10.1. OVERVIEW

DATA PROTECTION: Tunisia has a data protection law (2004/63) and a draft basic law (2018/25). Tunisia has acceded to the Council of Europe Convention 108 and will be bound by the ECOWAS Supplementary Act A/SA.1/01/10. Tunisia has a national authority for the protection of personal data (INPDP).

ELECTRONIC TRANSACTIONS: Tunisia has an Electronic Commerce Law regulating electronic transactions and electronic commerce in the country (Law 2000/83). Tunisia has a National Electronic Certification Agency (Tuntrust).

CYBERCRIME AND CYBERSECURITY: Tunisia has laws regulating cybercrime and cybersecurity: the Tunisian Penal Code; Law 2004/5 and the Telecommunications Code, 2001. Tunisia also has a draft cybercrimes law. Tunisia has a national policy for cyber security. A national cybersecurity strategy has been finalised. Tunisia has a National Agency for Computer Security (ANSI) and a Computer Emergency Response Team (TanCERT).

10.2. DATA PROTECTION

10.2.1. Overview of Data Protection Legislation

Privacy and personal information in Tunisia are principally protected under Article 24 of the 2014 Tunisian Constitution which provides that the “right to privacy and the inviolability of the home, and the confidentiality of correspondence, communications, and personal information” are protected by the State. The constitutional protection of personal information is codified under Law 2004/63 of 27th July 2004 relating to personal data protection (“Law 2004/63”) and the Draft Basic Law No. 2018/25 on the protection of personal data. (the “Draft Law 2018/25”). Tunisia also adheres to the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”) and as a member of the Economic Community of West African States, it will be bound by the regions Supplementary Act A/SA.1/01/10 on personal data protection.

These laws and legal instruments are discussed more fully below:

Law 2004/63 was the first statutory instrument in Tunisia that established a legal privacy framework. Law 2004/63 was implemented by Decree No. 2007/3004 of 27 November 2007 on the conditions and processing of notification and authorization for the processing of personal data, and Decree No. 2007/3003 of 27 November 2007 on the functioning of the national authority for the protection of personal data: l’Instance Nationale de Protection des Données à Caractère Personnel (“INPDP”). Under these laws, the protection of personal data is regulated across various provisions – these are canvassed below:

Article 75 of Law 2004/63 establishes a data protection authority whilst sanctions for non-compliance with Law 2004/63 are laid out under Chapter VII.

Section I (Articles 7 – 8) make provision for notifications to the National Authority for the Protection of Personal Data (“INPDP”) when processing operations are of a personal nature. Prior authorisations for the processing of various categories of personal information are required under Article 14 of Law 2004/63.

The basic principles for the processing of personal data are set out under Chapter II (specifically under Articles 9-14). Some of these principles require that:

- The processing of personal data must be done in the context of respect for human dignity, privacy and public freedoms (Article 9);
- The collection of personal data can only be carried out for lawful purposes, that is ‘determined and explicit’ (Article 10);
- Personal data must be treated fairly and to the extent necessary to the purposes for which they were collected (Article 11);
- Data Controllers must ensure that data are accurate and up to date (Article 11);
- The processing of personal data may not be carried out for purposes other than those for which they were collected except where sanctioned under the Act (Article 12);
- The processing of personal data relating to criminal records of a data subject is prohibited unless subject to an exception contained in the Act (Article 13); and
- The processing of personal data relating to racial or genetic origin, beliefs, religious, political, philosophical or trade unions, or health is prohibited unless subject to an exception contained in the Act (Article 14).
The processing of ‘special’ categories of data is catered for under Chapter V.

Data subject rights are set out in Section III of Law 2004/63 and include the rights to: retract consent (Article 27); the right of access (Article 32) and the right to object (Article 42).

Section II (Articles 9 – 26) sets out various obligations on data controllers and third-party processors. Confidentiality obligations on data controllers are provided for under Article 8 and Article 23, whilst security obligations on data controllers are provided for under Articles 18 – 19. The relationship between data controllers and third-party processors (‘sub-contractors’) is regulated under Articles 18 – 24. Interestingly, data controllers are required to choose sub-contractors ‘carefully’ (Article 20), both data controllers and sub-contracts have obligations to ensure that records are accurate and kept up to date (Article 21), and the obligations that apply to data controllers and sub-contractors also apply to any agents of a sub-contractor (Article 23). Obligations on data controllers relating to the preservation, erasure and destruction of personal data are contained between Articles 44-46.

Whilst Law 2004/63 is comprehensive, it has nonetheless been noted, with caution, that Law 2004/63 has a ‘major derogatory regime for processing of personal data by public authorities. This means that processing of personal data carried out by public persons is generally excluded.’ (Makulilo, 2016, 32)

**Draft Law 2018/25**

The Draft Law 2018/25 has been formally ratified by the Council of Ministers and has officially been referred to the Commission on Rights and Liberties (a specialised parliamentary commission that considers legislation that has the potential to impact or interfere with individual liberties) (Emna Sayadi, Dima Samaro & Klara Longfellow, 2019).

Saying this, it is important to note that the Draft Law 2018/25 has faced ongoing disapproval from civil society and other independent authorities in Tunisia who have criticised aspects of the draft law that have the potential to impact on the right to freedom of expression and the right of access to information. Specifically, Draft Law 2018/25 fails to differentiate between ‘public’ and ‘private’ personal information which falls contrary to both Article 24 (privacy) and Article 32 (access to information) of the Tunisian Constitution (Emna Sayadi, Dima Samaro & Klara Longfellow, 2019). No provisions protecting against surveillance through CCTV exist under Law 2018/25.

**The Draft Tunisian Digital Code**

In October 2018, the Ministry of Communications Technology and the Digital Economy introduced a draft Digital Code for Tunisia. The Digital Code focuses on three main axes: (1) the digital economy; (2) infrastructure and resources; and (3) digital confidence and cyber security.

The Ministry of Communications Technology and the Digital Economy launched public consultations on the draft Code in October 2018.

On 30 December 2019, the Digital Code was approved by the Tunisian Council of Ministers and returned to Parliament.

**Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data**

Tunisia has also acceded to the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”). In addition to providing guarantees concerning the collection and processing of personal data, in the absence of proper legal safeguards, Convention 108 prohibits the processing of “sensitive data” which includes data relating to a person’s race, political views, health, religion, sexual life, and criminal record. The Convention also provides individuals with a right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

**ECOWAS Supplementary Acts**

The Economic Community of West African States (ECOWAS) has an ICT legal framework revolving around: e-transactions (Supplementary Act A/SA.2/01/10); cybercrime (Directive 1/08/11) and personal data protection (Supplementary Act A/SA.1/01/10). The legal framework has yet to be implemented by its Member States (UNCTAD, 2019), Tunisia being one of such member states.

10.2.2. Data Protection Policy Developments

Tunisia does not have a national ICT policy that makes reference to data protection policy developments.
10.2.3. Data Protection Institutional Measures

The following institutions are relevant to Data Protection in Tunisia:

- The Ministry of Communications Technology and the Digital Economy;
- Tunisian Access to Information Authority (Instance Nationale d’Accès à l’information, INAI): The INAI was established under organic law n° 2016/22 of 24 March 2016 on the right of access to information. It has a mission to guarantee that citizens have access to public information.
- National Authority for the Protection of Personal Data (INPDP): Decree No. 3003 established Tunisia’s data protection body “l’Instance Nationale de Protection des Données à Caractère Personnel” (“INPDP”). The INPDP began to work efficiently since its inception in 2009 and ensures that specific activities related to the processing of personal data are subject to the authorisation of an administrative authority as stipulated in Article 10.4 of the AUCC; and
- The Commission on Rights and Liberties (CRL): the CRL is a specialised parliamentary commission that considers legislation that has the potential to prejudice protected rights and freedoms.

10.3. Cybercrime and Cybersecurity

10.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Tunisia are primarily governed by the following laws:

- Articles 199 and 199b of the Tunisian Criminal Code (“TCC”);
- Law No. 2004/5 of 3 February 2004 relating to electronic security and on the organisation of the field of computer security and setting the general rules for the protection of computer systems and networks (“Law 2004/5”); and

Other legal instruments that may impact the regulation of cyber-crimes and cyber security are:

- Decree 2004/1250 dated 25 May 2004 fixing the computer systems and networks of organisations subject to the periodic compulsory audit of IT security and the criteria relating to the nature of the audit and its periodicity and the procedures for follow-up on the implementation of the recommendations contained in the audit report;
- Decree 99/2768: it was under this Decree that the National Agency for Computer Security (“ANSI”) was created in 1999.
- Circular 19 dated 11 April 2007 regarding reinforcement of cybersecurity measures in public institutions;
- Circular 19 dated 18 July 2003 on safety and prevention measures for the buildings of ministries and local authorities and public enterprises;
- Decree 2008/2639 dated 7 July 2008 setting the conditions and procedures for importing and marketing encryption tools or services through telecommunications networks;
- Law 2005/51 dated 27 June 2005 relating to electronic transfer of funds (the "Electronic Transfer of Funds Law"); and
- Law 2015/26 dated 7 August 2015 regarding anti-terrorism and anti-money laundering (the “Anti-Money Laundering and Anti-Terrorism Law”).

Importantly, whilst the Tunisian Council of Ministers approved a draft ‘Cybercrime’ law that aims to “prevent and combat cyber-crimes of information and communication” (Emna Sayadi, Dima Samaro & Klara Longfellow, 2019), Tunisia does not currently have a consolidated and enforceable cybersecurity and cyber-crimes law – this draft Cybercrime law is not yet available for public comment. Apart from the patchwork of legal instruments described below, Tunisia does not have an omnibus law that adapts traditional offences or sanctions to information and communication technologies, or that provide for the protection of ‘critical infrastructure’ (despite the fact that Law 2004/5 excludes audits on computer systems and networks attached to the Tunisian defence Ministries).

Criminalisation of cyber-crimes through a patchwork of laws

The criminalisation of cyber-crime is not currently achieved by means of a dedicated cyber security and cyber-crimes law in Tunisia. Instead, the Tunisian Criminal Code, and a patchwork of other laws, make provision for criminal sanctions of various offences involving information and communication systems:

Article 199 bis of the TCC criminalises the:

- Unauthorised access to an automated data processing system;
- Modification or destruction of the system’s functioning or existing data;
- Intentional modification or destruction of an automated data processing system’s functioning; and
- Unauthorised insertion of data in an automated data processing system.
Article 199 ter of the TCC criminalises the:

- Harmful modification of an electronic document’s content.

A patchwork of other laws indirectly adapt certain offences / sanctions to Information and Communication systems:

- Electronic theft of data (which can extend to one’s identity) would be considered theft under Tunisian law (Article 261 of the TCC);

- The electronic theft of funds is considered an offence under the Electronic Transfer of Funds Law;

- Law 94/36 dated 24 February 1994 on literary and artistic property (the “Copyright Law”), prohibits the use of any protected work under copyright without obtaining proper authorisation is sanctioned. The misuse could be the result of an electronic theft; and

- Cauising an interruption of telecommunications by the breaking of lines or the deterioration or destruction of equipment by any means whatsoever (Denial-of-Service DDoS attacks) is an offence under Article 82 of the Code of Telecommunications.

Law 2004/5

Law 2004/5 primarily applies to public entities and companies that are operators of public telecommunications networks and providers of telecommunications and internet services, as well as companies whose computer networks are interconnected through external telecommunications networks, and companies performing automated processing of their customers’ personal data in connection with the provision of their services through telecommunications networks. In terms of Articles 5-9 of Law 2004/5, such entities must perform mandatory audits to assess their computer systems and networks at least once every twelve (12) months.

Article 10 Law 2004/5 also requires operators of computers systems or networks (whether public or private) to report ‘disturbances’ (breaches) to the National Computer Security Agency.

The Telecommunications Code

The Telecommunications Code details the conditions and procedures pertaining to the encryption of communications. Under the Code, the unauthorized use of cryptography is punishable by up to 5 years in jail. The unauthorised use of cryptography requires prior authorisation from the authorities. The Agence Nationale de Certification (ANC) is the authority that can grant such permissions.

The Draft Tunisian Digital Code

In October 2018, the Ministry of Communications Technology and the Digital Economy introduced a draft Digital Code for Tunisia. The Digital Code focusses on three main axes: (1) the digital economy; (2) infrastructure and resources; and (3) digital confidence and cyber security. The Ministry of Communications Technology and the Digital Economy launched public consultations on the draft Code in October 2018.

On 30 December 2019, the Digital Code was approved by the Tunisian Council of Ministers and returned to Parliament.

10.3.2. Cybercrime and Cybersecurity Policy Developments

The ‘National Trust in Cyberspace’ is Tunisia’s national policy coordinating cybersecurity efforts. It has been in existence since 2002. The policy provides for the creation of “more robust national information systems, legal aspects and strengthening the Tunisian cyber security workforce.” (African Union & Symantec, 91).

Tunisia has a national cybersecurity awareness campaign for children known as the Online Child Protection Initiative (COP). Tunisia also works with NGOs and civil society organizations to raise awareness about cyber risks. ANSI periodically organizes and conducts high-level training courses for Tunisian professionals (both public and private) (African Union & Symantec, 92).

A new Cybersecurity Strategy (2020-2024) has been drafted. However, it is not yet available for public consumption.

In June 2019, CyberSouth - a joint project of the European Union and the Council of Europe – hosted a meeting of the working group in charge of developing a manual on cybercrime and electronic evidence for Tunisian magistrates. According to CyberSouth, The Ministry of Justice and the Institut Supérieur de la Magistrature are strong supporters of this initiative and promote the specialisation of Tunisian magistrates.

10.3.3. Cybercrime and Cybersecurity Institutional Measures

Tunisia has the following cyber security and cyber-crime related institutions:

- The Ministry of Communications Technology and the Digital Economy;

- The National Agency for Computer Security (ANSI): The ANSI was established through Law 2004/5 and is responsible for controlling Tunisia’s information systems and ensuring the implementation of a general security strategy. It also conducts periodic audits of the systems and networks of operators in Tunisia.
The Tunisian Computer Emergency Response Team (TunCERT): the ANSI also hosts “TunCERT”, the emergency response team responsible for monitoring and supervising responses to cyber-attacks. TunCERT offers guidance to stakeholders in Tunisia on how to prevent attacks on vulnerable or sensitive infrastructure.

The National Agency for Electronic Certification. It also has the authority to grant permissions for the use of cryptography.

Circular 19 dated 11 April 2007 requires public enterprises to prevent Incidents through the creation of a “Computer Security Cell” in order to coordinate with the NISA and a “Computer Security Committee”. Also, per the guidance of the NISA, private entities shall implement a certified information security management system (“SMSI” in French) for the safe use of computer systems and networks.

10.4. ELECTRONIC TRANSACTIONS

10.4.1. Overview of Electronic Transactions Legislation

Electronic communications and transactions (in the context of electronic commerce) in Tunisia are governed by:

- Law 2005/51 dated 27 June 2005 relating to electronic transfer of funds (the “Electronic Transfer of Funds Law”);
- Decree 2001/1667 - Terms of reference relating to the exercise of the activity certification service provider;
- Decree 2000/2331 - Fixing administrative and financial organization and the operating procedures of the national electronic certification agency; and
- Decree 2639/2008 - Fixing the conditions and the procedures of importation and commercialization of means and services of encryption through the telecommunications network.

The Electronic Commerce Law

The objective of the Electronic Commerce Law is to promote e-business and facilitate its growth via the creation of a legal framework.

The validity of electronic writing is acknowledged in Article 4, whilst the validity of the use of electronic signatures is acknowledged in Article 5. On this note, the requirements for the use of electronic signatures are also provided for under Article 5, including taking minimum precautions relevant to the technical characteristics of the signature (laid down by the Ministry of Telecommunications); and utilise encryption. Obligations on electronic signature holders are also provided for under Article 5 which require that holders of electronic signatures inform the electronic certification service provider of any illegitimate use of his/her signature, as well as ensuring the veracity of all data reported to the electronic certification service provider (these requirements indirectly work towards securing/guaranteeing the safety of electronic transactions). Conversely, direct requirements to guarantee the safety of electronic transactions are provided for under:

- Article 17: requiring electronic certification service providers to only issue certificates that meet the security and reliability requirements set out via a Decree by the Ministry of Telecommunications;
- Article 18: requiring electronic certification service providers to guarantee:
  - The accuracy of the certified information contained in the certificate on the date of issue;
  - The link between the certificate holder and the signature verification;
  - Exclusive possession by the holder of the certificate of a signature creation device; and
  - Verify beforehand the identity and the power of representation of the natural person who presents himself to acquire an electronic signature.
- Article 19: requiring electronic certification service providers to revoke certifications in various circumstances.

The National Electronic Certification Agency is established and regulated under Chapter III of the Electronic Commerce Law, whilst electronic certification service providers are regulated under Chapter IV.

Electronic business transactions are regulated under Chapter V. Article 28 provides that (unless otherwise agreed upon between a seller and a consumer), an electronic contract is automatically entered into at the address of the seller and on the date of acceptance of the order by the consumer. Chapter V also requires online sellers to, amongst other things:

- provide consumers with various types of clear and understandable information (Article 25);
- provide consumers with all information related to the transaction within ten (10) days of entering into the electronic transaction (Article 29); and
- accept returns of goods/services ordered by consumers in certain circumstances (Articles 30-31).
Electronic business transactions are regulated under Chapter V. Article 28 provides that (unless otherwise agreed upon between a seller and a consumer), an electronic contract is automatically entered into at the address of the seller and on the date of acceptance of the order by the consumer. Chapter V also requires online sellers to, amongst other things:

Advertising by electronic means is not regulated under the Electronic Commerce Law, instead, this is regulated under Article 30 of Law 2004/63.

**The Draft Tunisian Digital Code**

In October 2018, the Ministry of Communications Technology and the Digital Economy introduced a draft Digital Code for Tunisia. The Digital Code focuses on three main axes: (1) the digital economy; (2) infrastructure and resources; and (3) digital confidence and cyber security. The Ministry of Communications Technology and the Digital Economy launched public consultations on the draft Code in October 2018.

On 30 December 2019, the Digital Code was approved by the Tunisian Council of Ministers and returned to Parliament.

**10.4.2. Electronic Transactions Policy Developments**

The implementation of the Tunisia’s electronic payment system titled ‘E-dinar’ by the Tunisian Post in 2001, as well as the secure online banking solution “Secure Payment Server” in 2005, both fostered the development of electronic commercial transactions (Tawfiq Jelassi, 2010). As early as 2005, a special unit attached to the Prime Minister’s office was created to coordinate and spearhead efforts to develop an “electronic government” program to make more services available online and boost the government’s digital readiness.

“As of November 2009, more than eighty (80%) percent of companies’ income taxes are paid online using electronic signatures, and all students in the country register online for their university classes” (Tawfiq Jelassi, 2010, 156).

In 2017, Tunisia ranked 99th among 176 other nations on the United Nations International Telecommunications Union’s ICT Development Index, a benchmarking tool based on eleven (11) major information and communications technologies (ICT) indicators used to measure ICT performance in and between countries (ITU, 2017).

The government of Tunisia is making efforts to promote digital payments. In May 2019, the Ministry of Finance introduced a set of new digital services to facilitate the payment of bills, taxes, and other charges by citizens and businesses. This set of new digital services, launched by the Ministry of Finance, is part of the national strategy to reduce the use of cash and increase electronic payments (Export.gov, 2019).

The ICT Ministry has introduced the Digital Code which will replace the Electronic Commerce Law. The Ministry introduced the Digital Code in response to a large number of cybercrimes taking place in Tunisia. The Digital Code is expected to create more institutions (cited below).

**10.4.3. Electronic Transactions Institutional Measures**

The following institutions play a fundamental role in Tunisia’s e-commerce:

- The National Electronic Certification Agency (Tuntrust); and
- The Ministry of Communication Technologies;
- The Ministry of Communications Technology and the Digital Economy;
- Under the Draft Tunisian Digital Code, the following new institutions relative to electronic transactions will be created:
  - The Internet Forum;
  - The Digital Development Fund;
  - The Tunisian Digital Development Foundation; and
  - The Digital Trust Services Committee.
10.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

<table>
<thead>
<tr>
<th>Policy and Governance Measures</th>
<th>Legislative and Regulatory Measures</th>
<th>Institutional Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Policy</strong> which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures.</td>
<td><strong>Data Protection Laws and Regulations</strong></td>
<td><strong>Data Protection Authority</strong> whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data.</td>
</tr>
<tr>
<td>The 'National Trust in Cyberspace' is Tunisia’s national policy coordinating its cyber security efforts.</td>
<td>Law 2004/63 of 27th July 2004 relating to personal data protection.</td>
<td>Decree No. 3003 establishes the National Authority for the Protection of Personal Data (&quot;l’Instance Nationale de Protection des Données à Caractère Personnel&quot; (&quot;INPDP&quot;)) as Tunisia's data protection body.</td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td>The Draft Basic Law No. 2018/25 on the protection of personal data.</td>
<td>Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications.</td>
</tr>
<tr>
<td>A new Cybersecurity Strategy (2020/2024) has been drafted. However, it is not yet available for public consumption.</td>
<td>And</td>
<td>The National Electronic Certification Agency (TunTrust) is the authority.</td>
</tr>
<tr>
<td><strong>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture</strong></td>
<td>The draft Digital Code.</td>
<td><strong>State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;</strong></td>
</tr>
<tr>
<td>The National Agency for Computer Security (&quot;ANSI&quot;) periodically organizes and conducts high level training courses for Tunisian professionals (both public and private).</td>
<td><strong>Electronic Commerce Laws and Regulations</strong></td>
<td>The Ministry of Communications Technology and the Digital Economy deals with the regulation of all electronic commerce payment methods.</td>
</tr>
<tr>
<td>Tunisia also has a national cyber security awareness campaign for children known as COP.</td>
<td>Law 2000/83 dated 9 August 2000 (the Electronic Commerce Law) .</td>
<td><strong>State Department to regulate vulnerability and safety guarantee assessments of ICT product vendors including ensuring mandatory disclosures of vulnerabilities and the solutions to such vendors consumers</strong></td>
</tr>
<tr>
<td>Cyber security is primarily criminalised in the Tunisian Criminal Code (&quot;TCC&quot;);</td>
<td>Decree 2001/1667; Decree 2000/2331; and Decree 2639/2008.</td>
<td><strong>Institutions with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution</strong></td>
</tr>
<tr>
<td>And</td>
<td><strong>Legislative and regulatory measures to identify the sectors regarded as sensitive for their national security and well-being of the economy (critical infrastructure), and measures to improve vigilance, security and management in such sectors</strong></td>
<td><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation</strong></td>
</tr>
<tr>
<td>The Telecommunications Code, 2001;</td>
<td>Tunisia does not have any omnibus laws that provide for the protection of 'critical infrastructure'</td>
<td>The Tunisian Computer Emergency Response Team (TunCERT).</td>
</tr>
<tr>
<td>In draft is the ‘Cybercrime’ law and the Digital Code.</td>
<td></td>
<td>And</td>
</tr>
<tr>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong></td>
<td></td>
<td>The National Agency for Computer Security (&quot;ANSI&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Tunisian Computer Emergency Response Team (TunCERT).</td>
</tr>
</tbody>
</table>
Disclaimer

This report was prepared independently by EndCode.

This report is based on a variety of inputs from multiple sources including official and private data sources such as public and governmental institutions, international organisations, academic research, news articles, sector reports and interviews with various stakeholders.

Accuracy of analysis and recommendations provided are dependent on the detail and accuracy of available and declared data. The information given herein is for informal guidance only and neither AUDA-NEPAD nor EndCode, nor any company or organisation stated within this paper makes any expressed or implied warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process disclosed.

AUDA-NEPAD nor EndCode bear no responsibility for any use that may be made of this report. Should you have any queries about the content within this report, please contact AUDA-NEPAD.

About EndCode

EndCode is a specialist advisory firm - servicing local, regional and international organisations navigating technology laws and policies in Africa. EndCode believes that it can promote access to the benefits of technology and innovation on the continent by growing the body of insights available in technology law and policy areas. EndCode is distinguished by its multidisciplinary expertise in law, policy, research and advocacy in the technology environment.