only as the national central bank, but also as the entity responsible for the regulation, licensing, and supervision of banks, insurance companies and others that carry out financial activities on the Timorese territory. The BCTL is also the sole responsible entity for the application of corrective measures and administrative sanctions to financial institutions.

The AML/CFT Framework

The Financial Intelligence Unit ('UIF') operates under the authority of the BCTL and has the competence to receive, analyse, and disseminate the information obtained through the mechanisms in force. Every employee and agent of the UIF is subject to a special confidentiality duty in relation to any information obtained in the course of its activity and can only use that information for the purposes forecasted in the law.

2.1.4. Key definitions

There are no key definitions in relation to data protection matters.

2.1.5. Data retention

There are no provisions on data retention.

2.1.6. Specific provisions on data breach and data breach notification

There are no specific provisions on data breach and data breach notification.

2.1.7. Specific provisions imposing limitations on data transfers

Please refer to point 2.1.1.

2.1.8. Sanctions and penalties

The Banking Regulation

In case of breach of the non-disclosure duty, the BCTL may:

- impose fines on the bank or on its administrators or principal shareholders in an amount from USD $500 to $5,000 per day for each day of non compliance, fines shall be determined considering other entities with comparable turnovers having incurred in identical infractions (so as to ensure proportionality and similarity between the fines);
- suspend temporarily or dismiss administrators from positions in a bank and terminate their receipt of remuneration from the bank; or
- revoke the license of the bank.

The BCTL may issue a written order containing any or all of the following provisions:

- requiring the dismissal of the person from his position in the bank;
- prohibit such person from participating in any manner in the conduct of the affairs of the bank;
- prohibit the person from the direct or indirect exercise of voting rights attached to shares of the bank;
- requiring the person to dispose of all or any part of his direct or indirect ownership interest in the bank;
- requiring the person to reimburse the bank for losses caused by violations.

These measures and penalties shall not preclude the application of other civil or criminal penalties.

The AML/CFT Framework

Whoever, whether through wilful intent or negligence, discloses to a client or third person confidential information will be punished with a fine between USD $250 to $150,000, in the case of natural persons, and between USD $1,250 to $750,000, in the case of legal persons. Those who breach the law may also be prohibited from exercising the activity or profession for a period of six months to three years.

2.2 HEALTH AND PHARMA SECTOR

2.2.1. Law: Scope of application/ Key provisions

Ministerial Diploma No. 51/2017 of 20 of December on Family Health (only available in Portuguese here) ('The Health Law') provides rules for the insertion, treatment, management, and access to clinical information of the users of the national health system within national health database and applies to all health professionals and teams.

The use of the database must be guided by the respect for the fundamental rights, freedoms, and guarantees of users of the national health system. As a result, the use of the database must be guided by the following principles:

- **principle of legality:** the collection, processing, management, and access to data shall only be done in accordance with constitutional, legal, and regulatory rules;
- **principle of sufficiency:** data may only be collected for the purposes and in accordance with the Health Law;
- **principle of confidentiality**: personal data contained in a database is of a confidential nature and can only be accessed by authorised persons. Confidentiality does not apply to users who want to access their personal data;
- **principle of actuality:** data relating to each user is updated on the request of the person concerned or officially, whenever the user attends a medical consultation or treatment; and
- **principle of integrity:** professionals and health teams are responsible for the truthfulness and integrity of data.

2.2.2 Case law

Please refer to section 1.4.

2.2.3 Presence of a regulator, its role/powers

The Central Services of the Ministry of Health are charged with promoting the following control actions to protect the confidentiality of information about the health of the user:

- the managers of health establishments should inform the Ministry of Health of who is given access credentials;
- administrative staff who access the database are subject to a duty of confidentiality;
- access to health data can only be performed when the data subject presents him/herself for medical consultation or treatment;
- access to personal information for economic or commercial purposes is prohibited; however, some entities authorised by the Government may access the database to analyse data and information, provided that the data went through an anonymisation process; and

- users may access all their data for information updating or correction purposes provided they do so personally.

2.2.4. Key definitions

Data relating to users of the health system: For the scope of the Health Law, the concept of data relating to users refers to all information relating to their personal identity, health, medical history, as well as that of their family.

2.2.5. Data retention

There are no provisions on data retention.

2.2.6. Specific provisions on data breach and data breach notification

There are no provisions on data breach and data breach notification.

2.2.7. Specific provisions imposing limitations on data transfers

Not applicable. There are no provision imposing limitation on data transfers.

2.2.8. Sanctions and penalties

Anyone who breaches the duty of confidentiality is subject to disciplinary proceedings.

2.3 TELECOMMUNICATIONS SECTOR

2.3.1. Law: Scope of application/ Key provisions

Timor-Leste does not have any legislation concerning telecommunications.

2.3.2. Case law

Please refer to section 1.4.

2.3.3. Presence of a regulator, its role/powers

Not applicable.

2.3.4. Key definitions

Not applicable.

2.3.5. Data retention

Not applicable.

2.3.6. Specific provisions on data breach and data breach notification

Not applicable.

2.3.7. Specific provisions imposing limitations on data transfers

Not applicable.

2.3.8. Sanctions and penalties

Not applicable.

3. OTHER JURISDICTIONAL ISSUES

As noted above, Timor-Leste does not have a comprehensive legal and regulatory framework regarding data protection and privacy, other than general Constitutional protection and provisions included in specific diplomas, mainly aimed at data processing by public entities; there is no legal document that addresses solely privacy and data protection in the country.

Without prejudice, Timor-Leste is part of several international conventions with the United Nations, which include general commitments and provisions on the protection of privacy, particularly for vulnerable groups (such as migrant workers, children and civil/political activists). Some of these treaties include, either directly or indirectly, State commitments with implications on the protection of privacy, such as:

- International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families;
- Convention on the Rights of the Child; and
- International Covenant on Civil and Political Rights.