TABLE OF CONTENTS

September 2020

1. THE LAW

1.1. Key Acts, Regulations, Directives, Bills

Specific legislation on data protection has been approved relatively recently in the country.

On 10 October of 2019, the Republic of Congo ('Congo') adopted Law 29-2019 on the Protection of Personal Data (only available in French here) ('the Law'). The Law's main objectives are to:

- set up a framework that ensures the protection of the fundamental rights and freedoms of natural persons, namely their privacy, regarding the processing of personal data;
- guarantee that information technology and communication remain at the service of citizens and do not infringe private and public freedoms, in particular the right to private life;
- ensure that, while the processing of personal data is conducted according to the fundamental rights, State prerogatives are also considered, as well as the rights of decentralised public administration entities, and the interest of companies and the civil society.

The majority of the essential principles and diligence arising from the Law are similar to those established under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), this may be related to the fact that it is a very recent law, that was enacted following the EU application of the GDPR. Moreover, the Law also contains provisions regarding privacy on the electronic communications sector that also reflects the principles underlying the EU's Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive').

In addition to the Law, which is a detailed and comprehensive legislation, there are other legal documents that include data protection provisions, specifically:

- Law 09/2009 dated 25 November 2009 regarding the regulation of the electronic communication sector (only available in French here) ('the Law 09/2009');
- Order No. 11221 from 31 December of 2010 laying down the procedures for identifying subscribers of fixed and mobile services and the retention period of electronic communication data (only available in French here) ('the Order No. 11221'); and
- Decree-Law No. 2010-554 from 26 of July 2010 regarding the identification of subscribers of fixed and mobile services and the retention period of electronic communication data (only available in French here) ('the Decree-Law No. 2010/554') (jointly referred to as, the 'Electronic Communications Framework').

In what concerns the Electronic Communications Framework, detailed below, are specific provisions and principles in the diplomas included in this framework, with direct impact on privacy and data protection:

- Law 09/2009 regulates the electronic communications sector in Congo and establishes the conditions with which service providers and networks operators must comply regarding the confidentiality of the electronic communications, as well as obligations regarding numbering, mailing and portability under the responsibility of the governmental Agency for Post and Electronic Communications ('ARPCE');
- Order No. 11221 lays down the procedures for the identification of subscribers concerning fixed and mobile services, users of electronic communications and data retention periods. In this context, the operators shall retain, throughout the duration of the subscription, the subscribers' identification data;
- Decree-Law No. 2010/554 establishes an obligation to ensure that electronic communications databases include incoming and outgoing calls, including those made without ID caller identification. The technical data to be retained in this context must allow for the geographical location of calls and the operators shall communicate this data to authorised national security services, upon request;
- Decree-Law No. 2009/156 dated 20 of May 2009 regarding public contracts (only available in French here) ('the Public Contracts Code'). The Public Contracts Code establishes that the communication, exchange and storage of information in the context of public contracting must ensure the integrity of data and the confidentiality of offers and requests to participate in public procurement procedures and other public contract processes.
- Law No. 26-2020 dated 5 of June 2020 regarding cybersecurity (only available in French here) ('the Law No. 26-2020'). The Law No. 26-2020, provides a framework for cybersecurity in Congo. Specifically, it identifies measures that must be put in place to guarantee the integrity, confidentiality, and security of data, such as authentication mechanisms and other recognised cybersecurity standards. Additionally, it also states the need to ensure the secu-

rity of information systems and networks in light of legal and regulatory obligations and standards applicable in the country (including for the purpose of protecting personal data). Under this law, in the event of any attack, intrusion and other disruptions that can hinder the operation of an information system or another electronic communications network, information system or network operators (regardless of whether they are public or private), must:

- promptly inform the Agence Congolaise des Systèmes d'Information ('ACSI') so that this entity may take the necessary measures; and
- inform users of the dangers incurred when using their networks and of the risks of security breaches and, when applicable, of the absence of technical means to ensure the security of their communications.

- Law No. 16-2020 also sets out further duties for network operators, electronic communications service providers and information system operators, including data retention obligations. Specifically, these entities must retain connection and traffic data for a period of ten years and install data traffic monitoring mechanisms on their networks and systems. Information system operators may provide this information in the event of a judicial order. Regarding network operators and electronic communication service providers their data must only be accessible to judicial investigators. Network operators and electronic communications service providers are liable for the use and retention of data in breach of applicable laws and regulations. Every (public or private) intervening party must conduct regular risk assessments, including key internal and external factors, in order to maximise safety and to achieve the desired level of digital security, primarily in a logic of self-regulation.

Electronic communications operators and information systems' content providers are required to ensure the availability of the contents, as well of the data contained in their facilities, subject to filters that ensure that no infringements may occur that are detrimental to the privacy and personal data of users.

- Law No. 27-2020 from 5 of June 2020 concerning the fight against cybercrime (only available in French here) ('the Law No. 27-2020'). The purpose of the Law N 27-2020 – which was also approved very recently - is to define and regulate information and communication technology offences, as a complement to any sanctions and penalties included in the country's Criminal Code ('the Criminal Code').

The provisions of the Law N 27-2020 shall apply to all persons, whatever their nationality, who have committed an offence through information and communication technologies in Congo, including offences concerning personal data protection. In this regard, Law N 17-2020 provides for the following:

- imprisonment for one to five years and/or a fine between one to ten million CFA Francs (approx. €15,270) to:
    - anyone who carries out processing of personal data without respecting the formalities imposed by law;
    - whomever continues to process personal data after the temporary lifting of the authorisation or after it has been temporarily prohibited;
    - anyone who fails to comply with the standards or exemptions established;
    - anyone that carries out processing activities regarding the citizen card number without having the required authorisation;
    - whomever carries out processing operations without implementing security measures to ensure data security, and in particular to prevent data from being distorted, damaged or access by unauthorised parties;
    - anyone who collects personal data by unlawful means;
    - anyone who processes data for direct marking purposes despite the opposition of the person concerned;
    - anyone who inserts in an informatic medium, without the consent of the person concerned, special categories of data;
    - anyone who processes personal data for health research without informing the persons concerned of the terms of the processing operation and without obtaining their express consent;
    - anyone who retains the personal data for longer that is required, unless retention is carried out for historical, statistical or scientific purposes, in the conditions laid down by law;
    - anyone who diverts personal data from being used for its intended purpose; and
    - anyone who discloses personal data without consent, knowing that the disclosure will have a prejudicial effect on the person concerned.
- imprisonment for six months to two years and/or a fine between one to ten million CFA Francs (approx. €15,270) to anyone who hinders the action of the personal data protection authority; or
- imprisonment for six months to five years and/or a fine between three hundred thousand to five million CFA Francs (approx. €460 to €7,600) to anyone who, negligently and without consent, discloses personal data.

1.2. Guidelines

Please refer to section 3.

1.3. Case Law

As far as we are aware, Congolese case law is scarce, as information is generally not entirely publicly accessible, and not well organised. Any analysis regarding this matter must be sector specific and subject to a case by case analysis.

2. SCOPE OF APPLICATION

Title I, Chapter 1 of the Law establishes the Law's scope of application.

2.1. Who do the laws/regs apply to?

The following are subject to the Law:

- any processing operation carried out by an individual or a legal entity, both in the public and private sector, by the State and by its decentralised administrative authorities and entities;
- any processing operation carried out by a data controller on Congolese territory or in any place where Congolese law applies (in the case of the latter, a local controller representative should be appointed); or
- any processing operation carried out by a data controller, whether established within Congolese territory or not, which uses means of treatment located in Congo, except for those that are only in transit on Congolese territory.

2.2. What types of processing are covered/exempted?

The Law applies to any personal data processing, specifically:

- any collection, transmission, processing, and retention of personal data by a natural, legal, private, or public person, by the State and by its decentralised administrative authorities and entities;
- any automated or non-automated processing of data contained or to be included in a file (with the exemptions set out in the following paragraph); or
- any personal data concerning public security, defence, investigation, and pursuit of criminal breaches or State security, including when the processing is linked to important economic or financial State interest, subject to any applicable derogations.

Excluded from the Law are:

- the processing of data carried out in the course of purely personal or domestic activities, except when personal data is intended for systematic communication to third parties or dissemination; and
- temporary copies associated with technical transmission and provision of access to a digital network for the purpose of automatic, transient and intermediate storage of data, for the sole purpose of allowing certain parties with the best possible access to the data.

3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

3.1. Main regulator for data protection

The Law provides for the institutional creation of a national data protection authority, the Commission, by a legislative act. As far as we are aware, this Commission has not yet been formally established and no statutes have been approved or are otherwise available.

3.2. Main powers, duties and responsibilities

There is no chapter devoted to the powers, duties, and responsibilities of the Commission. However, the Law determines that its powers and responsibilities include:

- receiving complaints, petitions and claims relating to the processing of personal data of an individual;
- receiving the declarations of the data controllers regarding processing operations;
- authorising processing operations that involve a high risk to rights and liberties of individuals;
- establishing and publishing standards for simplified personal data processing declarations;
- giving opinions on Data Protection Impact Assessments ('DPIAs'); and
- monitor compliance with data protection obligations.

4. KEY DEFINITIONS | BASIC CONCEPTS

The definitions are listed in Title 1, Chapter 2 of the Law. We provide below some of the major definitions and concepts used throughout:

Personal Data: Any information related to an identified or identifiable natural person, directly or indirectly referencing an identification number, or one or more elements specific to their physical, physiological, genetic, psychological, cultural, social, or economic identity.

Data Controller: Any natural, legal, public or private person, any organization or association which, alone or with others, makes the decision to collect and process personal data and determines the purposes thereof.

Any natural or legal, public or private person, any organization or association that processes data on behalf of the data controller.

Data Subject: The individual whose personal data is processed.

Data Subject consent: Any unequivocal, free, specific and informed manifestation of will, by which the data subject or his/her legal, judicial or conventional representative, accepts that his/her personal data is processed either by electronic means or manually.

Third party: Any natural, legal, public or private person, any organization or association other than the data subject, the controller, the processor, the sub-contractor and persons who, under the direct authority of the controller or processor, shall be entitled to process the data.

Special categories of data: Genetic data, data related to minors, data regarding offences, criminal convictions or security measures, biometric data, all personal data relating to religious, philosophical or political, opinions or activities trade union, sex life, race, health.

Third country: Any foreign State that is not a member of the Economic Community of Central African States ('CEEAC').

Remote service: All provision of value-added services, by means of telecommunications or information technology, allowing, in an interactive manner and at a distance, that an individual or moral person, public or private, to carry out activities, procedures or formalities, etc.

Processing of personal data: Any operation or set of operations provided in Article 2 of the Law, whether carried out using automated or non-automated processes, such as the collection, retention, organisation, adaption, modification, extraction, communication, consultation, or any other form of processing, the interconnection, the encryption and the erasure or destruction of personal data.

Third parties: Any individual or a legal entity, both in the public and private sector, any organisation or association other than the data subject, the data controller and the data processor or the persons who, under the direct authority of the controller or processor, are authorised to process the data.

Direct marketing: Any message, whatever the medium, of commercial, political or charity nature, intended to promote, directly or indirectly, goods, services or image of a person selling goods or providing services.

Recipient: Any person entitled to receive personal data besides the data controller and the data processor.

5. NOTIFICATION | REGISTRATION

5.1. Requirements and brief description

Title II, Chapter 4 of the Law establishes the formalities that must be followed to perform processing operations, which may include either prior notification to or authorisation from the Commission.

A prior authorisation is applicable in the event of:

- processing of personal data relating to genetic data or health research;
- processing of personal data relating to criminal offences, convictions or security measures;
- processing of personal data for the purpose of interconnection, as defined by law;
- processing of a national identification number or any other identifier;
- processing of personal data containing biometric data; or
- processing of personal data for reasons of public interest, in particular for historical, statistical or scientific purposes.

The Commission shall take a decision within two months of receipt of the request. The time limit may be renewed and extended once by a decision from the President of the Commission. In the event that the Commission has not taken a decision within these time limits, the application for authorisation should be presumed to have been rejected.

Some specific data processing activities are subject to presidential approval:

- processing carried out on behalf of the State, by a public authority, by a decentralised administrative authority, by a legal private person providing a public service; and

- processing aimed at State security, defence, or public safety, or which is carried out for the purpose of preventing, investigating, detecting, pursuing, or executing criminal infractions is approved by the President of Congo, subject to prior opinion by the Commission.

The processing of pensions, salaries, taxes, other liquidations, public census, or the processing of special categories of personal data by these entities must be approved by legislative measures.

All other data processing operations are subject to prior notification to the Commission, except if a complete exemption from notification or authorisation applies – specifically, the activities which are exempt from the law, as identified in 2.2. above.

Note that, even in the event of exemptions, the data controller must ensure compliance with the data subjects' rights.

The Commission is obligated to create a notification template, in which the data controller must certify that the processing of personal data is carried out in accordance with the law. The Commission shall deliver, within one month, a receipt that allows the data controller to carry out data processing operations. This time limit may only be renewed once.

Additionally, the Commission shall establish standards for data processing operations which, due to their simplicity and low-risk level, may be subject only to a simplified notification process or even an exemption of the declaration obligation. The standards shall include:

- the purposes of the processing operations subject to the simplified notification;
- the data retention periods;
- the recipients or categories of recipients to whom personal data are communicated;
- personal data or categories of personal data processed; and
- the category or categories of persons concerned.

These standards shall consider any Codes of Conduct approved by the Commission.

Furthermore, the Commission may decide that different data processing operations concerning the same purpose, identical categories of data and with same recipients may be subject to a single notification.

Notifications and requests for authorisations may be sent by electronic means or by postal services and shall specify:

- the identity of the data controller or the identity of its representative, if the data controller is not established within the Congolese territory;

- the purposes of the data processing as well as a general description of its functions;
- the predicted interconnections or any other connection with other data processing operations;
- the personal data intended for processing, its origin and the categories of persons concerned;
- the retention periods;
- the service(s) responsible for carrying out the processing and the categories of persons who, by reason of their duties or for the purposes of the service, have directly access to the personal data;
- the function of the person or department to which the right to access is exercised;
- the security measures in place to ensure the safety of the personal data;
- indication of the use of a data controller; and
- the intended transfer of personal data for a third country.

If any of the elements referred to above changes, the data controller must submit a new declaration/authorisation.

Upon termination of the processing, the controller must inform the Commission.

6. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

The data controller responsibilities are listed in Title III, Chapter 2 and can be categorised into six main groups:

- **Confidentiality:** the data controller must assure that the processing of personal data is only carried out under his authority and instructions; the data controller must guarantee that only individuals who have technical and legal knowledge regarding the integrity of data deal with personal data, in this sense the data controller must have those individuals signing an agreement where they undertake to comply with the obligations provided by law;
- **Retention:** the data controller must guarantee that the data is kept for no longer than the purpose for which was collected.
- **Security:** the data controller must take any appropriate precautionary measures at the time of determination of the means of processing and during the processing itself, regarding the nature of personal data, to ensure data security. Namely, the data controller must (i) ensure that only authorised persons can access the personal data by creating different levels of access permissions, on a need-to-know basis depending on the position of its employees, (ii) ensure the identity of the person who wants to access the data or the identity

of the parties to whom the data will be disclosed, (iii) keep a record of who accesses the personal data, when and why, ensuring traceability of its use, (iv) prevent any unauthorised access to premises and equipment used for data processing, (v) maintain backups in secondary sources to prevent accidental changes or loss of data, (vi) prevent the unauthorised introduction of any data in the information system as well as any acquaintance, any unauthorised alteration or deletion of the data of recorded data, (vii) prevent that data carriers be read, copied, modified, destroyed, or displaced by an unauthorised person, (viii) use encryption or pseudonymisation;

- **Transparency:** the data controller must inform the data subject of the terms of processing, when the data is not collected from the data subject, the data controller must inform the data subject at least before the first communication; the data controller must guarantee that has a lawful basis to carry out the processing operation; the data controller must inform data subjects in a clear and plane form; the data controller must cooperate with the Commission in the pursuit of the Commission's activities;
- **Recording:** the data controller must maintain a record of its processing activities. The record shall contain (i) the name and contact details of the data controller or joint data controllers, if applicable, (ii) the purposes of the processing operations, (iii) a description of the categories of the data subjects and of the personal data concerned, (iv) the categories of recipients to whom personal data are communicated, including third countries and international organisations, (v) the intended transfer of personal data for a third country or international organisation, (vi) the retention periods and time for deletion, (v) the security measures implemented. The data controller shall make the data records available to the Commission upon request;

- **Data breach notification:** these notifications must be carried out (i) to the Commission, without undue delay and in any case within 72 hours after becoming aware of the breach; (ii) where a data breach is likely to create a risk to a person's rights and freedoms, the data controller shall communicate the occurrence to the data subject concerned, if it does not fall under of the exemptions provided by law. The data controller shall document any violation of personal data, by indicating the facts concerning the data breach, its effects and the measures taken to fix it. This documentation is required to assist the Commission in verifying compliance with the provisions of the Law.

Specifically, when a processing operation through the use of new technologies and attending to the nature, scope, context, and purposes of processing, where it is likely to result in a high risk to the rights and freedoms of individuals, the data controller shall, prior to the processing, carry out a DPIA

on the proposed processing operation. The same analysis can cover a range of operations if intended for similar processing operations and with similar risks. If a data protection officer ('DPO') has been appointed, they must be consulted in this assessment.

The DPIA is mandatory in the case of:

- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects regarding the natural personal or similarly significantly affect the natural person;
- large-scale processing of special categories of data, namely data pertaining to criminal convictions and offences;
- systematic surveillance on a large scale of an area accessible to the public.

The Commission shall publish a list of the types of processing operations for which a data protection impact assessment is required. Conversely, the Commission may publish a list of the types of processing operations for which a DPIA is not required.

The data controller shall consult the Commission prior to processing when a DPIA indicates that the processing operation would present a high risk to the rights and freedoms of the individuals, provided that the data controller did not take any measures to mitigate such risk.

Where the Commission considers that the processing operation would constitute a violation of the Law, the Commission shall, within a maximum of eight weeks, provide in writing a receipt of the request and a written opinion on the processing. This period may be extended by six weeks, depending on the complexity of the processing operation.

The Commission shall inform the data controller and, where appropriate, the data processor of the extension of the deadline and the reasons for the delay, within one month of receipt of the request for consultation. These deadlines may be suspended until the Commission has obtained the necessary information.

Where the data controller consults the Commission, it shall communicate:

- where applicable, the responsibilities of the data controller, the responsibilities of the joint data controllers and of the data processors participating in the processing operation, in particular if the processing operation is to be carried out within a business group;
- the terms and means of processing considered;

- the measures and guarantees provided for in order to protect the rights and freedoms of individuals concerned;
- where applicable, the contact details of the DPO;
- the DPIA regarding the provision of information society services to minors; and
- any other information requested by the Commission.

The Law expressly provides for limited controller rights, including, (i) the right to process personal data in the conditions provided for by law, and (ii) the right to refuse compliance with unreasonable requests and demands from data subjects; (iii) right to request additional information, when having reasonable doubts about the data subject identity; and (iv) the right to appeal to the Supreme Court on the sanctions imposed by the Commission.

7. DATA PROCESSOR RIGHTS AND RESPONSIBILITIES

Under the law, the data processor must:

- present sufficient guarantees to ensure the security and confidentiality of the personal data;
- notify the data controller of any violation of personal data as soon as possible after becoming aware of it;
- maintain a record of the processing activities carried out on behalf of the data controller and shall make the data records available to the Commission upon request; and
- cooperate with the Commission.

8. DATA CONTROLLER AND PROCESSOR AGREEMENTS

An agreement between the data controller and data processor is mandatory, must take the form of a contract and include the obligations on confidentiality and security imposed by the data controller. Specific allocation of liability between controller and processor is not expressly provided for under the Law.

9. DATA SUBJECT RIGHTS

Title III, Chapter I of the Law establishes the following data subjects' rights:

- the right to be informed regarding the terms of processing, including the identity of the data controller, the purposes of processing, the categories of personal data processed, the recipients to which the data are communicated, if providing personal data is mandatory and the consequences of not doing it, data subjects rights, retention periods and possible transfers of personal data intended for a third country;
- when using an electronic communication network, the data subject must be informed if the data controller can access data stored in its equipment and the means to oppose to it;
- the right to request and access the information pertaining to them and challenge the processing operation;
- the right to obtain a copy of the personal data;
- the right to obtain information regarding the origin of the data;
- the right to complain to the Commission;
- the right to data portability;
- the right to oppose for legitimate reasons to the processing of personal data concerning them;
- the right to oppose to the processing of personal data for prospecting purposes;
- the right to have their personal data rectified, completed, updated, locked, or deleted where it is inaccurate, incomplete, equivocal, out of date;
- the right to be informed of a data breach likely to create risks for his rights and freedoms, in the cases provided by law; and
- the right to only receive direct marketing messages if consent was given prior to the receiving.

The rights of rectification and deletion are extended after the death of the data subject. In this sense, the data subject may indicate instructions regarding the conservation, deletion and communication of his/her personal data. The data subject shall designate a digitally certified third party, who will be responsible for administering the instructions. The data subject may amend, or revoke said instructions at any time. Heirs of the data subject may also request that the processing of the personal data is updated in light of the death of the data subject.

10. DATA PROTECTION OFFICER

10.1. DPO – compulsory appointment (yes/no)

Yes, it is compulsory to appoint a DPO in specific circumstances. Please refer to section 10.2 below.

10.2. Requirements

The data controller and data processor shall designate a DPO on the following cases:

- when the processing is carried out by an authority or a public body, except for the courts acting in the exercise of their jurisdictional function;
- when their core activities of the data processor consist on processing operations which, because of their nature, scope, and/or purpose, require regular and systematic monitoring at a large scale; and
- when their core activities consist on large-scale processing of special categories of data.

The DPO:

- must be a person with the required qualifications to carry out its role, namely its moral and professional qualities, and its knowledge of law and data protection related matters;
- may be an employee of the data controller and data processor or perfume its duties under a provision of services;
- shall not be the target of any sanction or liability before his/her employer when exercising its rights and obligations as a DPO and it reports directly to the highest level of the organization management; and
- shall be subject to professional secrecy or an obligation of confidentiality with respect to the exercise of his/her missions.

Additionally, the data controller and the processor shall publish the contact details of the DPO and communicate them to the Commission.

11. DATA BREACH NOTIFICATION

11.1. General obligation (yes/no)

Yes. In the event of a data breach, the data controller must notify the Commission as soon as possible, and at the latest 72 hours after becoming aware of it. Note that this obligation does not apply if the violation is not likely to create any risk to the rights and freedoms of the individuals concerned.

If the notification to the Commission surpasses the established time limit, it must be accompanied by a justification for the delay.

11.2. Sectoral obligations

As noted regarding the Electronic Communications Framework, in the event of any attack, intrusion and other disruptions that can hinder the operation of an information system or another electronic communications network, information system or network operators (regardless of whether they are public or private), must promptly inform the ACSI.

12. SANCTIONS

Apart from the sanctions established in the Law No. 27-2020, Title IV Chapter 1 of the Law stipulates the sanctions for non-compliance.

The Commission shall assess and impose measures or sanctions following:

- a warning to the data controller; and
- a formal notice to restore compliance within a time limit defined by the Commission.

If the data controller does not comply with the formal notice, the Commission may, after hearing the controller, apply the following sanctions:

- suspend the data controller data processing activities or provisionally withdraw the authorisation granted from a period up until three months;
- definitive withdrawal of the authorisation or definitive prohibition of carrying out data processing operations;
- an injunction to stop the processing, when it falls under the notification regime or when it benefits from the exoneration of obligation of notification; or
- a pecuniary penalty between one to 100 million CFA Francs (approx. €15,200).

In case of an emergency, provided that the breach is seriously hindering the data subject fundamental rights and after hearing the data controller, the Commission may:

- suspend the data processing activities of the data controller for a period up until three months;
- block certain processing operations for a period up until three months; or
- ban any processing operations contrary to the provisions of the Law.

If the processing has been authorised by a regulatory act under the conditions set out in the Law, the Commission shall inform the Government so that it can take, where appropriate, measures to end to the violation found.

The sanctions imposed by the Commission (based on a Commission report) will be notified to the data controller, and the sanctions applied by the Commission can be made public at the expense of the persons sanctioned, the sanctions can be included in publications, newspapers and other media mediums designated by the Commission.

Violations of Law provisions are also punishable under the Criminal Code.

13. ADDITIONAL RELEVANT TOPICS

13.1. Data Transfers and Outsourcing

Cross-border transfer of data can only take place if the third country ensures an adequate level of protection of the privacy, fundamental rights, and freedoms of persons concerned.

The data controller shall inform the Commission in advance of any transfer of personal data to a third country, that shall access the level of protection based on the following criteria: the legal provisions existing in the country in question, the security measures enforced, the specific circumstances of the processing (such as the purpose and duration thereof), as well as the nature, origin and destination of the data.

The controller may transfer personal data to third countries that does not meet the adequate level of protection if (i) the transfer is not regular, (ii) massive and data if (iii) the data subject has consented expressly to its transfer; (iv) if the transfer is necessary to save that person's life, to safeguard a public interest, to ensure the right of defence in a court of law, to the performance of a contract between the data subject and the data controller.

In the absence of an adequate level of protection in the third country, the transfer of data may still be authorized if the data controller offers adequate guarantees for the protection of the privacy and the rights and freedoms of data subjects, as well as offering the possibility for them to exercise their rights.

13.2. Employment

Under the Law, there are no specific provisions regarding privacy implications on employment, except the reference to the fact that the DPO may not be the target of any sanction or liability before his/her employer when exercising their rights and obligations as a DPO.

13.3. Data Retention

Under the Law, personal data must not be kept for longer than the period necessary to achieve the purposes for which it was collected and processed. This is without prejudice to specific retention periods provided by sector-specific regulation or generally applicable judicial/administrative retention periods.

13.4. Consent

A data subject may, from the age of sixteen, consent independently to the processing of personal data in the context of the provision of information society services. If the data subject is a minor under the age of 16, the consent is only valid if is provided jointly by the parents, tutors or other legal representative.

14. OTHER SPECIFIC JURISDICTIONAL ISSUES

The Regulation N 01/03 relating to the prevention and suppression of money laundering and financing of terrorism in central Africa enacted by the Economic and Monetary Community of Central Africa ('CEMAC') ('the AML/CFT Regulation') has direct applicability in the countries belonging to CEMAC, such as Congo. It is required by the AML/CFT Regulation that the verification of identity be done through the presentation of an official identification document with a photograph, which must be copied and kept. Moreover, the address must be proven by a substantiating document.

In addition, financial institutions must keep - for at least five years - all necessary records on national or international transactions performed. The AML/CFT Regulation also provides for obligations for casinos and gambling establishments.