Knowledge Consulting Ltd.
www.kcl.co.ug

Lisa Thornton Consulting

# Legal Review Report

## Submitted to

## Government of Malawi

### Malawi Communications Regulatory Authority (MACRA)

MACRA
Promoting Universal ICT Access

# Consultancy Services to Develop Draft Regulations for Electronic Transactions and Cyber Security Act for the Government of Malawi

**REF NO: MW-PPPC-147522-CS-QCBS**

**February 2021**

# Table of Contents

# Abbreviations

| Term | Description |
|---|---|
| **CA** | Certification Authority |
| **CAMA** | Consumers Association of Malawi |
| **CERT** | Computer Emergency Response Team |
| **Consulting Team** | KCL and LTC |
| **eIDAS Regulation** | Regulation (EU) No 910/2014 on electronic identification and trust services |
| **ETCA** | Electronic Transactions and Cyber Security Act |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **ICT** | Information and Communications Technologies |
| **KCL** | Knowledge Consulting Ltd |
| **LTC** | Lisa Thornton Consulting |
| **MACRA** | Malawi Communications Regulatory Authority |
| **MCCCI** | Malawi Confederation and Chambers of Commerce and Industry |
| **MoI** | Ministry of Information |
| **MDAs** | Ministries, Departments and Agencies of the Government of Malawi |
| **MGDS** | Malawi Growth and Development Strategy |
| **MPS** | Malawi Police Service |
| **PPPC** | Public Private Partnership Commission |
| **Regulatory Project Plan** | Regulatory Project Plan for the Implementation of the Communications Act, 2016 and Electronic Transactions and Cyber Security Act, 2016 (31 May 2018) |
| **UNCITRAL** | United Nations Commission on International Trade Law |

# Executive Summary

This Legal Review Report identifies the regulations that are necessary and appropriate for the implementation of the Malawi Electronic Transactions and Cyber Security Act. The identification of the regulations to be drafted follows a process of literature review, namely of the Malawi Constitution and relevant policy and strategy documents and a detailed review of the provisions of the ETCA and the Regulatory Project Plan for the Implementation of the Communications Act, 2016 and Electronic Transactions and Cyber Security Act, 2016, adopted by the Malawi Communications Regulatory Authority in 2018. Also informing the identification of the regulations to be drafted is a review of Malawian institutional frameworks, both existing and anticipated, and a review of the regulation of electronic transactions and cyber security in selected jurisdictions.

The table below summarises the regulations to be drafted.

| Regulations | Governing Provisions of the ETA | Provisions calling for Regulations |
|---|---|---|
| Digital signatures, Certification Authorities (CA) and encryption services | Sections 8-14; Part VI (sections 46-70) | Sections 51(2); 52(3); 53(3); 67(2) |
| Interception | Section 84 | Section 84(2) |
| Procedures for Malawi Computer Emergency Response Team (CERT) / Protection of Critical Information Infrastructure | Section 6 | Section 102(k)-(p) |
| Appointment of cyber inspectors | Section 69 | none |
| Online service liability (retention of data regulations) | Part IV (sections 24-32) | Section 29(3) [MACRA] |
| Domain Name Management and appointment of the Registrar to administer the .mw domain name space | Part VIII (section 75-79) | Section 102(a-f) |

# 1. Introduction

This Legal Review Report identifies the regulations that are necessary and appropriate for the implementation of the Malawi Electronic Transactions and Cyber Security Act (ETCA). The ETCA, enacted in 2016, introduces the legal framework for electronic transactions in Malawi. It is aimed at alleviating uncertainties and challenges associated with e-Commerce, thereby facilitating the use of Information and Communication Technologies (ICTs). It also provides for the appointment of a registrar for domain name management, sets out cyber offences, and provides for the protection of critical information infrastructure.

There is need to develop regulations to support the implementation of the ETCA. To identify regulations to be drafted, the process followed a literature review, namely of the Malawi Constitution and relevant policy and strategy documents and a detailed review of the provisions of the ETCA and the Regulatory Project Plan for the Implementation of the Communications Act, 2016 and Electronic Transactions and Cyber Security Act, 2016 (31 May 2018) (Regulatory Project Plan) adopted by the Malawi Communications Regulatory Authority (MACRA). To compliment this process, a review of Malawian institutional frameworks and a review of regulation of electronic transactions and cyber security in selected jurisdictions has been undertaken.

This Legal Review Report is organised as follows:

i. Review of the Malawi Constitution and relevant policy and strategy documents.
ii. Review of the governing legislation, the ETCA.
iii. Review of institutional set-up.
iv. Review of international practices in respect of electronic transactions and cyber security legislation.
v. Identification of regulations to be drafted.
vi. An appendix that identifies key stakeholders to engage during this assignment.

# 2. Constitution and Policy and Strategy Documents

In this section, the Consulting Team reviews the relevant provisions of the Malawi Constitution and relevant policies and strategies, which may inform the regulations to be drafted in terms of the ETCA.

## 2.1 Constitution

Above all legislation in Malawi, including the ETCA is the Constitution.

The Constitution, among other things, provides for fundamental rights to freedom of expression, freedom of the press and the right of access to information, as well as the right to privacy and the right of children to be protected from treatment that is hazardous or harmful, among others. All these rights must be activated through relevant laws, one of them being the ETCA and its enabling regulations.

The Constitution also provides for the three branches of government, the executive, the legislative and the judicial branches. The executive branch is composed of the President, Vice President and a cabinet appointed by the President. The Ministry of Information, responsible for ICT policy and the making of regulations in terms of the ETCA, is a part of the cabinet.

## 2.2 The Malawi Growth and Development Strategy (MGDS) III (2017 – 2022)

The Malawi Growth and Development Strategy (MGDS) III (2017 – 2022) builds on two prior iterations of medium-term strategies designed to contribute to achieving Malawi's long-term development aspirations. The objective of MGDS III is to move Malawi to a productive, competitive and resilient nation through sustainable agriculture and economic growth, climate change, environmental management and population challenges.

The medium-term strategy is to invest in sectors that can spur growth through the linkages they have with the other sectors of the economy. Five sectors are identified, including transport and ICT infrastructure. The transport and ICT sectors are pivotal to accelerating growth of other sectors and act as enablers for poverty reduction and wealth creation. In respect of ICT, the strategy focuses on increasing access, providing well-developed broadband infrastructure and services, and increasing the number of skilled workers.

Outside the ICT sector, and especially in the context of the fourth industrial revolution, ICTs

are universally recognised as critical for development and competitiveness, and therefore the regulations around electronic transactions and cybersecurity must be developed with this as a key consideration.

## 2.3 National ICT Policy, 2013

In 2013, the Government of Malawi adopted the National ICT Policy. The aims of the ICT Policy were to provide the framework for the development of the ICT sector, the development and use of ICT in all sectors, and the development of conditions for universal access to ICT services in order to achieve widespread socio-economic development. The overall policy goal is to "contribute to socio-economic development though maximum integration of ICT in all sectors and the provision of ICT services to the rural areas". The policy objectives are "to facilitate the creation of an enabling environment for efficient, effective and sustainable utilisation, exploitation and development of ICT in all sectors of the economy, including the rural and underserved communities, in order to attain an information-rich and knowledge-based society and economy". Ten priority areas set out, include the following:

i. Strategic ICT Leadership,
ii. Human Capital Development,
iii. e-Government Services,
iv. ICT in Industries,
v. ICT Infrastructure Development,
vi. ICT in the Priority Growth Sectors,
vii. Responsive ICT Legal, Regulatory and Institutional Framework,
viii. National Security,
ix. International Cooperation, and
x. Universal Access to ICT and ICT related services.

The ETCA and regulations made in terms thereof, have the potential to have a significant impact on the priority areas. Online transactions and cyber security are especially critical for e-Government services. The ICT Policy states that the "government shall deploy ICTs to facilitate effective and efficient public service delivery and interaction between the public service and citizens of Malawi, companies, government institutions, cooperating partners and other stakeholders of the Government of Malawi."[1] The ICT Policy cannot be achieved without well-developed cyber security and electronic transaction legislation and regulations.

The ICT Policy anticipates that the Department of e-Government within the Ministry of Information will be restructured into the Malawi Information Technology Agency and that a National ICT Steering Committee, District ICT Committees and Community ICT Committees will be established. The Consulting Team understands, however, that these institutions have not yet been established.

It must be recognised that in the drafting of regulations, these institutions will be key

1 *Government of Malawi, National ICT Policy, An ICT-Led Malawi, Government of Malawi, National ICT Policy, An ICT-Led Malawi, https://www.macra.org.mw/?wpdmpro=malawi-ict-policy-2013*

interested parties, and that while the likely impact of the regulations on such institutions can, to some extent, be taken into account during formulation, it would be prudent to defer the adoption of regulations to after the establishment of these institutions, which will develop implementation strategies whose intent must be taken into account in the regulations

## 2.4 National ICT Master Plan 2014 – 2031

The National ICT Policy, 2013 is operationalised through the National ICT Master Plan 2014 – 2031. The Plan covers 18 years, but is split into four separate timeline plans. The ICT Master Plan is centred on the need to transform Malawian society in four dimensions with ICT: Government, infrastructure, capacity and knowledge community, and businesses. The ICT Master Plan clustered the ten priority areas of the ICT Policy into four strategic pillars:

i. ICT Infrastructure Development,
ii. Innovation and Human Capital Development,
iii. ICT Industry Development and e-Business, and
iv. e-Government and Growth Sector Development.

Plan 1 (2014 – 2016) focused on infrastructure development. Plan 2 (2017 – 2021) focuses on innovation and human capital development. Plan 3 (2022 – 2026) shifts to industry development and e-Business, where the impact of the ETCA and regulations will be important. Plan 4 (2027 – 2031) shifts again, to e-Government and growth sectors, making cyber security and online transaction legislation paramount. The Master plan notes that "in this period, the government will serve its citizens with world-class online interfaces in citizen information as well as providing government business links to stimulate ICT Industry development and e-businesses growth."

## 2.5 National Cybersecurity Strategy, August 2018

The National Cybersecurity Strategy, which was adopted after the ETCA, aims to provide a framework for ensuring a secure, safe and resilient cyberspace and fostering trust and confidence in cyberspace by Malawians. It is anticipated that this will contribute to further growth of the ICT sector as well as socio-economic development across Malawi.

The vision of the Cybersecurity Strategy is "a nation with a secure, trusted, resilient and safe cyberspace that promotes a knowledge-based society and socio-economic development". The mission is to "to develop and deliver effective cybersecurity capacity, services and infrastructure that instils confidence in cyberspace". To achieve the vision, the following strategic goals are set out:

i. Identify and manage the critical information infrastructure of Malawi,
ii. Develop and enhance cybersecurity-related capacity, infrastructure, legal, regulatory and other related frameworks,
iii. Promote awareness, information sharing and collaboration on cybersecurity,

iv. Enable and continuously improve the safety of vulnerable groups in cyberspace, especially the safety of children,
v. Enhance and coordinate the fight against all forms of cybercrime, and
vi. Promote the use of cyberspace to drive social and economic development.

The strategic goal of identifying and managing critical information infrastructure includes the specific objectives of: identifying and protecting the critical information infrastructure; and protecting the critical infrastructure through the Computer Emergency Response Team (CERT).

Regulations to be drafted under the ETCA include regulations governing the CERT and regulations identifying and protecting critical information infrastructure.

## 2.6 Proposals for a Malawi Digital Government Strategy

In March 2018, Avasant provided a report to the Ministry of ICT and the Public Private Partnership Commission, setting out recommendations for the strategy and implementing plan for a compressive e-Government strategy. The recommended vision is "a transformed government with efficient and accountable administration, which provides seamless governance by making public services convenient and accessible, resulting in social-economic growth". One of the specific interventions recommended is the establishment of a Nodal Agency for Digital Government in Malawi, which would be the 'go-to agency' in matters of ICT for government.

In addition, the Consulting Team has been made aware of a project aimed towards drafting separate e-Government regulation. In that project, it is anticipated that the Department of e-Government within the Ministry of Information will be the primary entity responsible for the implementation of e-Government regulation and oversee the implementation of e-Government within Malawi.

## 2.7 Data Protection Bill, 2021

The Data Protection Bill, 2021 has been published for public comment due 26 February 2021. The aim of the Bill is to protect personal data of individuals collected, generated, stored and utilized by public and private sector entities.

The Bill designates MACRA to oversee the implementation of its provisions, through the establishment of a Data Protection Office. Amongst other things, MACRA must maintain a register of data controllers and data controllers must report breaches to MACRA.

The Bill comprehensively deals with personal data protection. It has provisions related to the processing of data by a data controller and the rights of a data subject, amongst others. It

also deals with data security, requires the implementation of technical and organisational measures, and deals with the transferees of data outside of Malawi.

It is anticipated that this Bill will be the umbrella law for personal data protection in Malawi and that the provisions relating to data protection in the ETCA will simultaneously be repealed.

# 3. Electronic Transactions and Cyber Security Act, 2016

The Electronic Transactions and Cyber Security Act was enacted in 2016. It introduces the legal framework for the recognition of electronic transactions in Malawi and establishes certain cybercrimes. It is aimed at alleviating uncertainties and challenges associated with electronic transactions, thereby facilitating the use of ICTs. More specifically, the ETCA provides for the following:

i. Legal recognition of electronic transactions,
ii. Online service provider liability limitations,
iii. Protections for consumers in e-Commerce transactions,
iv. Digital signatures, certification authorities (CA) and encryption services,
v. Personal data protection,
vi. Domain name management,
vii. e-Government,
viii. Cyber offences, and
ix. Protection of critical information infrastructure.

In 2018, MACRA adopted the Regulatory Project Plan. The Regulatory Project Plan encompasses regulatory implementation and related institutional restructuring and capacity building action plan for MACRA's four portfolios, three industry portfolios under the Communications Act and a new subject matter portfolio under the ETCA. A key recommendation is that MACRA must be cognizant of the necessary elements of achieving better regulatory outcomes. The four main elements are:

1) Well-designed rules and regulations that are efficient and effective;

2) Effective, consistent and fair operational processes and practices;

3) Appropriate institutional frameworks and related governance arrangements; and

4) High quality and empowered institutional capacity and resources, especially in leadership roles.

The Regulatory Project Plan has been taken into consideration in the development of this Legal Review Report.

## 3.1 Legal Recognition of Electronic Transactions

Part III (sections 7-23) of the ETCA concerns the legal recognition and validity of electronic transactions. Section 7 provides for the recognition of electronic writings. Sections 8-14 provide for the recognition of electronic and the more secure digital signatures. Section 12(2) provides that the MACRA may by notice in the Gazette, approve digital signatures, CA offering digital certificates, and may authenticate a foreign information security service provider. The remainder of Part III deals with the reliability of electronic records where a law requires an original, the admissibility of electronic messages as evidence, storage of and the security of electronic messages, and the validity of contracts.

## 3.2 Online Service Provider Liability

Part IV (sections 24-32) of the ETCA sets out the limitations of liability of online intermediaries. In exchange for the limitation of liability, online intermediaries and content editors must establish take down procedures, and provide for a right of reply.

Section 24 provides that there will be no limitation to online communications, with the exceptions stated. The exceptions prohibit child pornography, incitement to racial hatred, xenophobia or violence, or justification for crimes against humanity. In addition, electronic communications may be restricted in order to promote human dignity and pluralism, protect public order and national security, among others.

Section 29(3) provides that MACRA may issue regulations governing the retention of data by intermediary service providers that permits the identification of any person who contributed to the creation of content. The issuance of regulations by MACRA is a departure from the norm, which provides that regulations are issued by the Minister. To ensure harmonization, effort should be made to consult the Minister before the regulations are issued.

## 3.3 Protections for Consumers in e-Commerce Transactions

Part V (section 33-45) of the ETCA protects consumers in e-Commerce transactions by requiring online suppliers of goods and services to provide certain information, provides a cooling-off period, requires certain technical capabilities to protect consumers, prohibits misleading advertising, and regulates unsolicited communications.

Section 43 provides that the provisions protecting consumers apply to financial services subject to the Payment Systems Act, 2016. Section 43(2) provides that the Minister of Finance, on recommendation from MACRA and the Governor of the Reserve Bank of Malawi, shall make regulations defining specific obligations with regard to online banking. Sections 44 and 45 provide specific details of consumer protections in respect of financial services.

## 3.4 Digital Signatures, Certification Authorities (CA) and Encryption Services

Part VI (sections 46-70) concerns security and includes provisions related to digital signatures (sections 46-50), CA (section 51) and encryption (sections 52-70). The following sections specifically mention the making of regulations.

i. Section 51(2)—Regulations for CA accreditation (application procedures, fees, terms and conditions, standards, etc.).

ii. Section 52(2-3)—Regulations for the registration of providers of cryptograph services and products and for the use, importation and exportation of encryption programmes and products.

iii. Section 53(2-3)—Regulations for the registration of providers of cryptographic services and products and for the use, importation and exportation of inscription programmes and products.

iv. Section 67(2)—Regulations for conditions for making declarations by encryption service providers regarding technical characteristics of encryption and source code.

The powers and functions of cyber inspectors are detailed in section 70(1), and in respect of suppliers of encryption services, provides for investigating and issuing orders.

## 3.5 Personal Data Protection

Part VII (sections 71-74) of the ETCA concerns personal data protection and privacy. It deals with requirements for collection and processing, consent, and rights of a data subject, among others. There are no regulations mentioned.

The Data Protection Bill, 2021, is expected to replace the provisions in the ETCA regarding data protection.

## 3.6 Domain Name Management

Part VIII (section 75-79) of the ETCA concerns domain name management. It provides for MACRA to appoint a Registrar to administer the .mw domain name space, and for the powers and functions of the Registrar.

Section 102(a)-(j) provides that the Minister may make regulations providing for the following:

a) The requirements and standards that registries and the registrar must meet in order to operate with operational accuracy, stability, robustness and efficiency,

b) The circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries,

c) The pricing policy,

d) The provisions for the restoration of a domain name registration and penalties for late payments,

e) The terms of the domain name registration agreement that registries and the registrar must adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution,

f) The processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of, actual or prospective registrants, registries or the registrar, protocols or products,

g) The requirements to ensure that each domain name contains an administrative and technical contact,

h) The creation of sub-domains,

i) The procedures for ensuring the monitoring of compliance with the ETCA, including compliance with the ".mw" domain name and any other Malawian names to be used for domain names space technical audits, and

j) Any other matter relating to the ".mw" domain name space as may be necessary to achieve the objectives of the ETCA.

## 3.7 e-Government

Part IX (sections 80-82) of the ETCA concerns e-Government transactions. It requires public bodies to take steps to carry out their functions online. The Department of e-Government is called on to assist such public bodies.

The following sections mention the making of regulations.

i. Section 80(5)—Regulations defining the record keeping system for maintenance of electronic records by public bodies.

ii. Section 82—Regulations setting out the legal framework to ensure security, storage, confidentiality and integrity of e-Government transactions and the legal framework to ensure confidentiality of personal data.

## 3.8 Cyber Offences

Part X of the ETCA (sections 83-95) sets out cyber offences and a legal framework for investigations through a warrant procedure issued by a court on application by a cyber inspector. Section 83 provides that a court may issue a search warrant on application of a cyber inspector and section 70(1)(c) sets out details in respect of the contents of such warrants. Section 96 provides that a person affected by a criminal offence in terms of the ETCA, may submit a compliant and that inspectors are to investigate if the complaint is relevant.

Section 84 prohibits interception of electronic data. Section 84(2) provides that the Minister shall make regulations setting out the cases where unauthorized access to, or interception of, or interference with, data may be permitted in specific conditions (the exceptions to the prohibition).

Other offences created are child pornography, cyber harassment, offensive communication, cyber stalking, hacking, spamming, and using the Internet for illegal commerce.

## 3.9 Malawi Computer Emergency Response Team (CERT) / Protection of Critical Information Infrastructure

Section 6 of the ETCA establishes the Malawi Computer Emergency Response Team (CERT) as a MACRA unit. The Malawi CERT is responsible for information infrastructure protection actions and serves in a coordinating role for responses to ICT security threats. MACRA is responsible for ensuring that the CERT is capable of providing reactive and proactive services (as described in the Act) and artefacts analysis. MACRA must also ensure that the CERT is communicating timely ion threats and providing assistance with responses to incidents.

In addition, section 102(k)-(p) provides that the Minister may make regulations in respect of the following:

i. Declaring certain classes of information to be critical data,

ii. Establishing procedures for identification of databases with critical data,

iii. The registration of databases with critical data,

iv. Setting out minimum standards regarding management, access to transfer and control of databases with critical data,

v. The inspection of databases (see also section 70 regarding the powers of cyber inspectors), and

vi. Any other matter related to critical data.

# 4. Institutional Set-up

This section sets out the institutional set-up anticipated in the ETCA, compares it to the institutional set-up in place and anticipated by the ICT Policy and ascertains whether there are any gaps.

## 4.1 Current Institutional Set-up

The Constitution provides for the three branches of government, the executive, the legislative and the judicial branches. The executive branch is composed of the President, Vice President and a cabinet appointed by the President.

The reverent Ministry for the implementation of the ETCA is the Ministry of Information. The Ministry is largely responsible for setting policy in the sector and also has the role given to it in the ETCA to make regulations. There are several departments set up within the Ministry, one of which is the Department of e-Government, which is called upon in the ETCA in respect of implementing e-Government services.

The Minister of Finance is also referenced in the ETCA. Section 43(2) provides that the Minister of Finance, on recommendation from MACRA and the Governor of the Reserve Bank of Malawi, shall make regulations defining specific obligations with regard to online banking.

MACRA is a government body established by Part II of the Communications Act, 2016, to regulate and monitor the provision of communications services in Malawi. It comprises members appointed in accordance with the Act. MACRA appoints a Director General and other staff who are responsible for the day-to-day operations of MACRA. Other staff may be appointed by the Director General if indicated by MACRA.

## 4.2 Institutional Set-up Anticipated in the ICT Policy

The ICT Policy anticipates that the Department of e-Government within the Ministry of Information will be restructured into the Malawi Information Technology Agency and that a National ICT Steering Committee, District ICT Committees and Community ICT Committees will be established. These institutions, however, have not yet been established.

## 4.3 Institutional Set-up Required by the ETCA

The ETCA provides for the following institutions to be involved in the implementation of the legislation.

### 4.3.1 Ministry of Information

Section 102 of the ETCA provides for the making of regulations by the Minister of Information, in consultation with MACRA.

Part IX of the ETCA concerns e-Government. Section 80(2) provides that the Department of e-Government within the Ministry of Information, shall assist and supervise public bodies in the establishment and delivery of e-Government services. Section 81 provides for the periodic publication of guidelines by the Department of e-Government.

### 4.3.2 MACRA

Section 5 of the ETCA provides that MACRA is responsible for the implementation of the ETCA, unless otherwise provided for.

Section 6 of the ETCA establishes the Malawi CERT as a MACRA unit. The Malawi CERT is responsible for information infrastructure protection actions and serves in a coordinating role for responses to ICT security threats. MACRA is responsible for ensuring that the CERT is capable of providing reactive and proactive services (as described in the Act) and artefacts analysis. MACRA must also ensure that the CERT is communicating timely on threats and providing assistance with responses to incidents.

Section 69 of the ETCA provides that MACRA shall appoint cyber inspectors. It also set out qualifying and disqualifying criteria. The powers and functions of cyber inspectors are detailed in section 70(1), and includes monitoring critical information infrastructure and, in respect of suppliers of encryption services, investigating and issuing orders. Section 83 provides that a court may issue a search warrant on application of a cyber inspector and section 70(1)(c) sets out details in respect of the contents of such warrants. Section 70(3) provides that for the performance of the cyber inspectors functions, they may be accompanied by a police officer. Section 96 provides that a person affected by a criminal offence in terms of the ETCA, may submit a compliant and that inspectors are to investigate if the complaint is relevant.

Section 75 of the ETCA provides for MACRA to appoint a Registrar to administer the .mw domain name space. Section 76 sets out the powers and functions of the Registrar. Section 77 provides certain details in respect of the transition of the existing domain name management regime to that anticipated in the Act.

## 4.4 Gaps

The ICT Policy anticipates that the Department of e-Government within the Ministry of Information will be restructured into the **Malawi Information Technology Agency** and that a **National ICT Steering Committee, District ICT Committees and Community ICT Committees** will be established.

Of the institutional set-up anticipated by the ETCA, the establishment of the Malawi CERT will be necessary in terms of section 6. Cyber inspectors will need to be appointed in terms of section 69.

The ETCA calls for MACRA to appoint the Registrar to administer the .mw domain name space.

The ETCA calls for the Minister to make regulations for the appointment of the .mw domain name space Registrar. However, as discussed below, the development of those regulations will need to be preceded by a process involving the Internet Corporation for Assigned Names and Numbers (ICANN) for the substitution of the current country code manager.

In the drafting of regulations anticipated by the ETCA, all the existing institutions as well as those anticipated, will be key interested parties. They will be responsible for the development of implementation strategies that are key to successful the achievement of the policy, strategy and legislative goals.

Given the ever-increasing interrelated nature of ICT regulation, a collaborative approach to the development of regulations is appropriate, indeed necessary. Regulators must interact with peers from other economic sectors both within Malawi and beyond in order to better regulate the industry to leverage ICT as an engine for sustainable development. No institution, not even MACRA, will be able to address electronic transactions and cyber security issues alone.

Attached to this Legal Review Report is a list of key stakeholders identified that will be consulted and engaged for collaboration. Other entities and persons who may be interested in these matters may include online service providers, encryption providers, owners and/or operators of critical information infrastructure such as utility providers, the current administrator of the .mw domain, the media, academia, other development partners, law enforcement entities and other ministries, departments and agencies of the Government of Malawi (MDAs).

# 5. Lessons from International Practices

The purpose of this part of the Legal Review Report is to review international and selected countries' practices to ensure that the regulations to be drafted under the ETCA reflect international good practices There are valuable lessons to be drawn from jurisdictions that have implemented similar laws.

Internationally, the United Nations and other international bodies have developed model laws to be adopted by countries in many areas, including ICT, with leeway to make modifications taking into account the uniqueness of each country. In the area of ICTs, the following are instructive:

i. Convention on Cybercrime of the Council of Europe, also called the "Budapest Convention on Cybercrime,"[2]

ii. United Nations Commission on International Trade Law (UNCITRAL) Model Laws

   a) UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis adopted in 1998[3]

   b) UNCITRAL Model Law on Electronic Signatures 2001[4] and

iii. African Union Convention on Cybersecurity and Personal Data Protection.[5]

The Budapest Convention on Cybercrime and the UNICTRAL model laws provide best practices from an international perspective while the African Union Convention on Cybersecurity and Personal Data Protection provides a benchmark for the African continent.

The **Budapest Convention on Cybercrime** aims to create a common policy aimed at the protection of society against cybercrime by, among other measures, adopting appropriate legislation and fostering international co-operation in dealing with cybercrime. The Convention sets out various offences including the following:

i. Offences against the confidentiality, integrity and availability of computer data and systems such as illegal access to systems or data, system interference and illegal interception.

ii. Computer related offences such as computer related fraud or computer related forgery.

2 *https://rm.coe.int/1680081561*
3 *https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf*
4 *https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf*
5 *https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf*

iii. Content related offences such as offences against child pornography.

iv. Ancillary liability and sanctions for instance attempting, aiding or abetting.

The Convention further provides for procedural provisions for the purposes of specific criminal investigations and proceedings including expedited preservation of stored computer data, search and seizure of stored computer data and production orders.

The ETCA provides for various criminal offences in line with the Convention under Part X. Part X also sets out a legal framework for investigations through a warrant procedure issued by a court on application by a cyber inspector. It is recommended to make provision for process of appointing cyber inspectors in the regulations to be drafted.

The objective of the **UNCITRAL Model Law on Electronic Commerce** is to provide a model law that enables and facilitates the use of electronic commerce, providing equal treatment to users of paper-based documentation and to users of computer-based documentation, including electronic signatures. It also establishes rules for the formation and validity of contracts concluded electronically and for the attribution and retention of data messages.

The objective of the **UNCITRAL Model Law on Electronic Signatures** is to provide legal certainty to the use of electronic signatures. It establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures. It follows a technology-neutral approach, which avoids favouring the use of any specific technical product. It establishes basic rules for assessing possible responsibilities and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process.

The ETCA appears to follow many of the provisions of the UNCITRAL model laws. It provides for the functional equivalence between paper-based and computer-based information including specific provisions on the formation of contracts and legal certainty for electronic signatures. Section 4(a) of the ETCA is clear that one of the principles that shall be adhered to in the implementation and application of the Act is that e-Transactions shall benefit from a secure legal framework that recognizes the legal value of electronic transactions and electronic documents.

The **African Union Convention on Cybersecurity and Personal Data Protection** aims to establish a legal framework for cyber security and personal data protection on the African continent. The convention provides legal provisions on:

i. Electronic transactions including e-Contracts,
ii. Personal data protection, and
iii. Promotion of cyber security and combating cybercrime.

The ETCA provides includes provisions relating to e-Transactions and the provision of cyber offences in tandem with the provisions under the Convention. While the ETCA provides for an agency to respond to cyber incidents and emergencies (the CERT, to be established as a unit within MACRA) it does not provide a cyber security governance structure envisaged under the Convention, which requires clear accountability in matters of cyber security at all levels of

government. Further, the ETCA does not cover key provisions on the personal data protection, however, these provisions are being addressed through the development of a separate personal data protection law.

In terms of best practices from other countries, the following representative countries are included: Australia, Canada, South Korea, Argentina, and Singapore. The review of these countries' practices showcase best practices from advanced economies across the continent. All these countries have been at the top of the countries with a high online services index within their specific geographical regions and in the world.

Lastly, in Africa, the practice of Uganda, Ghana and South Africa are reviewed. South Africa was chosen because it is the most developed economy in Africa and is in the same region as Malawi. Review of practices in Uganda and Ghana provide information from low and middle-income countries that are consistently growing their online services index and have shown development of e-Government.

## 5.1 eIDAS Regulation

At the regional level, the European Union regulation on electronic identification and trust services provides illustrative standards and regulations for identifying, signing, and authenticating technologies and services. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS Regulation) was adopted by the European Parliament and the Council of the European Union (EU) on 23 July 2014. Its subject matter is described as follows:

"With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

i. Lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;

ii. Lays down rules for trust services, in particular for electronic transactions; and

iii. Establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication."[6]

The eIDAS Regulation provides for standards for electronic signatures and authentication mechanisms (trust services) to enable electronic transactions within the EU internal market. In that respect it is not unlike the ETCA. However, the eIDAS Regulation introduces a number of new concepts or developments such as electronic registered delivery services, electronic seals, and authentication of websites to secure online transactions through defined electronic identification services and trust services. It should be noted that these

6 *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG*

developments are not provided for under the ETCA specifically, however, the regulations to be drafted may be informed by eIDAS Regulation.

The key lessons from the regulation are compatible with other international frameworks that are technology neutral and thus allow for developments in technology such as mobile ID, mobile signing and other innovations. The regulation provides for minimum requirements that the technology should satisfy but does not prescribe the technology itself.

The provisions on supervision of providers of services and the requirements of providers to undergo periodic audits to confirm compliance with the Regulation is also of importance. Conformity assessments contribute to a safer online environment and increase trust in online services. Further, clear powers of the regulatory body (supervisory body) and responsibilities of the providers is important in building confidence in the use of digital tools. These lessons can inform the regulations to be drafted.

## 5.2 Australia, Canada and South Korea

The laws of **Australia** on electronic transactions are complicated by the federal nature of the country's government. At the Commonwealth (i.e., national) level, the key legislation is the Electronic Transactions Act 1999.[7] The Electronic Transactions Regulations 2020[8] set out which transactions and Commonwealth laws are exempt from the Act. Additionally, each State and Territory in Australia has its own electronic transactions' legislation, which broadly mirrors the national legislation but includes some specific exceptions that apply when a transaction is governed by the laws of the relevant State or Territory.[9]

The Electronic Transactions Act is largely in tandem with the UNCITRAL model laws on e-Commerce and e-Signatures. There are a number of exceptions where traditional signatures are required. For instance, the Corporations Act 2001 is exempt in its entirety from the provisions of the Electronic Transaction Act. This means that any provisions of the Corporations Act requiring a signature can only be satisfied using a traditional wet signature. Additionally, there are several instances that require additional consideration for e-Signatures, such as when transacting with public sector entities. If you provide an electronic signature to a government department or agency, the method of providing that signature must meet the department's specific information security requirements.

In response to COVID-19, the Commonwealth and most Australian States and Territories have introduced temporary measures to expand electronic signatures. Under the new temporary rules set out in the Corporations (Coronavirus Economic Response) Determination (No. 3) 2020 (Cth) (Determination)[10], companies can now execute documents under section 127(1) of the Corporations Act 2001 (Cth) if certain requirements are met.

Australian law on cybersecurity is found primarily in the Criminal Code Act 1995 as amended

7 *Source: Federal Register of Legislation https://www.legislation.gov.au/Series/C2004A00553*
8 *Source: Federal Register of Legislation https://www.legislation.gov.au/Details/F2020L00956*
9 *Source: Adobe https://helpx.adobe.com/sign/using/legality-australia.html#:~:text*
10 *Federal Register of Legislation https://www.legislation.gov.au/Details/F2020L01194*

by the Cybercrime Act 2001. The statutory offences include unauthorised modification of data, impairment of electronic communications, access to or modification of data restricted by an access control system, impairment of the security or reliability of data, and possessing or supplying data with the intent to commit an offence.

The Cybercrime Act amendments support the investigation of cybercrime, for example by allowing for specialists to support the police under the order of court.

Australia has separate legislation with regard to interception and privacy. And the Australian Prudential Regulation Authority regulates financial technology (Fintech).

Similar to Australia, electronic transactions in **Canada** are regulated at the federal and provincial level of Government. The Uniform Electronic Commerce Act adopted by the Uniform Law Conference of Canada on 30 September 1999 is the basis of most provincial legislation. It was designed to provide provinces with consistent legislation that implemented the principles of the UNICTRAL Model Law on Electronic Commerce. The Secure Electronic Signature Regulations (SOR2005-30)[11] defines the various actors in respect to electronic signatures and defines a secure electronic signature in detail.[12]

The general object of the Uniform Electronic Commerce Act is to provide legal recognition of information and documents, including contracts, which are communicated electronically. The approach of the legislation is to recognize electronic communications, documents, contracts and signatures as functionally equivalent to their written or printed counterparts.

The Act takes into consideration the UNICTRAL Model law on Electronic Commerce best practices. The Uniform Electronic Commerce Act provides safeguards against mistakes in the use of electronic documents, for instance, where an electronic document is created or sent in error by a natural person to an electronic agent. The person who sends it must give notice of the error as soon as practicable, respond to instructions, and not benefit from the mistake. A requirement in a law for the signature of a person is satisfied by an electronic signature. The essential function of a signature is to link a person with a document. The information purporting to constitute the signature must be created or adopted by a person with the intent to sign the document, and it must be associated in some way with the document. Someone who alleges that an electronic signature meets a signature requirement will have to prove these characteristics to the satisfaction of a court or other decision maker.

There is no specific legislation in Canada that apply specifically to cyber security, except for anti-spam legislation.

The Government of **South Korea** provides a most comprehensive legal regime for electronic transactions and cybersecurity. Having recognized the importance of e-Commerce it has enacted various laws over time including the Framework Act on Electronic Documents and Transactions (1999)[13] and Electronic Signature Act (1999)[14]. Korea has separate legislation

11 *https://laws-lois.justice.gc.ca/PDF/SOR-2005-30.pdf*
12 *Regulation 2*
13 *https://www.law.go.kr/lsInfoP.do?lsiSeq=195365&urlMode=engLsInfoR&viewCls=engLsInfoR#0000*
14 *https://www.law.go.kr/lsInfoP.do?lsiSeq=195204&urlMode=engLsInfoR&viewCls=engLsInfoR#0000*

regarding consumer protection, personal data protection, domain name administration and financial transactions.

The purpose of the Framework Act on Electronic Documents and Transactions is to contribute to the development of the national economy by clarifying the legal relevance of electronic documents and electronic transactions, ensuring the security and reliability of electronic documents and electronic transactions, and creating infrastructure for facilitating the use thereof.

The purpose of the Digital Signatures Act is to establish the basic framework for the system of digital signatures in order to secure the safety and reliability of electronic messages and to promote their use, thereby stimulating the use of electronic records and communications on a national level and advancing social benefit and convenience.

The Framework Act provides for the following:

a Provides that parties to electronic transactions must obtain the express consent of the other party before collecting personal information on him or her in matters related to e-Commerce and shall not use the collected information for purposes other than conducting electronic transactions;

b Encourages private sector led implementation of initiatives.

c Assigns an agency responsible for promoting the use of electronic documents and conduct of electronic transactions.

d Provides for certified electronic document centres and certified electronic document intermediaries.

e Provides for a mediation committee for disputes on electronic documents and electronic transactions.

f The Digital Signatures Act provides for the following:

- The obligations and responsibilities of the certification authorities including the maintenance of a secure and reliable certification system and the secure management of the private key and certificate-related records;
- A procedure for resolving subscriber complaints
- Financial assistance in promoting the use of digital signatures.

There are many laws in Korea applicable to cybersecurity. These include the Act on Promotion of Information and Communications Network Utilization and information Protection, the Electronic Financial Transactions Act, and the Act on the Protection of Information and Communication Infrastructure.

The review of the Korea's ICT laws shows the value in addressing each area in a standalone law, which provides an opportunity to detail the principles in a more comprehensive manner. Areas such as consumer protection, personal data protection, domain administration, and

electronic financial transactions are better dealt with in specific legislation addressing those areas of concern.

## 5.3 Latin America and Asia

Argentina, Brazil, Paraguay and Uruguay constitute the Common Market of the South (Mercado Común del Sur, or MERCOSUR), a South American economic bloc established by the Treaty of Asunción in 1991 and Protocol of Ouro Preto in 1994.[15] MERCOSUR's Working Subgroup 13 on e-Commerce has promoted negotiations to encourage cross-border e-Commerce through mechanisms that provide for the recognition of digital certificates between signatory States. In developing its laws, **Argentina** has largely followed the resolutions of MERCOSUR. These cover electronic transactions, consumer protection, international jurisdiction in issues of consumer relations, e-signatures and their recognition across the relevant states. These laws are consistent with the UNICTRAL model laws on e-Commerce and e-Signatures.

Argentina has regulations in different areas relating to e-Commerce as part of the Civil Code, the Commercial Code, the Digital Signature Act (Law 25.506) and the Consumer Protection Act (Law 24.240). The Civil Code governs various issues associated with the formation of contracts and related formalities. It sets forth the principal rules governing offerings to the public, their acceptance, the formation of contracts between parties both of whom are physically present, and between parties that are not, and the time at which a contract takes effect.

Under the Commercial Code, indeterminate offers to the public are not binding. To protect consumers, Law 24.240 makes offers that are directed to non-specific potential consumers binding on those issuing them over the period of time during which the offer is in force, and parties making offers must provide information regarding the modalities, conditions and limitations surrounding the offers. It also establishes that the specifics offered through advertising shall be binding on the party offering them and that these specifics must be included in the contract made with the consumer.

Law 24.240 sets forth special requirements for contracts with consumers, who, within five days of the date on which the product is delivered or on which the contract is signed, have the right to opt out without incurring any liability, if procurement of the goods is effected through electronic means. In addition, some sectors have adopted self - regulation measures to protect consumers' rights. These include the Code of Conduct of the Chamber of Commercial Information Firms and the Code of Ethics of Argentina's Direct and Interactive Marketing Association. Argentina also provides for consumers' right to information in connection with transactions conducted via the internet.

Law 25.506 recognises the legal validity of electronic documents and signatures and of digital signatures, making handwritten signatures and digital signatures legally equivalent. It also requires that digital documents comply with the requirements applicable to written

15 *MERCOSUR official website https://www.mercosur.int/en/*

documents. A number of Argentina's provinces have made this law applicable to public administration in their jurisdictions. In addition, Argentina has signed the Southern Common Market (Mercado Común del Sur, or MERCOSUR) regulations governing standards on the use of digital signatures (Resolutions GMC 34/06 and 37/06 on electronic and digital signatures) and has incorporated them in its domestic regulations.[16]

Blythe, Stephen E. in "A Critique of Argentine E-Commerce Law and Recommendations for Improvement"[17] provides a detailed analysis of Argentina's law on e-Commerce that is instructive. Areas to consider include ensuring that the relevant regulations make provision for digital certificate subscriber rights, procedures for certification authorities and penalties when the certification authorities do not comply, and consumer protection for online users.

**Singapore** regulates its online environment through the following laws and regulations including the Electronic Transactions Act Cap 88[18] and the Electronic Transactions (Certification Authority) Regulations S 650/2010.[19] Singapore has separate personal data protection legislation, the Personal Data Protection Act 2012.

In respect of cybersecurity, it also has enacted the Cyber Security Act 2018,[20] the Cyber Security (Critical Information Infrastructure) Regulations 2018[21], the Cyber Security (Confidential Treatment of Information) Regulations S 520/2018;[22] the Computer Misuse Act Cap. 50A[23] and the Computer Misuse (Composition of Offences) Regulations;[24] and the Strategic Goods (Control) Act (Cap.300).

The Cyber Security Act is an Act to require or authorize the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, and to regulate cybersecurity service providers. The Act provides for designation of critical infrastructure following criteria provided. This enables the regulator to address emerging industries and ensure they are put under the regulatory regime as and when they emerge. The law provides for the appointment of a Commissioner with wide powers that enable effective oversight and requires owners to furnish information. This provides an in depth knowledge of systems to ensure proper guidance on their security.

The Cyber Security Act also provides for:

i. Mandatory cybersecurity audits and risk assessment of critical information infrastructure with a requirement to submit the audit report to the regulator,
ii. The licensing of cyber security providers,
iii. The reporting of cybersecurity incidents to the regulator and adherence to codes of practice and performance standards as issued by the regulator, and

16 *Source: UNCTAD, Study on Prospects for Harmonizing Cyber Legislation in Latin America*
17 *Blythe, Stephen E. (2011) "A Critique of Argentine E-Commerce Law and Recommendations for Improvement," Annual Survey of International & Comparative Law: Volume. 17: Issue. 1, Article 6 https://digitalcommons.law.ggu.edu/annlsurvey/vol17/iss1/6*
18 *https://sso.agc.gov.sg/Act/ETA2010*
19 *https://sso.agc.gov.sg/SL/ETA2010-S650-2010?DocDate=20101101*
20 *https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312*
21 *https://sso.agc.gov.sg/SL/CA2018-S519-2018?DocDate=20180830*
22 *https://sso.agc.gov.sg/SL/CA2018-S520-2018?DocDate=20180830*
23 *https://sso.agc.gov.sg/Act/CMA1993*
24 *https://sso.agc.gov.sg/SL/CMA1993-RG1?DocDate=20080401*

iv. Protection of informers.

The Computer Misuse Act makes provision for securing computer material against unauthorized access or modification. The Act is comparable to the provisions on computer misuse on the ETCA. The Act provides for expanded territorial scope of offences under the Act. It provides that the Act shall have effect in relation to any person whatever his nationality or citizenship outside as well as within Singapore.

The Electronic Transactions Act is an Act to provide for the security and use of electronic transactions. It drew from the UNCITRAL Model Law on Electronic Transactions. Its provisions are comparable to the provisions within the ETCA. It only differs in specifically providing for excluded matters, while the ETCA gives the responsible Minister powers to make an order exempting certain transactions from the application of the Act.

The Electronic Transactions (Certification Authority) Regulations S 650/2010 provide the procedure for applications for accredited certification authorities and provide for accreditation requirements. These regulations are a useful benchmark.

Having separate laws for the various areas of ICT regulation is similar to the approach by Korea. Having reviewed this approach, the Consulting Team, where possible, will suggest the drafting of regulations to provide detail or address areas that are not covered in detail in the ETCA. The Consulting Team also understand that separate laws for matters such as personal data protection are currently underway.

## 5.4 Ghana, South Africa and Uganda

**Ghana** enacted the Electronic Transaction Act 772 in 2008.[25] The provisions on electronic transactions are based on the UNICTRAL Model Law on Electronic Transactions, as well as elements of the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005).

The Act provides for the following:

a The identification, registration rules for the management of critical databases,

b The establishment of a governing body for domain name administration and the licensing of registrars and registries, and

c Penalties for cyber offences.

The law regulating electronic transactions in **South Africa** is the Electronic Communications and Transactions (ECT) Act 25 of 2002.[26] It is similar to ETCA in addressing many areas of ICT regulation under one law. South Africa also has separate consumer protection legislation,

25 *https://www.moc.gov.gh/electronic-transactions-act-772*
26 *https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf*

personal data protection legislation, and interception legislation. A cybercrime bill has been before Parliament for several years, but has not yet been enacted. Fintech is regulated by an Intergovernmental Fintech Working Group under the direction of the National Treasury and the South African Reserve Bank.

Section 2 of the Act provides the objects of the ECT Act are to enable and facilitate electronic communications and transactions in the public interest. The ECT Act also makes provision for cybercrime in South Africa, introducing statutory criminal offences.

The areas covered in the legislation include the following:

i. Registration of cryptography providers and authentication service providers,

ii. Protection of critical databases,

iii. Establishment of an Authority for the management of the country code domain name and for alternative dispute resolution for domain name disputes,

iv. Provisions for the appointment and powers of cyber inspectors, and

v. Introduction of statutory cybercrime and penalties.

South Africa has enacted regulations in terms of its legislation for cryptography providers and authentication service providers as well as regulations for an alternative dispute mechanism.

**Uganda** has three laws governing electronic transactions including the Electronic Transactions Act 2011,[27] the Electronic Signatures Act 2011,[28] and the Computer Misuse Act 2011[29] ("Cyber laws"). Before the said laws came into effect, Uganda had passed the National Information Technology Authority Act[30] that set up the body in charge of regulating the sector, including the promotion of e-Government, regulation of e-Signatures and data protection and privacy.

The Electronic Transactions Act, provides a legal and regulatory framework that:

i. Enables and facilitates electronic communication and transactions;

ii. Removes and eliminates the legal and operational barriers to electronic transactions;

iii. Provides legal certainty and public confidence in the use of electronic communications and transactions;

iv. Promotes the use of e-Government services, and

v. Develops a safe, secure and effective environment for the consumer, business and the

27 *https://www.nita.go.ug/publication/electronic-transactions-act-2011-act-no-8-2011*
28 *https://www.nita.go.ug/publication/electronic-signatures-act-2011-act-no-7-2011*
29 *https://www.nita.go.ug/publication/computer-misuse-act-2011-act-no-2-2011*
30 *https://www.nita.go.ug/sites/default/files/publications/NITA-U%20Act%20%28Act%20No.%204%20of%202009%29.pdf*

Government to conduct and use electronic transactions.

The Electronic Signatures Act is an Act to make provision for and to regulate the use of electronic signatures. The Computer Misuse Act is an Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment. The laws benchmarked against the UNCITRAL model laws.

The cyber laws provide for the following:

i. Regulation of certification authorities

ii. Segregation of roles between certification authorities and repositories

iii. Procedures for the application and consideration of licences for certification authorities

iv. Technology neutrality,

v. Consumer protection, and

vi. Provision for a consumer to raise a complaint with the regulator.

**Uganda** has made great strides in implementing the cyber laws. It has increased its online services index within the private and public sector. Its laws are technology neutral and also principle based rather than prescriptive. To realize the benefit from the statutes, Uganda has relied on regulations to provide more detail and address any gaps identified as implementation proceeds. As a result, government agencies and private sector have embraced electronic transactions.

Successful implementation is attributed to the development and implementation of regulations under the law that enabled the development of common platforms that form the bed rock of the development of e Government in the country and their mandatory usage by government agencies. These include regulations that required all government agencies to connect and utilize the National Backbone Infrastructure, the National Data centre for hosting services, the National Data Bank platform that enables the integration of all government systems and the mandatory development of websites by all government agencies.

However, Uganda has no provisions on critical information infrastructure, regulation of domain name administration and provision for electronic identification and trust services. The slow progress of technology implementation in some cases affected the growth of the industry such as the regulation or licensing of the certification service providers. The government wanted to provide the services, yet it had no resources to build the infrastructure immediately. This has now been implemented by leveraging resources within the private sector.

Further, while Uganda has consumer protection provisions in the law, the enforcement of those rights has been minimal as the laws have weak penalties and the enforcement powers given to the regulator are weak. While within government and private sector the awareness of the cyber laws is recognizable, among the citizenry, the level of awareness of the laws is very low. This can be attributed to the fact that the laws have not been translated into local languages and funds for mass sensitization are very minimal. Studies have shown a big divide between the central government and local governments or regional offices. This is largely attributed to funding and also the lack of ICT professionals who can make a case for the development of ICT in local government.

## 5.5 Lessons

There are many practices that can be useful in guiding the development of regulations under the ETCA to provide a good enabling environment for the development and increased adoption of online services in Malawi. The countries from where the best practices have been derived have demonstrated the correlation between a good enabling environment and increased adoption of online services. Key best practices to adopt in the regulations include the following:

a Regulations should be technology neutral,

b Regulations should empower the regulator to enable effective implementation of the ETCA, including provisions relating to the CERT and cyber inspectors.

c Regulations should have provisions on issues related to critical information infrastructure with clear roles for the owners or operators and the regulator.

d Regulations should look to Singapore and Korea for cyber security measures.

e Regulations should be specific where they require compliance by government bodies.

f Regulations should recognize the international nature of electronic transactions and cyber security and facilitate collaboration by Malawi with international bodies.

# 6. Identification of Regulations to be Drafted

Section 102 of the ETCA provides for the making of regulations by the Minister of Information, in consultation with MACRA, for carrying out the purpose and provisions of the Act. It also provides that such regulations may create offences carrying a fine of up to K5,000,000 and to imprisonment up to seven years.

There are two exceptions to the provision that the Minister makes regulations. The first is in section 29, which provides that MACRA may issue regulations governing the retention of data by intermediary service providers. The second is section 43(2), which provides that the Minister of Finance, on recommendation from MACRA and the Governor of the Reserve Bank of Malawi, make regulations defining specific obligations with regard to online banking.

In addition, the Consulting Team has divided the list of regulations that may need to be drafted into the following categories:

i. Regulations that must or may be made in terms of the ETCA
   - Digital signatures, Certification Authorities (CA) and encryption services
   - Interception
   - Procedures for Malawi Computer Emergency Response Team (CERT) / Protection of Critical Information Infrastructure
   - Appointment of cyber inspectors
   - Online service provider liability (retention of data regulations)
   - Domain Name Management and appointment of the Registrar to administer the .mw domain name space.

ii. Regulations that may be made in terms of the ETCA, but where the matter is the subject of separate proceedings
   - e-Government
   - Personal data protection
   - Online banking.

## 6.1 Digital Signatures, CA and Encryption Services

The regulations called for in regarding digital signatures, certification authorities and encryption services are a key part of regulations to be drafted in terms of any electronic transactions law. It is not surprising therefore, that these sections specifically call for the making of regulations:

i. Section 51(2)—Regulations for the accreditation of CA (application procedures, fees, terms and conditions, standards, etc.).

ii. Section 52(2-3)—Regulations for the registration of providers of cryptograph services and products and for the use, importation and exportation of encryption programmes and products.

iii. Section 53(2-3)—Regulations for the registration of providers of cryptographic services and products and for the use, importation and exportation of inscription programmes and products.

iv. Section 67(2)—Regulations for conditions for making declarations by encryption service providers regarding technical characteristics of encryption and source code.

Section 12(2) also informs the making of these regulations. It provides that MACRA may, by notice in the Gazette, approve digital signatures, CA offering digital certificates, and may authenticate foreign information security service providers.

## 6.2 Interception

Part X of the ETCA sets out offences, one of which is the offence of interception. However, section 84 provides that regulations must set out the cases where unauthorized access to, or interception of, or interference with, electronic data may be permitted (the exceptions to the prohibition on interception).

## 6.3 Procedures for the CERT / Protection of Critical Information Infrastructure

Section 6 of the ETCA establishes the Malawi Computer Emergency Response Team (CERT) as a MACRA unit. The Malawi CERT is responsible for information infrastructure protection actions and serves in a coordinating role for responses to ICT security threats. MACRA is responsible for ensuring that the CERT is capable of providing reactive and proactive services (as described in the Act) and artefacts analysis. MACRA must also ensure that the CERT is communicating timely ion threats and providing assistance with responses to incidents.

There are no specific provisions in the ETCA calling for the making of regulations governing the operations of CERT. Section 102, however, provides for the making of regulations for carrying out the purpose and provisions of the Act.

In addition, section 102(k)-(p) provides that the Minister may make regulations in respect of the following:

i. Declaring certain classes of information to be critical data,

ii. Establishing procedures for identification of databases with critical data,

iii. The registration of databases with critical data,

iv. Setting out minimum standards regarding management, access to transfer and control of databases with critical data,

v. The inspection of databases (see also section 70 regarding the powers of cyber inspectors), and

vi. Any other matter related to critical data.

The strategic goal of identifying and managing critical information infrastructure set out in the Cybersecurity Strategy, includes the specific objectives of identifying and protecting critical information infrastructure through the CERT.

## 6.4 Appointment of Cyber Inspectors

Section 69 of the ETCA provides that MACRA shall appoint cyber inspectors. It also set out qualifying and disqualifying criteria. The powers and functions of cyber inspectors are detailed in section 70(1), and includes monitoring and, in respect of suppliers of encryption services, investigating and issuing orders. Section 83 provides that a court may issue a search warrant on application of a cyber inspector and section 70(1)(c) sets out details in respect of the contents of such warrants. Section 96 provides that a person affected by a criminal offence in terms of the ETCA, may submit a compliant and that inspectors are to investigate if the complaint is relevant.

There are no specific provisions in the ETCA calling for the making of regulations for the appointment of cyber inspectors, however section 102 provides for the making of regulations for carrying out the purpose and provisions of the Act. The Consulting Team points out also that MACRA may provide for the appointment of staff by the Director General in terms of the Communications Act.

## 6.5 Online Service Provider Liability

Section 29(3) of the ETCA states that MACRA may issue regulations governing the retention of data by intermediary service providers that permits the identification of any person who contributed to the creation of content.

## 6.6 Domain Name Management and Appointment of the Registrar to administer the .mw Domain Name Space

Part VIII (section 75-79) of the ETCA concerns domain name management. It provides for MACRA to appoint a Registrar to administer the .mw domain name space, and for the powers and functions of the Registrar.

Section 102(a)-(j) also provides that the Minister may make regulations providing for the following:

a) The requirements and standards that registries and the registrar must meet in order to operate with operational accuracy, stability, robustness and efficiency,
b) The circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries,
c) The pricing policy,
d) The provisions for the restoration of a domain name registration and penalties for late payments,
e) The terms of the domain name registration agreement that registries and the registrar must adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution,
f) The processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of, actual or prospective registrants, registries or the registrar, protocols or products,
g) The requirements to ensure that each domain name contains an administrative and technical contact,
h) The creation of sub-domains,
i) The procedures for ensuring the monitoring of compliance with the ETCA, including compliance with the ".mw" domain name and any other Malawian names to be used for domain names space technical audits, and
j) Any other matter relating to the ".mw" domain name space as may be necessary to achieve the objectives of the ETCA.

The history of delegation and re-delegation of Malawi country code top level domain (ccTLD) (namely, .mw) was set out in the Regulatory Project Plan. It is also indicated that MACRA will appoint the current administrator, SDNP Ltd, as the Registrar. The Consulting Team agrees with this plan.

## 6.7 Regulations where the matter is the subject of separate proceedings

### 6.7.1 e-Government

e-Government is a key area of concern in the ICT Policy and ICT Master Plan. Part IX of the ETCA requires public bodies to take steps to carry out their functions online. The Department of e-Government within the Ministry of Information, is called on to assist such public bodies. The following sections indicate that the Minister may make regulations:

i. Section 80(5) – Regulations defining a reliable record keeping system for maintenance of electronic records by public bodies.

ii. Section 82 – Regulations setting out the legal framework to ensure security, storage, confidentiality and integrity of e-Government transactions, and setting out the legal framework to ensure confidentiality of personal data and inviolability of private life.

There is a Malawi Digital Government Strategy, which deals with these matters in a more comprehensive manner. In addition, it is anticipated that the Department of e-Government within the Ministry of Information will be the primary entity responsible for the implementation of new e-Government legislation and oversee the implementation of e-Government within Malawi. The Consulting Team advises, therefore, that these regulations do not form part of this consultancy.

### 6.7.2 Personal data protection

Part VII of the ETCA sets out requirements for collection and processing online data, consent, and rights of a data subject, among others. There are no regulations mentioned.

The Consulting Team has been made there is noaware that there is a separate Data Protection Bill being developed, which will supersede the provisions of the ETCA in respect of online privacy and data protection.

### 6.7.3 Online banking

Section 43 provides that the ETCA applies to electronic financial services, subject to the Payment Systems Act and any other financial services law. Section 43(2) provides that the Minister of Finance, on recommendation from MACRA and the Governor of the Reserve Bank of Malawi, shall make regulations defining specific obligations with regard to online banking.

The recommendation from MACRA and the Governor of the Reserve Bank of Malawi will emerge from consultations between MACRA, the Governor or the Reserve Bank of Malawi and the Ministry of Finance. The purpose of specific obligations with regard to online banking may include special protections to online or mobile banking customers or may be intended

to increase mobile money usage, amongst others. The consultations are urgent in order to provide regulatory guidance consistent with the protection of users while being responsive to macro-economic policy requirements.

## 6.8 Conclusion

Following the review of the Constitution, policies, and strategies of Malawi, analysis of the ETCA and international practices, it is clear that the regulations concerning digital signatures, CA and encryption services need to be drafted, along with procedures governing CERT, the protection of critical information infrastructure, and the appointment of cyber inspectors, among others.

Table 1 provides a summary of the regulations to be drafted.

***Table 1: Regulations to be Drafted***

| Regulations | Governing Provisions of the ETA | Provisions calling for Regulations |
|---|---|---|
| Digital signatures, Certification Authorities (CA) and encryption services | Sections 8-14; Part VI (sections 46-70) | Sections 51(2); 52(3); 53(3); 67(2) |
| Interception | Section 84 | Section 84(2) |
| Procedures for Malawi Computer Emergency Response Team (CERT) / Protection of Critical Information Infrastructure | Section 6 | Section 102(k)-(p) |
| Appointment of cyber inspectors | Section 69 | none |
| Online service liability (retention of data regulations) | Part IV (sections 24-32) | Section 29(3) [MACRA] |
| Domain Name Management and appointment of the Registrar to administer the .mw domain name space | Part VIII (section 75-79) | Section 102(a-f) |

In drafting these regulations, the following best practices will be followed to the extent that they are not in conflict with the law:

i. Regulations should be technology neutral.

ii. Regulations should empower the regulator to enable effective implementation of the ETCA, including provisions relating to the CERT and cyber inspectors.

iii. Regulations should have provisions on issues related to critical information infrastructure with clear roles for the owners or operators and the regulator.

iv. Regulations should look to Singapore and Korea for cybersecurity measures.

v. Regulations should be specific where they require compliance by government bodies.

vi. Regulations should recognize the international nature of electronic transactions and cyber security and facilitate collaboration by Malawi with international bodies and other countries.

# Appendix A: Key Stakeholders

This Appendix sets out the key stakeholders who may be interested in or will be impacted by the implementation of the ETCA. The consultation of and collaboration with these entities will be a key to the drafting of effective regulations. For clarity, this will be alongside a call for input from all interested parties, which may include online service providers, encryption providers, owners and/or operators of critical information infrastructure, the current administrator of the .mw domain, the media, academia, other development partners, and other ministries, departments and agencies of the Government of Malawi (MDAs).

## A.1 MDAs

| MDA |
|---|
| Ministry of Information (MoI) |
| MoI, Department of e-Government |
| MACRA |
| Malawi Police Service (MPS) |
| Attorney General |
| Ministry of Justice |
| Ministry of Defence |
| Ministry of Homeland Security |
| Ministry of Trade |
| Ministry of Finance |
| Governor, Reserve Bank of Malawi |
| Financial Intelligence Authority |
| Malawi Revenue Authority |
| National Registration Bureau |

## A.2 Parliament

| Organisation |
|---|
| Media and Communications Committee |
| Legal Affairs Committee |

## A.3 Licensees and Service Provider Organisations

| Organisation |
|---|
| Malawi Internet Service Providers' Association |
| Association of Telecommunication Operators |
| ICT Association of Malawi |
| Internet Society, Malawi Chapter |

## A.4 Consumer and Professional Organisations

| Organisation |
|---|
| Human Rights Defenders Coalition |
| Consumers Association of Malawi (CAMA) |
| Malawi Confederation and Chambers of Commerce and Industry (MCCCI) |

## A.5 Academia

| Organisation |
| --- |
| University of Malawi |
| Malawi University of Science and Technology |

## A.6 Development Partners

| Organisation |
| --- |
| HIVOS |
| OXFAM International |
| Plan International |

kcl.co.ug
thornton.co.za