TABLE OF CONTENTS

July 2020

1. THE LAW

1.1. Overview of the privacy/data protection situation

The Democratic Republic of Congo ('DRC') consecrates the respect for private life and the secrecy of correspondence as a fundamental right. There is no specific constitutional article on the protection of personal data and there is no specific and comprehensive legislative framework on data protection. In fact, the data protection rules are spread over several laws and decree-laws. Curiously, as you will see in section 2 of this Note, the only definition of personal data is only to be found in the Decree-Law that establishes the measures of application of the Customs Code.

1.2. Constitutional provisions

The Constitution of the Democratic Republic of Congo (only available in French here) was enacted on 18 February 2006, as amended by the Law 11/2002 of 20 of January 2011 ('the Constitution'). Article 31 of the Constitution, under the title 'Human Rights, fundamental freedoms and the duties of the citizen and the State,' chapter 'Civil and Political Rights,' establishes that: 'Everyone has the right to respect for his or her private life and the secrecy of the correspondence, telecommunication or any other form of communication. This right may be only infringed in the cases provided by law.'

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

- Law No. 013/2002 (only available in French here) ('the Telecoms Law') governs the telecommunication sector;
- Law No. 04/016 of 19 July 2009 concerning the fight against money laundering and terrorism funding (only available in French here) ('the AML Law') and Instruction N15 from 15 December 2006 ('Instruction N15') enacted by the Central Bank of the DRC ('the Central Bank').

1.4. Case law

We are not aware of any relevant case law in the DRC regarding privacy and data protection matters, which may be due to the public/non-public format of official sources on these matters, as well as the absence of a specific legal framework aimed specifically at data protection, which may have an impact on public and private sensitivity on the matter regarding the possibility of initiating judicial procedures.

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

- Law 10/002 of 20 August 2010 (only available in French here) establishing the Customs Code and Decree-Law 011/46 of 24 November 2011 (only available in French here) regarding the application measures of the Customs Code (jointly 'the Customs Regime').

1.6. Possible amendments/draft data protection laws under discussion

Not applicable.

2. SECTORAL LEGISLATION

2.1 FINANCIAL SECTOR

2.1.1. Law: Scope of application/ Key provisions

Applies to any natural or legal person who, within the framework of its profession, carries out, controls, or advises on operations deposits, exchanges, investments, conversions, and all other movements of capital, in particular to:

- the Central Bank;
- credit Institutions, financial companies, micro-finance institutions, credit and exchange agencies, insurance undertakings, insurance intermediaries, leasing companies, and other financial intermediaries;
- postal order services;
- stockbrokerage firms, intermediaries in stock exchange operations, management companies of wealth, companies offering investment services, and undertakings for collective investment in transferable securities;
- lottery companies;
- managers, owners, and directors of casinos;
- notaries;
- real estate agencies;
- travel agencies;
- to members of the independent legal professions, including lawyers, when they advise or assist clients, in the cases provided by law;
- auditors and consultants; and
- art dealers.

Credit institutions shall be required to ensure the identity and address of their costumers before entering in a business relationship with a natural or legal person. Namely, the AML Law requires that:

- verification of the identity of a natural person shall be carried out by the presentation of a valid, original, and official document with a photograph, and a copy of the document must be taken. Moreover, the address must be proven by a substantiating document; and
- the identification of a legal person shall be carried out by the verification of company's statutes and a document proving that it has been legally constituted and that it has a real existence at the time of identifications, and a copy of the documentation must be taken.

The documentation must be saved for ten years after the closing of the accounts or the termination of the relationship with the natural or legal person, and must be kept at the disposal of the following entities:

- the Central Bank;

- officials responsible for the detection and repression of money laundering and terrorism funding holding judicial warrant; and
- the Financial Intelligence Unit ('CENAREF').

The documentation must only be communicated to other natural or legal persons with authorisation.

2.1.2. Case law

Please refer to point 1.4. above.

2.1.3. Presence of a regulator, its role/powers

The regulator is the Central Bank and it has the power to impose administrative sanctions, as well as to initiate disciplinary proceedings.

The AML Law has created the CENAREF, an administrative authority under the supervision of the Ministry of Finances and Budget, which has the competence to receive and analyse financial information to establish the origin of suspicious transactions.

2.1.4. Key definitions

Not applicable.

2.1.5. Data retention

The referred documentations must be kept for ten years within the conditions described in 2.1.1.

2.1.6. Specific provisions on data breach and data breach notification

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

2.1.7. Specific provisions imposing limitations on data transfers

There are no specific provisions imposing limitations on data transfers.

2.1.8. Sanctions and penalties

The sanctions and penalties provided by the AML Law and Instruction N15 are the following:

- when, as a result of either a serious lack of vigilance or of a failure to act, the supervisory authority may act, *ex officio*, under the conditions laid down in the professional and administrative regulations. In this case, it shall notify the CENAREF of the disciplinary proceedings initiated;
- those who communicate information or documentation to other entities than the ones permitted by law shall be punished by imprisonment from two to five years and a fine;
- those who have not complied with the identification obligation shall be punished by a fine of up to three times the amount of money laundered;
- the persons who are guilty of the above-mentioned offences may be sentenced to a permanent or temporary ban of practising the profession in which the offence has been committed; and
- the Central Bank may attribute an administrative sanction and communicate publicly the infraction.

2.2 HEALTH AND PHARMA SECTOR

2.2.1. Law: Scope of application/ Key provisions

Decree-Law 18/049 of 18 December 2018 (only available in French here) creates and establishes the organisation and function of the National Agency for Clinical Engineering and Health Informatics ('ANICiiS'), placed under the direct authority of the Ministry of Health.

The mission of the ANICiiS is to develop health informatics in the DRC that include: digital health, e-health, telemedicine, medical robots, Big Data and/or open health data, digital mapping of the use of unmanned aerial vehicles ('UAVs') in the health logistics chain, the maintenance of biomedical equipment, bioinformatics, predictive medicine, and others.

2.2.2 Case law

Not applicable.

2.2.3 Presence of a regulator, its role/powers

Not applicable.

2.2.4. Key definitions

Not applicable.

2.2.5. Data retention

Not applicable.

2.2.6. Specific provisions on data breach and data breach notification

Not applicable.

2.2.7. Specific provisions imposing limitations on data transfers

Not applicable.

2.2.8. Sanctions and penalties

Not applicable.

2.3 TELECOMMUNICATIONS SECTOR

2.3.1. Law: Scope of application/ Key provisions

Telecoms Law

The Telecoms Law regulates the telecommunications sector in the DRRC and:

- determines the terms and conditions for the ownership, installation and operation of telecommunications throughout the national territory;
- guarantees the harmonious and integrated development of telecommunication networks and services; and
- facilitates the mobilisation of financial resources through the participation of the private sector in the development of telecommunications in a fair competitive environment.

Although the Telecoms Law does not define personal data, nor does it include a specific provision governing the processing of personal data, certain provisions indirectly concern, and impact privacy and data protection matters.

Note that the Telecoms Law includes a concept of data protection for the specific purpose of this law. In this context, data protection is considered the protection of personal data, the confidentiality of the information transmitted and stored, and the protection of privacy.

Under this law, one of the essential requirements for the imposition of conditions on the establishment and/or operation of telecommunications networks, or to the provision of telecommunications services is data protection.

Concession contracts regarding telecommunications networks must include confidentiality obligations. Additionally, as regards telecommunications services for value-added services, including direct data processing, direct database registration and retrieval, electronic data interchange, email, and voicemail, an authorisation is necessary.

The Telecoms Law allows for the provision, exploitation, and use of encryption services by entities. In order to safeguard the interests of state security, the provision, exploitation, and use of these services shall be subject to prior declaration to the national telecom regulator when the only purpose is to guarantee the secrecy and integrity of the communications or obtain written authorisation from the Minister of National Security and Defence, in the other cases.

All stakeholders are obliged to respect the confidentiality of telecommunications and cannot intercept, record, transcribe, and/or disclosure any communication without prior authorisation from the Attorney General of the DRC. This authorisation may only be granted if motivated by the need to assert truth in a judicial proceeding. The Minister of the Interior may also authorise the interception of communications if regarding national security, the protection of the essential elements of the scientific, economic, and cultural potential of the country, or the prevention of crime and organised crime.

2.3.2. Case law

Please refer to point 1.4. above.

2.3.3. Presence of a regulator, its role/powers

There is no national regulator specifically charged with monitoring and controlling compliance with data protection and privacy matters.

In the telecom sector and since there are provisions in the respective law with impact on data protection, we would just note that the Post and Telecommunications Regulatory Authority ('ARPTC') is the national telecom regulator and one of the main purposes of this authority is to ensure that telecoms providers comply with all laws, regulations, and conventions related to postal services and telecommunications. Moreover, the ARPTC can conduct site visits, investigate, and assemble all the necessary data to ensure that all the stakeholders comply with the secrecy of the communications.

2.3.4. Key definitions

Given that there is no autonomous data protection law, there are no overall formal privacy definitions. However, the following definitions, that have an impact on privacy and data protection stem from the Telecoms Law.

Essential requirements: The reasons for imposing conditions relating to the establishment and/or operation of telecommunications networks or the provision of telecommunications services. These reasons shall be the security of operation of the network, the maintenance of its integrity and, where justified, the interoperability of services, data protection, the protection of the environment, and town and country planning objectives, as well as the rational use of the frequency spectrum and the prevention of harmful interferences between radio telecommunications systems and other systems based on terrestrial or space technology. Data protection may include the protection of personal data, the confidentiality of information transmitted or stored, and the protection of privacy.

Value-added services: All telecommunications services which, while not final telecommunications services, add other services to the support service or meet new specific telecommunications needs. We have included this as a relevant definition, since examples of these services may include direct data processing through direct database registration and retrieval, electronic data interchange, email, or voicemail.

2.3.5. Data retention

There are no provisions on data retention.

2.3.6. Specific provisions on data breach and data breach notification

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

2.3.7. Specific provisions imposing limitations on data transfers

There are no specific provisions imposing limitations on data transfers.

2.3.8. Sanctions and penalties

The sanctions provided by the Telecoms Law are the following:

- anyone who alters, copies without authorisation, or destroys any correspondence sent by telecommunications, and/or opens or takes possession of it to gain improper knowledge of it shall be punished by imprisonment for six months and/or a fine not exceeding CDF 100,000 (approx. €45);

- any agent in the service of an operator or public telecommunications services who has committed one of the acts provided for in the preceding point, or has facilitated it, or who has intentionally omitted, distorted, or delayed the transmission of correspondence by telecommunications, shall be punished by imprisonment for a maximum of one year and/or a fine not exceeding CDF 100,000; and
- any agent in the service of a public telecommunications service provider shall be punished by imprisonment of up to six months and/or a fine not exceeding CDF 100,000, if they have revealed or ordered to be revealed the existence or content of correspondence sent by telecommunications, except where required by law.

3. OTHER JURISDICTIONAL ISSUES

3.1 Imports and exports

Customs Regime

For the purposes of the application of the Customs Regime, any person directly or indirectly interested in the operations carried out shall provide the Customs Authority, at the latter's request, with all the required information.

This information may refer to information that does not constitute personal data, such as data on assets, financial, and logistical data, however, as it may also involve the processing of personal data, we have decided to include it in this section.

In order to facilitate customs procedures and enhance the quality of controls, the Customs Authority shall, wherever possible, use new technologies to:

- collect data;
- process customs procedures;
- carry out controls;
- manage and control goods and travellers; and
- exchange and disseminate information.

In this sense, all information of a confidential nature, or provided on a confidential basis, shall be covered by professional secrecy and may not be disclosed by Customs Authority without the express permission of the person who provided it.

The communication of information shall only be permitted in so far as the Customs Authority is required or authorised to do so in accordance by law, namely regarding data protection or in connection with legal proceedings.

The Customs Authority shall freely determine the modalities and conditions of access to its systems. However, the Customs Authority shall maintain a high level of security of its computer systems to ensure that they are only used for the intended purpose. In this sense, any user allowed to access the systems must sign a security policy, which must define:

- safety specifications for the use of the computer system;
- conditions and procedures to ensure identification, access, and use of the computer systems;
- responsibilities of the persons concerned;
- the modalities of electronic signature; and
- criminal sanctions.

From what we know, the Customs Authority has yet to elaborate and implement this security policy. Moreover, the security measure in place to protect the data must be guided by the principles of integrity, authentication, non-repudiation, confidentiality, and availability.

The Customs Authority is bound to implement the data security measures and the most recognised standards at an international level. To achieve the safety of the electronic transactions and data, the Customs Authority must use the most reliable procedures of electronic signatures. Electronic signature processes shall be presumed to be reliable until proven otherwise, provided that the signature is secure, it is created using a signature creation device, and that the electronic certificate, where applicable, is qualified.

To presume that the electronic signature creation device is secure and reliable, the device must link the electronic signature to the signatory, to enable the electronic signature to be created by such means that the signature is under exclusive control of the signatory, and securely store data in such a way that any future changes to it are detectable.

The Customs Authority may also use qualified electronic signatures. In this case, the use of such procedure must include:

- a statement indicating that it is issued as a qualified electronic certificate;
- the identity of the provider of electronic certification, their electronic signature, as well as the State in which it is established;
- the names of the signatory or a pseudonym, which must be identified as such;

- an indication of the status of the signatory, where appropriate;
- signature verification data;
- expiry date of the certificate;
- the code of the certificate; and/or
- where applicable, the conditions of use of the electronic certificate, including the maximum amount of transactions for which the certificate can be used.

The Customs Authority is required to set up the technical resources necessary for the implementation of the electronic signature. In the event of recourse to an external service provider for the implementation of the electronic signature, the Customs Authority shall use service providers internationally renowned.

In addition, the Customs Authority is obliged to inform individuals to whom the data concerns as to the terms of the data processing and shall ensure compliance with the legal and regulatory provisions relating to the freedoms of the persons concerned. The Customs Authority shall ensure that the individual can access their data and correct it, when appropriate.

The Customs Authority, as the entity legally responsible for all operations that are carried out, directly or indirectly by itself, on the data contained in its systems, and particularly on personal data, must ensure that all its service providers present sufficient guarantees of secure and confidential data processing. When third parties manage customs data or part of the data in customs computer systems, the personal data must be encrypted. To this end, service providers cannot disclose the data to third parties nor use such data for purposes not defined. At the end of the contract, the service providers must refund or destroy the Customs data, at the Customs Authority request.

3.1.2 Key definitions

Personal data: is any information related to an identified or identifiable natural person, directly or indirectly referencing an identification number, or one or more elements specific to his/her physical, physiological, genetic, psychological, cultural, social, or economic identity.

Signature creation device: set of personal encryption elements or configured set of equipment specifically for the creation of electronic signatures.

Signatory: means a person who holds the information regarding the electronic signature and who is either acting on their own behalf, or for the person they represent;

Electronic signature: data contained in a message, attached to a message or logically associated with a message, which can be used to identify the signatory;

Customs computer systems: all the computerised means and telecommunication to process, automatically store, and circulate customs information.

3.1.3 Data retention

The information and documents must be kept for a period of ten or 15 years, as determined by a customs check.

3.1.4 Specific provisions on data breach and data breach notification

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

3.1.5 Specific provisions imposing limitations on data transfers

There are no specific provisions imposing limitations on data transfers.

3.1.6 Sanctions and penalties

Not applicable.

3.2 Cybersecurity

Although the DRC is part of the African Union, it has yet to ratify the African Union Convention on Cyber Security and Personal Data Protection (27 June 2014).

On this note, the stakeholders have been advocating for a more comprehensive cyber law, providing more rights to internet users. In this regard, in February 2020, a Member of Parliament drafted a law on cybersecurity and cybercrime to be included, if accepted, on the political agenda being debated by the Chamber on the National Assembly. As far as we are aware, this draft has not, at this stage, been approved into law.