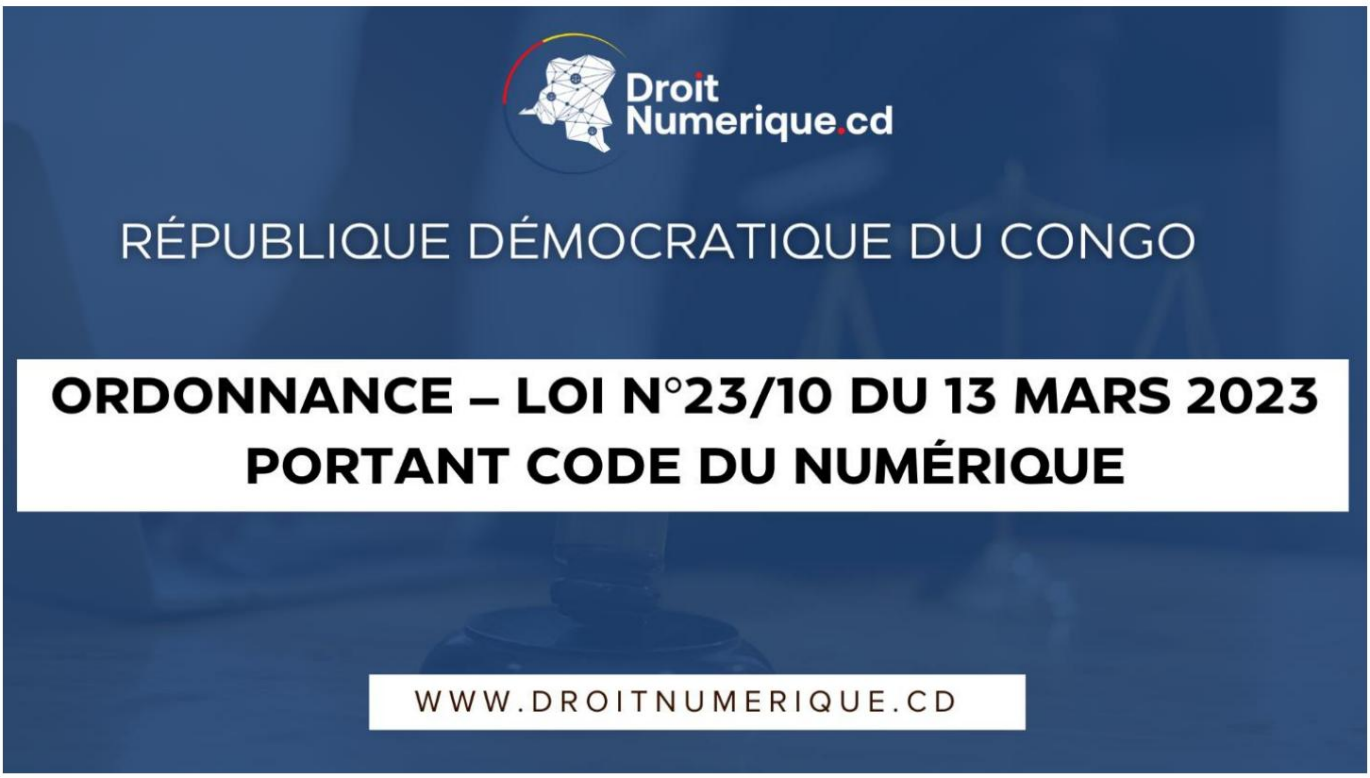

Code outline

The President of the Republic,

Having regard to the Constitution, as amended by Law No. 11/002 of 20 January 2011 relating to revision of certain articles of the Constitution of the Democratic Republic of Congo of 18 February 2006, especially in its articles 31 and 129;

Having regard to Law No. 22/060 of December 27, 2022 authorizing the Government, especially in its articles 1, 2 and 3;

In view of Ordinance No. 22/002 of January 7, 2022 relating to the organization and operation of the Government, modalities of collaboration between the President of the Republic and the Government as well as between the Members of the Government, especially in its articles 45 and 46;

Having regard to Order No. 21/006 of February 14, 2021 appointing a Prime Minister ;

Having regard to Order No. 21/012 of April 12, 2021 appointing the Deputy Prime Ministers Ministers, Ministers of State, Ministers, Ministers Delegate and Vice-Ministers;

Given the necessity and urgency

On the proposal of the Government, deliberated in the Council of Ministers;

Orders:

PRELIMINARY BOOK: ON THE OBJECT, SCOPE OF APPLICATION AND DEFINITIONS

CHAPTER I: PURPOSE AND SCOPE OF APPLICATION

Article 1.

Digital legislation is constituted by this ordinance-law and the provisions legal and regulatory provisions issued for its application.

This ordinance-law applies:

1. to digital activities and services;
2. to writings, electronic tools and trusted service providers;
3. to digital content;
4. to the security and criminal protection of computer systems.

In addition, it sets out the tax, parafiscal, customs and exchange rate regime applicable to the activities and digital services in the Democratic Republic of Congo.

CHAPTER II: DEFINITIONS

Article 2.

For the purposes of this ordinance-law, the following terms shall apply:

1. **Access :** direct or indirect connection in whole or in any part of a computer system via an electronic communications network;
2. **Address :** physical and/or electronic location element;
3. **Archiving :** operation consisting of organizing and preserving archives for the purposes of a further use, whether this conservation is administrative or historical;
4. **Electronic archiving :** archiving which consists of implementing actions, tools and methods for preserving data, documents and information for the long term and in electronic format and in a secure manner for possible later use;
5. **Archives :** documents, whatever their dates, formats and media, products or received and deliberately retained by any person, natural or legal, public or

private;

6. **Authorization :** administrative act of a Competent Authority which grants its beneficiary a set of specific rights and obligations concerning the exercise of an activity determined in accordance with this Ordinance-Law;

7. **Competent authority :** authority designated by legal or regulatory means exercising a valuable mission within its competences under this ordinance-law or any other law;

8. **Electronic seal :** electronic data, attached or logically associated with other electronic data in order to guarantee their originality and integrity;

9. **Specifications :** document integrating the organizational, technical, operational and operating conditions imposed on any operator and/or supplier of digital services;

10. **Special categories of data :** data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership union, as well as genetic data, biometric data for the purpose of identifying a natural person in a unique manner, including data concerning health and data concerning sexual life, minors and judicial convictions;

11. **Website Authentication Certificate :** certificate enabling the authentication of a website and associating it with the natural or legal person to whom the certificate is issued;

12. **Electronic signature certificate :** electronic attestation which associates the data of validation of an electronic signature to a natural person and confirms at least the name or the pseudonym of that person;

13. **Qualified electronic seal certificate :** document issued by a service provider qualified trust that meets legal requirements;

14. **Qualified electronic signature certificate :** act issued by a service provider qualified trustee who meets legal requirements;

15. **Electronic commerce :** commercial activity by which a person offers or provides electronically or via a computer system, for payment of a fee, the supply of goods or services;

16. **Electronic communication :** emission, transmission and reception of signs, signals, of writings, images, sounds or information of any nature by wire, optical fiber, radioelectricity or other electromagnetic systems;

17. **Confidentiality :** security status that guarantees the secrecy of information, data and stored resources from unauthorized third parties;
18. **Consent :** an express and unequivocal manifestation of will by which the data subject agrees that his/her personal data may be subject to a treatment ;
19. **Data Retention :** Saving data in the state in which it is found. find ;
20. **Consumer or user :** user of digital activities and/or services;
21. **Digital content :** set of data, computer programs, mobile or web applications as well as audio, video, text files, in digital form;
22. **Cryptology :** set of practices aimed at data protection and security digital including confidentiality, authentication, integrity and non-repudiation;
23. **Cryptography :** set of principles, means and methods of transforming data, in order to hide their content, to prevent their modification from happening unnoticed and/or to prevent their unauthorized use;
24. **Cybercrime :** all specific criminal offences linked to cybersecurity technologies information and communication as defined by this ordinance-law, as well as than those provided for in other specific laws, the commission of which is facilitated or linked to the use of technologies;
25. **Cybersecurity :** set of prevention, protection and deterrence measures technical, organizational, legal, financial, human and procedural or other enabling the achievement of security objectives for computer systems and networks electronic communication and to ensure the availability, integrity, confidentiality, the authenticity or traceability of stored, processed or transmitted data and services related;
26. **Declaration :** act prior to any activity emanating from an operator or a supplier of digital services in accordance with the provisions of this ordinance-law;
27. **Recipient :** person authorized to receive communication of the data other than the data subject, the controller, the processor and the persons who, in due to their functions, are responsible for processing the data;
28. **Data :** information or set of information capable of being stored, processed or

analyzed within a computer system or electronic communications network;

29. **Biometric data :** data relating to physical, biological characteristics or behavioral data that can identify a natural person, such as fingerprints digital, facial images, voice, iris or gait;

30. **Personal data or personal data :** any information relating to a natural person identified or identifiable directly or indirectly;

31. **Public data :** data produced, managed and stored in public registers of data on the territory of the Democratic Republic of Congo as part of a public service mission by the State, provinces, territorial entities, services, establishments and public bodies as well as legal entities under private law responsible for a mission public service;

32. **Sensitive data :** biometric data, personal data relating in particular racial or ethnic origins, political opinions or activities, beliefs religious or philosophical, union membership, sexual life, health, genetics;

33. **Strategic data :** data of public or private legal entities, institutional or professional, relating to State security, with economic or security value, the leakage, alteration, deletion and/or fraudulent use would be detrimental to the institutions, organizations or professions concerned;

34. **File :** structured directory of digital data, centralized, decentralized or distributed functionally or geographically;

35. **Online service provider :** natural or legal person offering services via Internet in accordance with this Ordinance-Law;

36. **Digital service provider :** natural or legal person operating in the digital activities and services sector in accordance with this ordinance-law;

37. **Phishing :** manipulation technique by deception used by hackers aiming to recover from a user or computer system or an electronic communications network, information or data of a personal nature personnel ;

38. **Host :** natural or legal person who provides a transmission service electronic information by storing data provided by the user of the service;

39. **Electronic timestamping :** operation aimed at associating a file with its date and time of creation.

creation or reception in accordance with the provisions of this ordinance-law;

40. **Certified electronic time stamp :** electronic time stamp that meets the requirements set by this ordinance-law and generated by a trusted service provider quality ;

41. **INACO :** National Institute of Archives of Congo;

42. **Electronic identification :** process which consists of the use of data and elements constituting the identity of a natural or legal person by processes electronic which uniquely represent the natural or legal person concerned;

43. **Critical or essential infrastructure :** set of installations, resources, of non-interchangeable equipment and/or services with particular characteristics which, because of the prohibitive cost of their reproduction, it would be impossible for competitors potential, to reproduce them by reasonable means;

44. **Integrity :** security state ensuring that an electronic communications network, computer system or terminal equipment that has remained intact and that the resources and information stored therein has not been altered, modified or destroyed in any way intentional or accidental, so as to ensure their accuracy, reliability and sustainability;

45. **Interception :** acquisition, knowledge, seizure or copying of the content or of a part of the content of any communication, including data relating to the content, the computer data, traffic data, during non-public transmissions by through technical means. Interception includes, but is not limited to, listening to, monitoring or surveillance of the content of communications and obtaining the content of the data, either directly, by means of access to computer systems and their use, either indirectly, through the use of listening devices electronic or listening devices by technical means;

46. **Interoperability :** capacity for collaboration and communication between two or more computer systems, services or digital content;

47. **Hyperlink :** characteristic or property of an element such as a symbol, a word, a sentence or image that contains information about another source and links to it displays other content or information when executed;

48. **Limitation of processing :** mechanism consisting of only processing data which are

useful for a specific purpose;

49. **Software :** set of programs or procedures necessary for the operation of a computer system or electronic communications network;

50. **Market place :** platform that connects buyers and sellers in a computer system or electronic communications network;

51. **Electronic message :** information sent or transmitted through a system computer or electronic communications network;

52. **Electronic identification means :** material and/or immaterial element containing identification data of natural or legal persons;

53. **Technological neutrality :** obligation for digital legislation to be non-discriminatory between operators in the sector;

54. **Digital Norms and Standards applicable to the public sector :** set of good government practices, technical references and guidelines, specifying in particular the architecture of data management systems of the State, territorial entities and other public persons, the level of security and the interoperability standards of public sector IT systems of the Democratic Republic of Congo;

55. **Digital :** set of processes and means using tools and services which allow data to be created, processed, stored and distributed;

56. **Operators of vital importance (OIV) :** public or private operators operating establishments or using facilities and works, the unavailability of which could risk significantly diminish the war or economic potential, security or national survivability;

57. **Data subject :** natural person who is the subject of data processing and which is identified or identifiable;

58. **Complaint :** request addressed to the competent Authority to claim and have a right that the author considers he possesses or to express dissatisfaction with an operator;

59. **Spam :** unwanted electronic mail, unsolicited by the recipient;

60. **Trusted service provider :** natural or legal person who provides one or several trust services in accordance with this ordinance-law;

61. **Qualified trust service provider :** service provider responsible for verifying identity of a natural or legal person in order to be able to issue an electronic certificate in its favor in accordance with this ordinance-law;

62. **Profiling :** personal data analysis technique that allows profiles to be created and/or models to identify characteristics or behaviors of a group or of an individual;

63. **Direct prospecting :** sending messages intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services;

64. **National Population Register :** general population file;

65. **Public data register :** database containing various information collected by sectoral systems that participate in digital governance;

66. **Representative of the data controller :** natural or legal person established in stable manner on the territory of the country, which replaces the data controller in the fulfillment of the obligations provided for by this ordinance-law;

67. **Electronic communications network :** installation or set of installations of transport or distribution as well as, where applicable, other means ensuring delivery electronic communications and networks providing or used for the dissemination distribution of communication services;

68. **Data controller :** natural or legal person, public authority, service or any other body which, alone or jointly with others, determines the purposes and means of processing personal data;

69. **Electronic identification scheme :** system or process for identification electronic under which electronic identification means are issued to natural or legal persons, or to natural persons representing persons morales ;

70. **Digital data security :** confidentiality, integrity and availability of data computers;

71. **Trust service :** electronic service normally provided for remuneration and which consists of:

a. in the creation, verification and validation of electronic signatures, seals electronic or electronic time stamps, registered mail services electronic and certificates relating to these services;

b. in the creation, verification and validation of certificates for authentication of site Internet ;

c. in the conservation of electronic signatures, electronic seals or certificates relating to these services;

72. **Digital service or activity :** service offered and/or provided by means of a computer system or an electronic communications network, in particular for the purpose of create, process, store or distribute data;

73. **Electronic communications services :** services including the transmission, transmission or reception of signs, signals, writings, images, sounds or information of any kind or a combination of these functions;

74. **Electronic signature :** mechanism for guaranteeing the integrity and non-repudiation of a document, and to authenticate with certainty the author and to provide the proof of his consent, in accordance with the provisions of this ordinance-law;

75. **Subcontractor or subcontracting company :** natural or legal person whose activity, on a regular, temporary or occasional basis, is linked, by a contract or an agreement, to the carrying out the main activity or the execution of a contract of a main business;

76. **Subcontracting :** activity or operation carried out by a company known as a subcontractor, for the account of a company called the main company and which contributes to the achievement of the main activity of this company, or to the performance of one or more services of a main contractor contract;

77. **Digital sovereignty :** the right of self-determination that a country has to decide on its own digital policy, particularly on its infrastructure and its data and their treatments;

78. **Computer system :** device composed of procedures, hardware and software enabling the exchange, storage or automated processing of data;

79. **Correspondence table :** list of associations of computer or electronic values;

80. **Third party :** natural or legal person, public authority, service or any other body other than the data subject, the controller, the processor and the persons who, placed under the direct authority of the data controller or the processor, are authorized to process the data;

81. **Treatment :** operation or set of operations carried out or not using processes fully or partially automated and applied to personal data, such as collection, recording, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other

form of provision, rapprochement or interconnection, as well as locking, erasure or destruction;

82. **Electronic transactions :** secure exchanges made during a purchase or a online payment;

83. **User or user :** consumer of digital services;

BOOK ONE: DIGITAL ACTIVITIES AND SERVICES

TITLE I: PURPOSE AND SCOPE OF APPLICATION

Article 3.

Without prejudice to specific provisions, this book governs the activities and services digital services carried out from or to the Territory of the Democratic Republic of Congo, by any natural or legal person, whatever their legal status, their nationality or that of the holders of its share capital or its directors, of the place of its head office or its principal establishment.

Article 4.

The following are excluded from the scope of this book:

1. digital activities and services carried out for the needs of public security and of national defense;
2. regulation and regulation of telecommunications;
3. regulation and regulation of the audiovisual sector.

TITLE II: INSTITUTIONAL FRAMEWORK

Article 5.

The institutional framework of the digital activities and services sector includes:

1. the Minister responsible for digital technology;
2. the Digital Regulatory Authority;
3. the National Electronic Certification Authority;

4. the National Cybersecurity Agency;
5. the National Digital Council.

The organization, operation and skills of the National Cybersecurity Agency are mentioned in the provisions of Book IV of this ordinance-law.

CHAPTER I: OF THE MINISTRY

Article 6.

Without prejudice to the missions provided for in other legislative and regulatory texts in force, the Minister responsible for digital technology has the following missions:

1. design, propose and implement government policy in the sector digital;
2. ensure, within the limits of its powers, the regulation, promotion and monitoring digital sector activities and services.

CHAPTER II: DIGITAL REGULATORY AUTHORITY

Article 7.

The Digital Regulatory Authority is a public establishment created by decree of Prime Minister, deliberated in Council of Ministers and placed under the supervision of the Minister having digital in its attributions.

The regulatory missions for digital activities and services are carried out by the Authority Digital Regulation, designated by the acronym ARN.

The Digital Regulatory Authority's missions include:

1. regulate digital activities and services;
2. ensure fair prices and the quality of services provided to users;
3. define the principles of interoperability of digital services;
4. protect the interests of users and providers in the digital market digital services, ensuring the existence and promotion of competition effective and loyal, fairness and transparency by ensuring the balance of the market digital sector and to take all necessary measures to restore competition for the benefit of users, and resolving disputes;

5. ensure the policing of activities and services in the digital sector;
6. promote and develop activities in the digital sector;
7. ensure compliance with the specific obligations imposed on platforms and suppliers in a dominant position;
8. ensure participation in research, training and study activities relating to to electronic trade and commerce;
9. contribute to the research, mobilization and channeling of funding necessary for the development of the sector and the reduction of the divide digital ;
10. ensure the mission of prevention and repression against platforms and suppliers in a dominant position after analysis of the state and foreseeable developments aspects of market competition.

Article 8.

A portion of the universal service fund provided for by law no. 20/017 of November 25, 2020 relating to telecommunications and information and communication technologies will be allocated in particular to the promotion and development of activities and services digital.

CHAPTER III: OF THE NATIONAL AUTHORITY OF ELECTRONIC CERTIFICATION

Article 9.

An Authority is hereby created by decree of the Prime Minister deliberated in Council of Ministers: Electronic Certification called National Electronic Certification Authority, “ ANCE » in simple.

The National Electronic Certification Authority is a public institution of a technical, placed under the supervision of the Minister responsible for digital technology.

It has legal personality, enjoys management autonomy and has a own heritage.

Article 10.

The National Electronic Certification Authority's mission is to ensure the role of the Electronic Certification Authority for digital activities and services.

Without prejudice to the specific skills assigned to certain particular public services, the National Electronic Certification Authority is responsible for:

1. provide advice on requests for the exercise of activities by service providers confidence throughout the national territory;
2. ensure monitoring of compliance by certification service providers electronic of the provisions of this ordinance-law and its measures d'applications ;
3. establish the characteristics of the signature creation and verification device electronic, electronic seal, electronic archiving, time stamping electronic and website authentication;
4. manage the national public key infrastructure;
5. issue, deliver and store electronic certificates of authorized public officials to carry out electronic exchanges.

CHAPTER IV: THE NATIONAL DIGITAL COUNCIL

Article 11.

A consultative body called the National Digital Council (CNN) is created whose organization and operation are determined by Order of the President of the Republic.

The CNN is placed under the authority of the President of the Republic.

It includes a representation of all the players in the digital sector, namely the Presidency of the Republic, the Government and its services, the private sector, Parliament, the scientific world, the Courts, tribunals and public prosecutors, civil society and others stakeholders.

Article 12.

Without prejudice to the powers assigned to other bodies, the National Digital Council has the following missions in particular:

1. serve as a framework for consultation and evaluation of Government projects in the digital sector;
2. provide advice to the Government and conduct studies on related issues with digital;
3. evaluate sectoral policies and digital investment initiatives;
4. ensure the ethics of digital technology and especially advanced digital technology, Artificial Intelligence, Big Data, Collaborative Robotics and Blockchain
5. propose and present to the Government sectoral initiatives as well as obstacles to the execution of digital projects.

TITLE III: LEGAL REGIME APPLICABLE TO ACTIVITIES AND DIGITAL SERVICES

CHAPTER I: GENERAL PROVISIONS

Article 13.

The exercise of digital activities and services is subject to the authorization regime, declaration or approval, as the case may be, in accordance with the terms and conditions granting fixed in this ordinance-law and by order of the Minister responsible for digital in its attributions.

Without prejudice to the provisions applicable to commercial companies, no one may exercise an activity in the digital sector in the Democratic Republic of Congo, without submit to one of the legal regimes provided for by this ordinance-law.

Article 14.

The instruction of requests for authorization or declaration as well as the preparation of the notebook charges are the responsibility of the Digital Regulatory Authority.

The instruction of requests for authorization or declaration as well as the preparation of the notebook charges for trust service providers are the responsibility of the National Electronic Certification Authority.

The processing of safety approval applications is the responsibility of the National Agency for Cybersecurity as provided for in Article 278, Book IV of this Ordinance-Law.

CHAPTER II: AUTHORIZATION

Article 15.

The following are subject to the authorization regime:

1. operators and/or digital service providers building data centres data ;
2. providers of qualified trusted digital services;
3. providers of essential digital services;
4. providers of application hosting services, including those financial;
5. digital platforms and suppliers in a dominant position operating in Democratic Republic of Congo.

A Decree of the Prime Minister deliberated in the Council of Ministers completes, on the proposal of the Minister responsible for digital technology, list of digital activities and services subject to the authorization regime, the Digital Regulatory Authority and the National Electronic Certification Authority heard by written notice.

Article 16.

The authorization is issued by the Minister responsible for digital technology after consultation written from the Digital Regulatory Authority, the National Electronic Certification Authority or the National Cybersecurity Agency, as the case may be

CHAPTER III: OF THE DECLARATION

Article 17.

The following are subject to the declaration regime:

1. digital service providers of buffer copies or cache servers data or media content from other providers;
2. Internet exchange point operators;
3. developers of applications from Congolese startups.

An order from the Minister responsible for digital technology completes the list of activities and digital services subject to this reporting regime, the Regulatory Authority of Digital heard by written notice.

Article 18.

The declaration is made to the Digital Regulatory Authority which keeps a register public.

The Digital Regulatory Authority acknowledges any declaration by issuing a certificate of approval and informs the Minister responsible for digital technology.

CHAPTER IV: APPROVAL

Article 19.

The approval system certifies that the digital infrastructures and services provided to the State comply with the Digital Norms and Standards applicable to the public sector in the Democratic Republic of Congo as well as good practices in this area.

The following are subject to approval:

1. providers of digital services to the State or any other public entity;
2. providers of digital services to a public service or a company state portfolio.

A Decree of the Prime Minister deliberated in the Council of Ministers completes, on the proposal of the Minister responsible for digital technology, list of digital activities and services subject to the approval regime, the National Cybersecurity Agency heard by opinion writing.

An order from the Minister responsible for digital technology sets out the conditions and procedures of granting approval.

Article 20.

The approval certificate is issued by the Minister responsible for digital technology attributions after advice from the National Cybersecurity Agency.

TITLE IV: RIGHTS, GENERAL PRINCIPLES AND OBLIGATIONS APPLICABLE TO SUPPLIERS OF ACTIVITIES AND SERVICES DIGITAL

CHAPTER I: GENERAL RIGHTS AND PRINCIPLES APPLICABLE TO PROVIDERS OF DIGITAL ACTIVITIES AND SERVICES

Article 21.

Without prejudice to the specific provisions, digital activities and services are carried out freely, in compliance with the legal and regulatory provisions applicable in the Republic Democratic Republic of Congo. They are subject to the following principles:

1. Equal treatment;
2. Transparency;
3. Non-discrimination ;
4. Free competition;
5. Technological neutrality.

Article 22.

Digital service providers enjoy the same rights and are subject to the same obligations in accordance with the provisions of this ordinance-law.

With the exception of free competition and technological neutrality, the principles referred to in Article 21 above also applies to any administrative authority, in particular the Digital Regulatory Authority, the Electronic Certification Authority and the National Cyber Security Agency.

Article 23.

Digital service providers operating under the same legal regime enjoy, under the same conditions, the same rights and are subject to the same obligations provided for in this regime.

Without prejudice to the provisions of the preceding paragraph, the conditions of exercise depend on the compliance with the material or technical conditions previously set by the Authority Digital Regulation.

These conditions must be compatible with national competition rules.

Article 24.

The Digital Regulatory Authority and the National Electronic Certification Authority, depending on the case, ensure the application of the principle of technological neutrality.

Article 25.

Digital activities and services carried out on the national territory by the representations diplomatic missions, foreign institutions and bodies with special status legal in international law, are exercised in accordance with treaties and agreements international agreements ratified by the Democratic Republic of Congo.

Subject to international treaties and agreements ratified by the Democratic Republic of Congo, digital activities and services of diplomatic representations, institutions foreign entities and organizations enjoying legal personality under international law are subject to the provisions of this ordinance-law.

Article 26.

With a view to carrying out the work necessary for the operation and extension of their activities, digital service providers are required to comply with all the legislative and regulatory provisions in force, in particular the requirements relating to land use planning and environmental protection.

Article 27.

Agreements between digital service providers and users on the conditions commercial and technical, such as prices, data volumes or throughput and any business practices implemented by digital service providers, may limit users' acquired rights in the provision of services.

Article 28.

The Digital Regulatory Authority and the National Electronic Certification Authority, depending on the case, ensure the quality and permanent availability of digital services provided.

They impose requirements regarding technical characteristics, requirements minimum quality of service and other measures appropriate and necessary for one or more digital service providers.

At the request of the Digital Regulatory Authority or the National Authority of Electronic Certification, digital service providers make available to them any information relating to their obligations and communicate this information in the deadlines and according to the degree of precision required by them.

CHAPTER II: OBLIGATIONS OF SUPPLIERS OF ACTIVITIES AND DIGITAL SERVICES

Article 29.

The digital service provider has the obligation to:

1. Make open digital infrastructures and services available to all users to the public it provides;
2. Ensure that fees, rates, practices and classifications are fair, reasonable and transparently available;
3. Provide efficient, reliable services that comply with recognized standards at the national level national, international set by the Digital Regulatory Authority;
4. Publish by any means of mass information and without delay, the forecasts interruption of services, in particular for reasons of installation, repair or of equipment change;
5. Establish an effective complaints handling and resolution mechanism expeditious incidents;

6. Ensure compliance with the rules relating to the protection of personal data
personnel.

Article 30.

Subject to the provisions in this area, any natural or legal person who meets the contractual and financial conditions offered by a digital service provider cannot be refused the provision of these services, if he has requested them.

The digital service provider requires the user requesting said services to provide: security deposit, the amount of which is fixed in advance and published in a transparent manner and non-discriminatory.

Any user of a digital service who complies with the contractual conditions and financial services subscribed to does not suffer any interruption in the provision of services, unless it is make the express request, except in cases of force majeure or for security reasons public.

Article 31.

Transparent and up-to-date information relating to all services offered, rates charged as well as the general conditions of sale and/or services, are regularly published and made available to users by providers of digital services at their points of sale and by any other means of advertising.

The Digital Regulatory Authority specifies, by decision, the publication deadlines, the form and content of the information and documents to be published.

Article 32.

The digital service provider draws up standard contracts for the provision of user services.

The Digital Regulatory Authority specifies the provisions that must be contained in the contracts to be concluded with users.

Article 33.

The digital service provider may not limit the user's right to enjoy fully of the services to which he has subscribed.

Article 34.

The digital service provider cannot unilaterally modify the terms of a current contract that binds them to users that:

1. For reasons stated in the terms of the contract and in accordance with the contract;
2. On the basis of a change in legislation or a decision of the Authority Digital Regulation in application of a legal or regulatory provision.

The draft amendment to the contractual conditions for the provision of a digital service is communicated by the provider of said service to users in writing or otherwise durable medium made available to them at least thirty (30) working days before its entry into force, accompanied by the information that users may, both that they have not expressly accepted the new conditions, terminate the contract without penalty termination and without the right to compensation, up to a period of sixty (60) days working days after the amendment comes into force.

The modification only takes effect after this period of sixty (60) working days.

Article 35.

The digital service provider has an obligation to guarantee access to the services emergency in accordance with the applicable rules and under the conditions specified by the Authority of Digital Regulation.

Access to these services in the areas covered by the supplier's activities cannot be affected of no limitation.

Article 36.

The digital service provider may not use their infrastructure or knowingly allow use for purposes contrary to legal and regulatory provisions in force.

It is required to take all appropriate measures to ensure that its infrastructure does not are not used for illegal or fraudulent purposes.

Article 37.

Except in the event of legal requisitions, the digital service provider is required to:
confidentiality requirements of the data it processes in accordance with the provisions of the Book III of this ordinance-law.

TITLE V: DEMATERIALIZED ADMINISTRATION

CHAPTER I: EXCHANGES OF INFORMATION WITHIN PUBLIC ADMINISTRATION

Article 38.

The public administration responds electronically to any request for information sent to it is addressed either by a person or by another administration.

The exchange of information, documents and/or administrative acts may be subject to a electronic transmission.

Where a special formal requirement is provided for in a special procedure,
This requirement can be met electronically.

In this respect, each administration communicates the electronic coordinates allowing to get in touch with her.

Any natural or legal person who wishes to be contacted by email by
The administration provides him with the necessary contact details. He regularly consults his email and notifies the administration of any change of contact details.

Article 39.

Administrations exchange electronically between themselves all information or data strictly necessary to process a request.

The government is setting up a secure IT infrastructure for transmission of information between the different public administrations at the central and provincial level in the form of a government or provincial intranet.

Article 40.

Any communication made electronically as part of a procedure
administrative is deemed to have been received at the time when its recipient has the possibility of
to take note.

A Decree of the Prime Minister deliberated in the Council of Ministers on the proposal of the Minister
having digital in its attributions sets the methods of implementation.

CHAPTER II: DIGITAL COUNTER

Article 41.

The Government is establishing an integrated system of electronic exchanges and activities, provision
of services, state benefits and other state interventions in the
local and remote networks, called “Digital Counter of the Democratic Republic of
Congo”, abbreviated GN-RDC.

The GN-RDC is placed under the authority and control of the Minister responsible for digital technology.
attributions.

A Decree of the Prime Minister establishes the organization of the GN-RDC on the proposal of the Minister
having Digital in its attributions.

TITLE VI: ELECTRONIC ARCHIVING

CHAPTER I: GENERAL PROVISIONS

Article 42.

Subject to specific legal provisions, the retention of documents
archived electronic records meet the following requirements:

1. The information contained in the document is accessible and consultable;
2. The document is retained in the form in which it was created, sent or received, or
   in a form which can be demonstrated to be incapable of modification or

alteration of its content, and that the document transmitted and the one kept are strictly identical;

3. The information makes it possible to determine the origin and destination of the document, as well as the date and time of sending or receipt are preserved.

Electronic archiving guarantees the authenticity and integrity of documents, data and information stored by this means.

Article 43.

The data concerned by electronic archiving must be structured, indexed and preserved in formats suitable for conservation and migration.

Electronic archiving guarantees the integrity of stored or retrieved data. their accessibility in a changing technological context.

The rules of electronic archiving apply equally to digitized documents. and to documents initially designed on electronic media.

Article 44.

A Decree of the Prime Minister, on the proposal of the Ministers having respectively the digital and culture in their attributions, sets the conditions and the methods of electronic archiving.

CHAPTER II: PUBLIC DIGITAL ARCHIVES

Article 45.

The National Archives Institute of Congo, known by the acronym "INACO", ensures the supervision and regulation of the general conditions for the management of electronic archives as well as assistance and advice to public services in the management and conservation of electronic archives.

Article 46.

For the purpose of financing the archiving of public digital archives by the Institute National Archives of Congo, a fee is imposed on all acts and documents issued by public services and establishments and intended to be saved or archived. The archiving fee is a portion applied to the price of obtaining said documents or documents.

An interministerial decree of the Ministers responsible for Finance, Digital Affairs and culture and heritage, in their attributions fixes the rate, the list of acts and documents, as well that the mechanisms for perception, recovery and retrocession to the National Institute of Archives of the Congo of the royalty mentioned in the preceding paragraph.

TITLE VII: INTELLECTUAL PROPERTY RIGHTS AND INDUSTRIAL

CHAPTER I: GENERAL PROVISIONS

Article 47.

Also constitute intellectual works protected respectively by law n° 82-001 of 7 January 1982 on industrial property and Ordinance-Law No. 86-033 of April 5, 1986 relating protection of copyright and related rights in the Democratic Republic of Congo, including: software, applications, digital platforms, including hardware of preparatory design.

A Decree of the Prime Minister deliberated in the Council of Ministers, on the proposal of Ministers responsible for digital technology and industry, specify the rights and determines the criteria, conditions and methods for granting, where applicable, withdrawing securities which enshrine the rights referred to in the preceding paragraph.

TITLE VIII: ELECTRONIC COMMERCE

CHAPTER I: GENERAL PROVISIONS

Section 1: Purpose and scope of application

Article 48.

This title sets out the general rules governing exchanges and transactions electronics.

It also applies to the provision of insurance activities and services, to service providers offering mobile and electronic payment services to commercial intermediaries and to digital marketplaces.

Without prejudice to the provisions of Law No. 01-10-19 of July 9, 2018 relating to systems payment and securities settlement, it also applies to credit institutions, microfinance institutions as well as financial services provided electronically.

Section 2: Principles governing electronic commerce

Article 49.

Electronic commerce is subject to the following principles:

1. freedom to exercise electronic commerce;
2. responsibility;
3. the obligation of information and transparency.

Article 50.

Electronic commerce is practiced freely throughout the territory of the Republic Democratic Republic of the Congo, subject to the laws and regulations in force.

Attacks, in particular on public order and security, the protection of minors, protection of public health, morality, national defense, protection of persons or the environment, observed in the exercise or on the occasion of the exercise of the electronic commerce, give rise to restrictive measures and are sanctioned in accordance with this ordinance-law or with the legal and regulatory provisions in force.

An interministerial decree of the Ministers responsible for trade and digital technology determines the terms of application of the restrictions mentioned in the previous line.

Article 51.

The natural or legal person carrying out electronic exchanges and transactions electronics is fully liable to its co-contractor for the proper performance of obligations resulting from the contract concluded at a distance, whether these obligations are

executable by itself or by other service providers, without prejudice to its right of recourse against these.

However, the person is exempted from this liability by providing proof that the non-performance, late performance or poor performance of the contract is attributable either to the buyer, either to a case of force majeure or to a third party to the provision of the planned services to the contract.

Article 52.

Without prejudice to other obligations provided for by legislative and regulatory texts in force, any person who carries out an online commercial activity or an exchange electronics is required to ensure that the customers for whom the supply of goods is intended and the providing services with easy, direct, permanent access, while using an open standard for the following information:

1. First name, last name and post-name, if a natural person;
2. Company name, if it is a legal entity;
3. Full address of residence or head office, mailing address electronic and telephone number;
4. If it is subject to the formalities of registration in the commercial register, the number of its registration in the Trade and Personal Property Credit Register, its legal form, his national identification number, tax identification number, share capital and the address of its head office;
5. If its activity is subject to any prior authorization regime, the address and the function of the authority having issued it;
6. If she is a member of a regulated profession, the reference to the rules applicable professional qualifications, the professional title, the State in which this title was granted as well as the name of the order or professional body with from which it is registered;
7. The code of conduct to which it may be subject as well as the information relating to how these codes and information can be accessed by electronic.

Anyone involved in e-commerce mentions the prices of their offer
clearly and indicates whether taxes and delivery charges, in particular, are included.

The obligation defined in the preceding paragraph applies without prejudice to other obligations.
of pricing information. It does not preclude the pricing conditions and
taxation provided for by the legal and regulatory provisions in force.

CHAPTER II: CONCLUSION OF THE CONTRACT IN THE FORM
ELECTRONIC

Section 1: Principle and content of the offer

Article 53.

Any person who offers, professionally, by electronic means, the supply of goods
or the provision of services, makes the contractual conditions available to customers
applicable in such a way as to allow their analysis, conservation and reproduction.

Without prejudice to the conditions of validity mentioned in the offer, its author remains committed
by it as long as it is accessible electronically by its own doing.

The offer further states, in particular:

1. the essential characteristics of the good or service;
2. the different steps to follow to conclude the contract electronically;
3. the technical means enabling the user, before the conclusion of the contract,
   to identify errors and correct them;
4. the duration of the offer of the product or service;
5. the price of the good or service offered;
6. the terms and deadlines for payment;
7. the terms and deadlines for delivery of the goods or the provision of services;
8. the language(s) proposed for the conclusion of the contract;
9. in the event of archiving of the contract, the terms of this archiving by the author of the offer and
   the conditions of access to the archived contract;
10. provisions relating to the protection of personal data;
11. the consequences of the absence of confirmation of the information communicated by the
    client ;

12. the consequences of non-performance or poor performance of the obligations of the supplier ;
13. the telephone number and e-mail address of the supplier for the purpose possible claims;
14. the procedures provided by the supplier for handling complaints;
15. where applicable, information relating to out-of-court procedures claims and remedies to which the supplier is subject, and the conditions access to these;
16. the existence or absence of a right of withdrawal and the conditions for exercising it;
17. where applicable, the terms of return, exchange and reimbursement of goods;
18. where applicable, information relating to after-sales assistance, after-sales service sale and the conditions relating thereto;
19. where applicable, information relating to the nature and extent of the guarantees commercial;
20. information relating to legal guarantees of conformity, legal guarantees of hidden defects and legal eviction guarantees.

Article 54.

Where it is able to do so, the online supplier of goods or services shall implement:

1. a service allowing customers to communicate directly with him;
2. the means of electronically consulting professional rules and commercial conditions to which the offeror is subject.

The information contained in the offer is provided before the customer of the service or good places an order. The electronic order is made in a clear manner, understandable and unambiguous.

Section 2: Conditions of validity of a contract concluded electronically

Article 55.

The electronic contract is validly concluded if the customer accepts the offer, after having had the opportunity to check and respond to the details of his order in advance.

The author of the offer acknowledges receipt by electronic means of the order sent to him in accordance with the terms of the offer.

In the case of a contract concluded between a professional and a non-professional, the provisions provided for in Article 55 apply. The order, confirmation of acceptance of the offer and acknowledgement of receipt are considered received when the parties have access to it electronically.

Section 3: Contractual liability of the parties

Article 56.

Upon conclusion of the electronic contract, the supplier is required to send the customer a electronic copy of said contract.
Any sale of a product or provision of a service by electronic means gives rise to the establishment, by the supplier, of an invoice sent to the customer.

The invoice must be drawn up in accordance with current legislation and regulations.

CHAPTER III: EXECUTION OF THE ELECTRONIC CONTRACT

Section 1: Payment of the price, delivery of the product and provision of services services

Article 57.

Unless otherwise provided in the electronic contract, the customer is required to pay the price agreed upon upon conclusion.

Article 58.

Upon actual delivery of the product or provision of the service which is the subject of the electronic contract, the supplier requires the customer to acknowledge receipt and the customer is required to comply.

A copy of the acknowledgement of receipt must be given to the customer. Subject to the provisions of the preceding paragraph, when the supplier delivers a product and/or a service ordered by the customer, it requires payment of its price and delivery costs.

In the event of non-compliance by the supplier with delivery times, or when the conditions of the offer are not fulfilled, the customer may reship the product within a period not exceeding four (04) working days from the date of delivery of the product, without

prejudice to his right to claim compensation for the damage caused. In this case, the
The supplier must refund to the customer the amount paid and the expenses relating to the return of the product within fifteen (15) days from the date of receipt of the product.

Article 59.

In the event of delivery of an item not conforming to the order or in the case of a product defective, the supplier takes back his goods.

Where the defective product poses a threat to public health, safety or the environment, this is noted and destroyed by the competent services in accordance with the legislation in force.

The customer returns the goods in their original packaging within a maximum period of seven (07) days plus the distance period in accordance with the legislation in force, from the date of actual delivery, indicating the reason for refusal, the costs being at the supplier's responsibility.

If the customer fails to return the goods within the period provided for in the preceding paragraph, the goods are deemed to be accepted.

The supplier is required to do either:

1. a new delivery in accordance with the order;
2. repair of the defective product;
3. an exchange of a product for an identical one;
4. cancellation of the order and a refund of the sums paid, without prejudice to the possibility of a request for compensation by the customer, in the event of damage suffered.

Reimbursement must take place within fifteen (15) days from the date of receipt of the product.

Section 2: Obligation to keep records of transactions

Article 60.

The supplier operating on the national territory is required to keep records of commercial transactions carried out and their dates, and to transmit them by

electronic on the platforms of the National Institute of Statistics, the Authority of Regulation, as well as the single window for foreign trade in the event that the transaction operates with a client located outside the territory of the Democratic Republic of Congo, or when the service or good which is the subject of the transaction comes from abroad.

CHAPTER IV: RIGHT OF WITHDRAWAL

Article 61.

The provisions of this chapter relating to the right of withdrawal only apply to contracts concluded between professionals and non-professionals.

These provisions apply without prejudice to any possible more conventional provisions favorable for the non-professional.

Section 1: Withdrawal period

Article 62.

Notwithstanding the agreement between the parties, before the day of shipment provided for in the contract, the The customer has a period of seventy-two (72) hours to exercise his right of withdrawal.

This right is exercised by the customer, without justification and without costs other than any possible costs. direct return of the goods to the professional, if applicable.

In the event that the information provided for in Articles 49 and 52 of this Book is communicated to the non-professional before the conclusion of the contract, the period for exercising the right of withdrawal begins to run:

1. From the period indicated in the preceding paragraph, with regard to contracts relating to the supply of goods;
2. Forty-eight (48) hours at the most from the placing of the order, with regard to contracts for the provision of services.

In the event that the professional fails to comply with his obligation to provide prior information provided for in Article 49 of this Book, the withdrawal period is extended to fifteen (15) days.

The customer notifies the professional of his decision to exercise his right of withdrawal by mail electronically within the seventy-two (72) hour period provided for in paragraph 1 above.

Section 2: Rights and obligations of the professional

Article 63.

In the event of exercising the right of withdrawal, the professional is required to reimburse any amount received from the customer in payment of his order or related to it. This reimbursement intervenes within a maximum period of seventy-two (72) hours, from the date of receipt of notification of withdrawal.

In the event of non-reimbursement within the period provided for in the preceding paragraph, the sums due to the customer are, by operation of law, increased at the legal interest rate, from the day after the expiration of the deadline.

Section 3: Loss of the right of withdrawal and termination or cancellation of contract

Article 64.

The customer loses his right of withdrawal when:

1. The goods have been delivered and received by the customer in accordance with the order;
2. The service has been provided;
3. The legal withdrawal period is forfeited.

In the event of exercising the right of withdrawal after the start of the provision of the service, the customer is required to pay the part of the price determined in proportion to the service actually provided, between the day the provision of the service begins and the day of its notification of exercise of the right of withdrawal.

Article 65.

Notwithstanding the agreement between the parties, the supplier shall execute the order within a period maximum of thirty working days, starting from the day after the conclusion of the contract.

In the event of a contractual breach by the supplier after formal notice of two (02) working days remaining without response, the customer automatically obtains the termination of the contract, by simple notification sent to the supplier by letter with acknowledgment of receipt.

The response time to all customer requests and complaints is seventy-two (72) days. hours.

In the event of termination of the contract by the customer, the supplier is required to reimburse the customer for the amounts due under the contract, where applicable, within five (05) working days from from the day of notification of termination by the customer.

CHAPTER V: ELECTRONIC ADVERTISING

Section 1: General provisions

Article 66.

Without prejudice to the legal provisions applicable to advertising in the Republic Democratic Republic of Congo, any advertising, in any form whatsoever, accessible by a electronic communications service open to the public or an online service, must be clearly identified as such upon receipt.

It makes its sender clearly identifiable, as well as the natural or legal person. on whose behalf it is carried out, by bringing to the attention of the recipients of the services its name, its geographic address at which it is established, its contact details including his email address, possibly his Trade and Companies Register Crédit Mobilier, its tax number, and the legal document authorizing the exercise of the activity.

The advertisement may be identified as such in particular because of its title, its presentation or its object.

Failing this, it includes the words “advertising” in a clear, legible, visible and non-visible manner. ambiguous, if any, in the subject or in the body of the message which carries it.

Article 67.

Promotional offers featuring price reductions, joint offers, bonuses or gifts of any nature whatsoever, provided that they are addressed or accessible by electronic communications channel open to the public or via an online service, are identifiable as such upon receipt by the user or as soon as the latter has access to them.

The conditions for benefiting from it are easily accessible and presented in a clear manner, precise and unequivocal.

Similarly, competitions or promotional games are clearly identifiable as such from the moment they are their receipt by the user or as soon as the latter has access to them.

The conditions for participation in competitions or promotional games are accessible and presented in a clear, precise and unambiguous manner. Where applicable, offers, competitions and Promotional games must be identifiable in the subject or body of the message that vehicle.

Section 2: Conditions of direct prospecting

Article 68.

Direct prospecting by means of automated communications systems is prohibited. electronic, networks, services and/or electronic communications terminals, of faxes, e-mails and SMS using personal data personal data of a user who has not previously expressed consent to receive direct prospecting by these means.

For the purposes of this article, calls and messages intended to incite the user to call a premium rate number or send a premium rate text message is the responsibility of direct prospecting.

Failure to respond cannot be considered consent.

The burden of proof of the consent of the recipient of direct marketing lies with the natural or legal person at the origin of the prospecting.

Article 69.

Direct prospecting is permitted, without the prior consent of the recipient person. physical, if all of the following conditions are met:

1. The recipient's contact details have been collected from him/her with full knowledge of the facts of cause, and in compliance with the provisions of Book III of this ordinance-law, on the occasion of a sale or provision of services;
2. Direct prospecting concerns exclusively similar products or services offered by the same supplier;
3. The recipient is offered, in a simple, express and unambiguous manner, the possibility to object free of charge to the use of your contact details at the time they are collected and each time a prospecting message is sent to him, case where he has not previously refused such exploitation.

Direct prospecting is authorized, without the prior consent of the recipient, no one moral, if the electronic coordinates used for this purpose are impersonal.

Article 70.

Any person may notify a supplier of goods or services directly online, without justification and free of charge, his wish to no longer receive direct prospecting. In this case, the supplier is required to:

1. Deliver, without delay, an acknowledgement of receipt by any means, including by post electronically, confirming to that person the registration of their request;
2. Take, within a reasonable time, the necessary measures to comply with the wishes of this person;
3. Maintain the list of people who have expressed their wish to no longer receive direct prospecting on his part.

Article 71.

When direct marketing is aimed at children, the elderly, people sick or vulnerable, or to anyone who is unable to understand fully the information presented to him, the exceptions provided for in this Title must be interpreted more strictly and without fraud.

Article 72.

It is prohibited to send messages for direct prospecting purposes using systems automated electronic communications, networks, services and/or terminals electronic communications, faxes, emails or SMS, without indicate the means and valid contact details to which the recipient transmits a request to obtain, free of charge, that these communications cease.

It is also prohibited to conceal the identity of the person on whose behalf the communication is issued, in particular in:

1. Using the email address or identity of a third party;
2. Falsifying or concealing any information that would identify the origin of the message. or its transmission path;
3. Mentioning an object unrelated to the goods or services offered;

4. Encouraging the recipient of the messages to visit third-party websites.

The Data Protection Authority provided for in Book III of this Ordinance-Law ensures, with regard to direct prospecting using the contact details of a user person physical, in compliance with the provisions of this Title using the skills assigned to it recognized.

To this end, it collects, in particular, by all means, complaints concerning breaches of the provisions of this article.

TITLE VIII: DIGITAL PLATFORMS AND SUPPLIERS POSITION DOMINANTE

Article 73.

The dominant position concerns in particular internet access providers, services cloud computing, marketplaces, app stores, networks social networks, content sharing platforms, online banking platforms, financial, travel, transportation, accommodation and search engine technologies.

The dominant position of the provider of digital activities and services is appreciated on the based on the following criteria:

1. its ability to influence the market;
2. its turnover in relation to market size;
3. the control it exercises over the means of access to the end user;
4. its ability to act independently of its competitors, customers and consumers.

Article 74.

An order from the Minister responsible for digital technology sets out the terms of application provisions relating to the regulation of digital platforms and suppliers in dominant position, the Digital Regulatory Authority being heard by an opinion according to.

TITLE IX: MONITORING, TECHNICAL CONTROL OF DIGITAL ACTIVITIES AND SERVICES, DISPUTE RESOLUTION, ADMINISTRATIVE MEASURES AND SANCTIONS AND PRESCRIPTION

CHAPTER I: MONITORING AND TECHNICAL CONTROL OF DIGITAL ACTIVITIES AND SERVICES

Article 75.

The digital sector is monitored by the Minister responsible for digital technology.
its attributions and, where applicable, through the establishments, services and/or organizations there attached in accordance with the provisions of this ordinance-law as well as the laws and regulations in force.

The provider of digital activities and services has an obligation to cooperate and act promptly following a violation reported by the bodies listed in the preceding article, on request of the latter. An order from the Minister responsible for digital technology sets out the conditions and methods of monitoring and technical control of digital activities and services.

CHAPTER II: SETTLEMENT OF DISPUTES

Article 76.

Without prejudice to the consultative competence recognized to the Regulatory Authority of Digital, it experiences disputes between digital service providers
than between users and providers of digital services.

It is seized at the request of the most diligent party or by ex officio referral.

Article 77.

The Digital Regulatory Authority may be notified of a dispute between a supplier national digital activities and services and a provider of activities and services foreign digital, at the diligence of one of the parties.

In this capacity, it contacts the Digital Regulatory Authority of the country of the supplier of the digital activities and services called into question.

Article 78.

When the Digital Regulatory Authority is contacted or informed by a competent regulatory authority of another State in the context of a dispute between a provider of national digital activities and services and a provider of activities and services foreign digital, the Digital Regulatory Authority coordinates its efforts with it in the settlement of the dispute.

Article 79.

The Digital Regulatory Authority is notified by way of a request when the request emanates from one of the parties to the dispute or precedes by way of instruction when it takes up the matter d'office.

The Digital Regulatory Authority takes action ex officio when the dispute is of a nature to undermine the continuity of services in the digital sector.

Article 80.

The Digital Regulatory Authority is attempting an amicable settlement in the event of of disputes between digital service providers or between the latter and the users.

It processes requests within a period which may not exceed thirty (30) working days. date of its referral.

The decisions of the Digital Regulatory Authority are justified and are subject to legal appeal before the Council of State in accordance with the provisions of the law. organic law no. 16-027 of October 18, 2016 relating to organization, competence and operation administrative courts.

CHAPTER II: ADMINISTRATIVE MEASURES AND SANCTIONS

Article 81.

When a provider of digital activities and services holding an authorization or a certificate of approval does not comply with the obligations prescribed by the provisions of the this ordinance-law as well as its applicable regulatory measures, including those of its specifications, on proposal or after advice from the Authority of Digital Regulation or the National Electronic Certification Authority, the

The Minister responsible for digital technology is ordering him to comply with it in a period of fifteen (15) days.

Where the digital service provider holding an authorisation or certificate approval does not comply with the formal notice sent to it, the Minister having the digital in its attributions, by a decision motivated according to the seriousness of the breach, may proceed to:

1. to the payment of a fine;
2. reduction of the validity period of the title;
3. suspension of the title;
4. upon withdrawal of the title.

Decisions to reduce the period of validity of titles, to suspend or withdraw them may be appealed before the Council of State.

CHAPTER III: PRESCRIPTION

Article 82.

1. The prescription is acquired:
2. For the benefit of digital service providers in their contractual relationships with users, for any request for reimbursement of the price of their services submitted by a user after a period of 365 days from the date of the payment ;
3. For the benefit of users in their contractual relations with suppliers of digital services, for amounts owed to a digital service provider for the payment of his benefits, when he has not claimed them in a period of 365 days from the date they become due.

BOOK II: WRITINGS, ELECTRONIC TOOLS AND TRUSTED SERVICE PROVIDERS

TITLE I: WRITINGS AND ELECTRONIC TOOLS

CHAPTER I: GENERAL PROVISIONS

Article 83.

Subject to specific legal provisions, this Title deals with writings and tools electronics in the Democratic Republic of Congo.

It sets out the rules and principles applicable in particular to:

1. electronic writing;
2. electronic signature;
3. to the electronic seal;
4. electronic time stamping;
5. electronic certification;
6. authentication of websites.

It also applies to any sequence of letters, characters, numbers, digits, symbols or any other saved signs that have an understandable meaning on a electronic media, regardless of the methods of their transmission.

CHAPTER II: ELECTRONIC WRITING

Section 1: General principles

Article 84.

Electronic writing obeys the principles of:

1. integrity;
2. freedom;
3. transparency;
4. clarity.

Article 85.

The integrity of an electronic document results from:

1. The ability to verify that the information is not altered and that it is maintained in its entirety;
2. The certainty that the electronic medium carrying the information provides it with the stability and sustainability desired.

Article 86.

No one may be forced to use electronic writing.

Article 87.

Any person who uses electronic writing ensures that the information they provide on electronic media, guarantee authorized access and use an open standard.

Article 88.

Electronic writing consists of readable content and a quality that guarantees its understanding.

Section 2: Validity of electronic writing

Article 89.

Electronic writing has the same legal value as writing on paper.

Article 90.

The authentic act established on electronic media has the same legal value as the act authentic on paper subject to the conditions of validity provided for herein ordinance-law.

An interministerial decree of the Ministers responsible for justice and digital technology respectively their attributions, defines the conditions and modalities of this article.

Article 91.

The electronic document is time-stamped and includes a certified electronic signature.

The time stamp and the certified electronic signature give the electronic document the same probative force than the writing on legalized paper having a certain date.

Article 92.

Subject to specific legal provisions, where a writing is required for validity of a legal act, it is established and stored in electronic form according to the conditions provided for in this Book.

Documents or titles that legal and regulatory texts subject to conditions particular in form and substance, take the form of electronic writing provided that it complies, in addition to these specific requirements, with those of this Book.

Article 93.

May in particular take the form of electronic writing following specific rules and specific:

1. contracts;
2. acts relating to the civil law of persons;
3. acts relating to personal or real securities, of a civil or commercial nature;
4. acts which create or transfer real rights over immovable property;
5. legal acts for which the law requires the intervention of courts and tribunals;
6. the declarative and liquidative acts of the tax, parafiscal and customs administrations and social security;
7. invoices for goods and various services provided by individuals or legal entities, public or private;
8. all other acts for which the law requires not only a written document in paper format or in any format other than electronic format, but also certain special formalities.

Article 94.

The legal and judicial professions use electronic writings and tools in the establishment of their acts and in the administration of proof.

The players in these professions, in particular notaries and bailiffs, guarantee legal and technical security through verification and certification processes.

All information concerning the act, from its establishment, such as data allowing it to be identified, its properties to be determined and its traceability to be ensured, is also preserved.

Section 3: Electronic evidence

Article 95.

Electronic writing is admissible as proof in the same way as the original of the writing on paper. and has the same evidentiary force as the latter, provided that the person from whom it emanates and that it is established and preserved in conditions of a nature in ensure integrity in accordance with legislation relating to the conservation of archives.

Article 96.

The preservation of writings in the form of documents, recordings or information under electronic form meets the following requirements:

1. the documents, recordings, contents or electronic information stored are stored in such a way that they are accessible and searchable;
2. the documents, recordings, contents or electronic information stored remain in the format in which they were generated, sent or received, or are in a format guaranteeing the integrity and accuracy of the information generated, sent or received;
3. the documents, recordings, contents or electronic information stored in a format that allows their origin and destination to be identified, where applicable as well as the date and time they were generated, sent and received for the first time, as well as those for which they were first preserved.

The technical specificities related to the storage format will be defined by the National Electronic Certification Authority.

Article 97.

Any electronic document, record, content or information meets the obligations legal to present or retain the information they contain in their form original, since:

- the integrity and accuracy of the information generated are guaranteed and maintained reliably;
- it is possible to reproduce accurately all of the information such as that they were first generated.

The integrity requirement referred to in this Article is satisfied when the information is remained complete and unchanged.

Article 98.

The copy or reproduction of an act in electronic form has the same value and force probative as the act itself provided that it preserves the integrity of the electronic act original.

Integrity is proven by means of a certificate of conformity issued by a service provider. trust services in accordance with Book II of this Ordinance-Law.

Article 99.

In cases where the production of a document in physical format is required, a printout on paper of said document certified as a true copy of the original may be admitted.

This certification is provided by a trusted service provider in accordance with the provisions of Book II of this ordinance-law.

Article 100.

The delivery of a document in electronic form is effective when the recipient, after having was able to take note of it, acknowledged receipt.

Article 101.

Electronic communication may be made by registered mail with acknowledgment of receipt. reception. In this case, it is routed by a third party using a process that allows determine reliably and accurately:

1. the identity of the sender, the recipient and the third party who forwards the communication electronics;
2. the date and time the message was sent;

3. the date and time the message was received by the recipient;
4. where applicable, technical data relating to the routing of the message the sender to the recipient;
5. the acknowledgement of receipt is sent to the sender electronically or by any other means means of preserving and reproducing it.

Article 102.

Data sent and received using a registered electronic delivery service qualified persons benefit from a presumption as to the integrity of the data, from the sending of these data by the identified sender.

They also benefit from a presumption of the accuracy of the date and time of sending. and receipt, upon receipt by the recipient identified by the sending service qualified recommended electronics.

Article 103.

Qualified electronic registered mail services must:

1. be provided by one or more qualified trust service providers;
2. ensure the identification of the sender with a high degree of confidence;
3. ensure the identification of the recipient with a high degree of confidence before the provision of data;
4. ensure that sending and receiving data is secured by a signature certified electronic or by a qualified electronic seal from a service provider qualified trust services, so as to exclude any possibility of modification data;
5. ensure that any changes to data necessary for sending or receiving these are clearly identifiable and reported to the sender and recipient of the data. The date and time of sending and receipt, as well as any changes to the data, are indicated by a certified electronic timestamp.

In the event that data is transferred between two trusted service providers qualified or more, the requirements set out in this article apply to all service providers qualified trust services.

CHAPTER III: ELECTRONIC TOOLS

Section 1: Electronic signature

Article 104.

Without prejudice to the specific legal provisions in force in the Democratic Republic of Congo, the electronic signature is an element of validity of a legal act. It identifies the person who affixes it and manifests his consent to the obligations arising from it. Electronic signature is permitted in electronic exchanges and transactions.

The electronic signature can be simple or qualified.

Article 105.

Anyone wishing to affix their simple electronic signature to a document uses to the trusted service provider.

Article 106.

The qualified electronic signature meets the following requirements:

1. be linked to the signatory in a unique manner;
2. enable the signatory to be identified;
3. be created using electronic signature creation data that the signer can, with a high level of confidence, use under its exclusive control;
4. be linked to the data associated with this signature in such a way that any modification subsequent data collection is detectable.

Article 107.

The reliability of an electronic signature process is presumed to be established until proven. contrary when this process implements a qualified electronic signature; and this, thanks to a secure device for creating electronic signatures and verifying this signature is based on the use of a qualified device.

Article 108.

The qualified electronic signature linked to a qualified electronic certificate has the same force more convincing than the handwritten signature.

Article 109.

Unless proven otherwise, a document written in electronic form is presumed to have been signed by its author and its text is presumed not to have been modified if an electronic signature qualified is affixed there.

Article 110.

A qualified electronic signature is one that results from a reliable identification process which guarantees its link with the act to which it relates in such a way that any modification subsequent to said act is detectable.

Qualified electronic signature certifications meet integrity requirements provided for in this Book.

Qualified electronic signature certificates guarantee interoperability and recognition of qualified electronic signatures across borders.

Article 111.

A qualified electronic signature certificate revoked after its first activation loses its validity from the time of its revocation.

This revocation does not affect the previous validity of the certificate, unless it is established that:

1. the certificate was issued on the basis of false information;
2. the certificate was issued on the basis of an unlawful cause or object;
3. the certificate was issued in violation of the provisions of this Ordinance-Law.

Article 112.

Qualified electronic signature creation devices meet the requirements following:

1. the guarantee of technical means and appropriate procedures, in particular:
   - confidentiality of data used for creation;
   - the certainty that the verification data corresponds to the creation data;

- the reliability of the signature and the protection of the data of its creation against any falsification by technical means;
- the reliability of the signature and the protection of its creation data against possible use by third parties.

2. qualified electronic signature creation devices do not modify the data to be signed and do not prevent the presentation of such data to the signatory before the signature ;
3. the generation or management of electronic signature creation data for the The signatory's account is exclusively entrusted to a trusted service provider qualified.

Article 113.

Without prejudice to the provisions of the preceding article, a trusted service provider qualified manager of electronic signature creation data on behalf of a The signatory may only reproduce the electronic signature creation data for the purposes safeguard, subject to compliance with:

1. the level of security of the reproduced data sets must be equivalent to that original data sets;
2. the number of datasets reproduced does not exceed the minimum necessary to ensure continuity of service.

Article 114.

Certification of the simple or qualified electronic signature creation device is provided by the National Electronic Certification Authority in accordance with the requirements fundamental techniques according to:

1. the system or product in which the private signing key is implemented is certified;
2. systems or products contributing to protecting this private key against a use by others than the legitimate signatory are certified;
3. cryptography.

An order from the Minister responsible for digital technology determines the requirements possible additional techniques adapted to technological developments as well as other necessary operational arrangements.

Article 115.

The process of validating a qualified electronic signature confirms its validity to conditions below:

1. the conformity of the certificate with the requirements of this text;
2. the issuance by a qualified trust service provider of said certificate as well as that its validity at the time of its signature;
3. the correspondence of the data to be validated from the signature to those communicated to the person concerned;
4. the unique and correct representation of the data provided to the data subject;
5. the clear indication of a pseudonym if applicable;
6. the certainty that it is created by a qualified and certified creation device.

Article 116.

Qualified validation services for qualified electronic signatures cannot be provided only by a qualified trusted service provider who:

1. provides validation in accordance with the requirements applicable to the validation of qualified electronic signatures;
2. allows users to receive the result of the validation process of a automated, reliable, efficient manner and bearing the qualified electronic signature or the qualified electronic seal or the qualified electronic seal of the service provider who provides the qualified validation service.

Article 117.

The qualified storage service for qualified electronic signatures cannot be provided only by a qualified trust service provider who uses procedures and

technologies to extend the reliability of qualified electronic signatures beyond
of the technological validity period.

Section 2: Electronic stamp

Article 118.

The electronic seal is accepted in electronic exchanges and transactions and strengthens the validity of the electronic document. Its validity is subject to the same requirements as those to which the electronic signature is subject in accordance with this Book.

A qualified electronic seal benefits from a presumption of data integrity and
accuracy of the origin of the data to which it is linked.

Article 119.

The provisions of Article 106 apply mutatis mutandis to the stamp requirements.
qualified electronics.

Article 120.

Without prejudice to the provisions of this Ordinance-Law, the provision of the stamp
electronic to a service meets the following requirements:

1. Be a qualified electronic stamp;
2. Be a qualified electronic seal based on a qualified certificate;
3. Be a qualified electronic stamp in at least the formats or using the
   methods provided for in this ordinance-law.

Article 121.

The qualified electronic stamps required for the use of an online public service are:

1. Those which are based on a qualified certificate;

2. Those whose formats use the methods provided for by the Minister's decree referred to in the following paragraph of this article.

An order from the Minister responsible for digital technology determines the formats of reference of qualified electronic stamps as well as additional usage requirements electronic signatures and seals in the public sector.

Article 122.

Qualified electronic seal certificates meet the following requirements:

1. A statement indicating, at least in a form suitable for automated processing, that the certificate was issued as a qualified electronic seal certificate;
2. A data set unambiguously representing the service provider of qualified trust issuing qualified certificates, including at least:
   - For a legal entity: the registered office, the company name and, where applicable where applicable, identification information relating to its legal status;
   - For a natural person: the first name, last name and last name of the person;
3. The name of the creator of the stamp and, where applicable, the related identification information to its legal status;
4. Correspondence of the validation data of the electronic stamp to those of creation ;
5. The validity of the certificate;
6. The unique identity code for the qualified trust service provider;
7. The qualified electronic signature or qualified electronic seal of the service provider qualified trust services issuing the certificate;
8. The place of issue of the certificate on which the qualified electronic signature is based or the qualified electronic seal;
9. The location of services that can be used to know the status of validity of the qualified certificate.

Article 123.

A qualified electronic stamp creation device is a stamp creation tool electronics which meets mutatis mutandis the requirements applicable to devices of creation of qualified electronic signatures.

Article 124.

The criteria for validation and conservation of qualified electronic seals meet mutatis mutandis to the provisions applicable to electronic signature.

Section 3: Electronic time stamping

Article 125.

The legal effect and admissibility of an electronic timestamp cannot be denied as evidence solely on the grounds that the timestamp is in electronic form or that it is not does not meet the requirements for certified electronic time stamping.

A certified electronic timestamp benefits from a presumption of accuracy of the date and the time it indicates and the integrity of the data to which these dates and times relate.

Article 126.

Certified electronic time stamping meets the following requirements:

1. Link the date and time to the data in such a way as to exclude the possibility of a indefectible modification of this data;
2. Be based on an accurate clock linked to coordinated universal time; and
3. Be signed using a qualified electronic signature or sealed using a qualified electronic seal of the qualified trust service provider.

Section 4: Website authentication

Article 127.

Qualified website authentication certificates must contain:

1. A statement indicating, at least in a form suitable for automated processing, that the certificate was issued as a qualified site authentication certificate internet ;

2. A data set unambiguously representing the service provider of
qualified trust issuing qualified certificates, including at least:
- For a legal entity: the registered office and identification information
linked to its legal status,
- For a natural person: first name, last name and post-name;
3. For the natural person, at least the name of the person to whom the certificate was issued
issued, or a pseudonym. If a pseudonym is used, this is clearly indicated;
4. For the legal entity, the business name under which the certificate is issued
as well as identifying information relating to its legal status;
5. The details of the address of the natural or legal person to whom the certificate is
issued and the elements as they appear in the official registers;
6. The domain name(s) operated by the natural or legal person to whom the
certificate is issued;
7. Details of the start and end of the certificate's validity period;
8. The certificate identity code, which must be unique to the service provider.
qualified trust;
9. The qualified electronic signature or qualified electronic seal of the service provider
qualified trust services issuing the certificate;
10. The place where the certificate on which the electronic signature is based can be obtained
qualified or the qualified electronic seal referred to in point 8;
11. The location of certificate validity status services that may be
used to know the validity status of the qualified certificate.

Article 128.

The qualified website authentication certificate is issued by a service provider
quality trust services and meets the requirements set out in Article 127 of this
ordinance-law.

TITLE II: TRUSTED SERVICE PROVIDERS

CHAPTER I: GENERAL PROVISIONS

Article 129.

The legal provisions relating to trust services apply to providers of trust services established in or destined for the Democratic Republic of Congo.

They set:

1. the rules applicable to trust services;
2. means of securing electronic documents;
3. certificate services for electronic signature or seal, time stamping electronic, electronic registered mail and website authentication.

Article 130.

Trusted service providers are those who provide services following:

1. electronic signature;
2. the electronic seal;
3. electronic time stamping;
4. electronic archiving;
5. electronic certification;
6. website authentication;
7. electronic registered mail;
8. cryptology.

An order from the Minister responsible for Digital Technology completes the list of providers of trusted services, the National Electronic Certification Authority heard by written notice.

Article 131.

On the proposal of the Minister responsible for Digital Affairs, the Government is implementing in place a national public key infrastructure, the basis of the techniques of the services trust, and determines the terms of its implementation and operation.

CHAPTER II: PRINCIPLES AND CATEGORIES OF SERVICE PROVIDERS

Section 1: Principles

Article 132.

Trust service providers adhere to the principles of:

1. non-discrimination ;
2. functional equivalence;
3. technological neutrality;
4. autonomy.

Article 133.

The trust service provider is required to guarantee, regardless of any consideration, in particular of color, sex, language, religion, national origin, ethnic or social, the integrity and reliability of the trusted service(s) it provides.

Article 134.

The trusted service provider providing one or more services is free to use any technology, certified by the National Electronic Certification Authority, which guarantees the inviolability of several trusted services provided.

Article 135.

Trust services provided by a trust service provider located in the foreigner has the same value and is assimilated to the trust service provided by a service provider trust services established in the Democratic Republic of Congo if the two conditions following are met:

1. the trust service provider must have representation in the territory of the Democratic Republic of Congo;
2. the trust service provider meets the conditions set out in this Book, after verification by the National Electronic Certification Authority.

Section 2: Categories of Trusted Service Providers

Article 136.

Trusted service providers are of two categories:

1. qualified trust service providers;
2. unqualified trust service providers.

Article 137.

Qualified trust service providers are subject to the authorization regime:
while the reporting regime is required for trust service providers
unqualified.

Article 138.

The authorization and declaration are made in accordance with the provisions of Book I.
of this ordinance-law.

Article 139.

Practical arrangements for carrying out activities relating to cryptology and algorithms
specialized data security measures are carried out in accordance with the provisions of this
ordinance-law.

An order from the Minister responsible for digital technology determines the terms and conditions
practices as well as the conditions for carrying out the activities referred to in the preceding paragraph.

Article 140.

Unqualified trust service providers who wish to carry out trust services
qualified trustees submit to the National Electronic Certification Authority, a
request accompanied by a conformity assessment report.

Article 141.

The National Electronic Certification Authority verifies in particular that the requests of Trust service providers and the trust services provided comply with the provisions of this ordinance-law.

The National Electronic Certification Authority shall decide within thirty (30) days date of request.

If the required conditions are met, it grants the status of “qualified” to the requesting provider.

In the event of refusal, it shall rule by means of a reasoned decision which it shall notify to the applicant.

Article 142.

The admission of trust service providers to one of the legal regimes provided for by this ordinance-law takes into account:

1. the infrastructure, technical security and organizational measures implemented by the service provider;
2. the regularity and extent of the certified audits carried out to verify compliance with its services to its statements and policies;
3. financial guarantees for his civil liability;
4. guarantees of impartiality, independence and probity of the service provider;
5. accreditation or assessment of the quality of its security processes already in place awarded to the service provider established abroad by an independent body.

CHAPTER III: OBLIGATIONS AND RESPONSIBILITIES

Section 1: Obligations and liability of trust service providers

Paragraph 1: Obligations

Article 143.

The qualified trust service provider established in the Democratic Republic of Congo is required to submit to the National Electronic Certification Authority, in particular, the following information:

1. For a natural person:
   - his first name, last name and post-name;

- his home address, his email address and his telephone number phone ;
- his certified electronic signature;
- its certified electronic seal;
- all mandatory information inherent to its legal status.

2. For a legal entity:
   - proof of registration in the Trade and Personal Property Credit Register ;
   - its company name;
   - its head office, its email address and its telephone number phone ;
   - his certified electronic signature;
   - its certified electronic seal;
   - all mandatory information inherent to its legal status.

Article 144.

The qualified trust service provider must:

1. inform the National Electronic Certification Authority of any changes in the provision of its qualified trust services and its possible intention to cease its activities;
2. demonstrate that it has reliable technical means to provide the services of qualified trust in complete safety;
3. ensure the operation of a fast and secure directory service and a safe and immediate revocation;
4. ensure that the date and time of issue and revocation of a certificate can be determined precisely;
5. take measures against counterfeiting of certificates and, in cases where the Trusted service provider generates data relating to the creation of electronic signature or seal, ensuring confidentiality during the process of generation of this data;

6. take out an insurance policy covering any damage that may occur
caused in the exercise of this activity;
7. employ staff with the expertise, experience and qualifications
necessary for the security of computer networks and systems;
8. inform users of qualified trust services in a clear manner,
exhaustive and before any contractual relationship, on the precise conditions of use
of the service, including limits on its use, complaints and recovery procedures
dispute resolution. This information may be transmitted electronically and
must be easily understandable. Relevant elements of this information
must also, upon request, be made available to third parties who claim the
certificate ;
9. use reliable systems and equipment, protected against risks of
modifications and ensuring the technical security of the supported processes;
10. use reliable systems for storing data communicated to it, under
a verifiable form so that:
- the data are only publicly available for processing after
having obtained the consent of the person concerned;
- only data controllers can enter and modify data
the data retained;
- the authenticity of the data can be verified.
11. take appropriate measures against falsification, hacking and theft of data
;
12. record, store and keep accessible for a period of administrative utility
fixed in an archive retention schedule, including after the cessation of the
activities of the qualified trust service provider, all information
relevant to the data sent and received by the service provider
qualified trust, particularly for evidentiary and service continuity purposes;
13. have an updated business shutdown plan to ensure service continuity;
14. ensure the lawful processing of personal data in accordance with the
provisions of this ordinance-law;
15. establish, make public and maintain a database of certificates granted;

16. ensure that certificates are only available to the public in cases where the certificate holder has given consent;
17. take out a liability insurance policy.

Article 145.

The trust service provider is required to send a reasoned notification to the beneficiary of the trusted service prior to any revocation of the certificate.

When the revocation is effective, he is required to publish this revocation in the newspaper technical aspects of its servers.

Qualified trust service providers provide users with information relevant to the validity or revocation status of the certificates they have issued. These information is available, at least by certificate, at any time and beyond the period validity of the certificate, in an automated, reliable, free and efficient form.

Article 146.

Without prejudice to the provisions of Book III of this Ordinance-Law, the service provider Trust services that issue certificates to the public cannot collect data personal data only directly from the person concerned, with the explicit consent of the latter, and only to the extent that this is necessary for the delivery and certificate retention.

The data transmitted to them, in particular personal data, does not may be collected or processed for other purposes without the express prior consent of the interested person.

Service providers may only hold, consult, exploit and disclose this data in the measure strictly necessary for the performance of their services.

Where the certificate holder uses a pseudonym and the investigation requirements of police or judicial investigations require it, the trust service provider having issued the certificate is required to communicate to the competent authority any data and/or information relating to the identity of the holder at his disposal.

Article 147.

Qualified and non-qualified trust service providers are required to take the following technical and organizational measures necessary to prevent and manage risks related to the security of the trust services they provide. Given the developments technological, these measures ensure that the level of security is proportional to the degree of risks.

Measures are taken in particular to prevent and limit the consequences security incidents, to inform the parties concerned of the detrimental effects of such incidents incidents and to ensure continuity of services in the event of technical failures in their head or cessation of activity.

Article 148.

Qualified and non-qualified trust service providers notify the Authority National Electronic Certification by any means, and where appropriate, to others organizations concerned, within twenty-four (24) hours of having received them knowledge, any breach of security or loss of integrity having an impact significant on the trust service provided or on the personal data contained therein are preserved.

Article 149.

Where the targeted security breach or loss of integrity is likely to cause harm to a user of the trust service, the trust service provider notifies him also the breach of security or loss of integrity within twenty-four (24) hours.

Where the threat to security or loss of integrity concerns a foreign State, the Authority The National Electronic Certification Authority which has received notification shall inform the Authority in advance the competent authorities.

The National Electronic Certification Authority also informs the public or required of the trust service provider that it informs the public, as soon as the National Electronic Certification Authority finds that it is in the public interest to be alerted of the breach of security or loss of integrity.

Article 150.

When a qualified trust service provider issues a qualified certificate for a trust service, it verifies by appropriate means the identity and, where appropriate, all the identification details of the natural or legal person to whom it issues the certificate qualified.

This information is verified by the qualified trust service provider.

Means of verification include, in particular:

1. the physical presence of the person concerned or the authorized representative of the legal entity;
2. the qualified electronic signature or qualified electronic seal certificate;
3. other identification methods recognized in the Democratic Republic of Congo which provide an equivalent guarantee in terms of reliability to physical presence of the person concerned or the authorized representative of the legal person. The equivalent guarantee is confirmed by the National Electronic Certification Authority.

Article 151.

At the request of the holder of the previously identified certificate, his beneficiaries or his proxies, the trust service provider immediately revokes the certificate.

Article 152.

The trust service provider also revokes a certificate when:

1. there are serious reasons indicating that the certificate was issued on the basis of erroneous or falsified information, that the information contained in the certificate are no longer valid or that the confidentiality of the data relating to the signature has been raped or are at risk of being raped;
2. the trust service provider takes the necessary measures to respond to at any time and without delay to a request for revocation.

Article 153.

When the revocation decision is made, the trust service provider notifies the revocation of the certificate to the holder within thirty (30) days before the expiration of the certificate. The revocation decision must be justified.

The certificate holder has thirty days to lodge an appeal with the the competent authority. This period begins on the day of notification of this decision by the trusted service provider.

Paragraph 2: Responsibility

Article 154.

The trusted service provider is liable for any harmful acts caused by negligence or clumsiness to any natural or legal person.

In this case, it is the responsibility of the natural or legal person claiming damages to provide proof.

However, in the event that the trusted service provider has previously informed the natural or legal person of the technological limits of its services and that these limits have been reported to the National Electronic Certification Authority, it cannot be held liable for damages incurred through the use of the services beyond its limits.

Section 2: Obligation and responsibility of the certificate holder

Paragraph 1: Of the obligation

Article 155.

The holder of an electronic certificate is required to take all necessary measures to keep it under its exclusive control to prevent theft, loss or disclosure.

In the event of theft, loss or disclosure, the holder must immediately inform the trusted service provider for the latter to revoke it.

In case of doubt or risk of violation of the confidentiality of data relating to the electronic signature or seal, or in the event of non-conformity of the information contained in the certificate, the holder has the right to have it revoked.

When a certificate has expired or has been revoked, the holder may not, after certificate expiration or revocation, use signature data to sign or have this data certified by another trusted service provider.

Paragraph 2: Responsibility

Article 156.

Any action taken with a stolen, lost or disclosed certificate without the holder having taken measures for its revocation are deemed valid and binding on the holder.

The certificate holder is liable for all damages caused to third parties by acts taken in the context of the preceding paragraph.

TITLE V: CONTROL OF TRUSTED SERVICE PROVIDERS

Article 157.

Control of the activities of trust service providers is exercised in the conditions provided for by the laws and regulations in force.

Article 158.

Qualified trust service providers are subject, every twenty-four (24) months, to: of an audit carried out by an audit firm or a conformity assessment body.

The objective of this audit is to confirm that qualified trust service providers and the qualified trust services they provide meet the requirements set by the present ordinance-law.

Within ten (10) business days of receipt, the service providers of qualified trustees transmit the conformity assessment report to the National Authority of Electronic Certification.

Article 159.

Without prejudice to the provisions of the preceding article, the National Certification Authority Electronics may, at any time, submit qualified trust service providers to an audit or request a conformity assessment body to carry out an assessment of the conformity of qualified trust service providers, at their expense

latter, in order to ensure that the qualified providers and trusted services they provide meet the requirements set out in this Book.

The conformity checks carried out by the National Electronic Certification Authority do not may be abusive and must be justified in light of the situation of the service provider of trust and the elements concerning it that it has.

Article 160.

The National Electronic Certification Authority maintains and publishes trusted lists including information relating to qualified trust service providers, as well as that information relating to the qualified trust services they provide.

The National Electronic Certification Authority establishes, maintains and publishes in a secure and in a form suitable for automated processing, the trusted lists referred to in Article 1 relating to electronic signatures and electronic seals.

The National Electronic Certification Authority makes available to the public, by through a secure channel, the information referred to in the preceding paragraphs under a form bearing an electronic signature or an electronic seal suitable for processing automated.

TITLE VI: CESSATION OF ACTIVITIES

Article 161.

The trust service provider ceases its activities:

1. if its technological and material means no longer guarantee the security of certificates issued;
2. if it no longer has the necessary financial cover to enable it to carry out its activities;
3. if he voluntarily decides to leave the sector;
4. if he is subject to an administrative sanction.

Article 162.

The trust service provider informs the National Electronic Certification Authority sixty (60) days of its intention to cease its activities or of any fact which could lead to the cessation of its activities.

In this case, it ensures that its activities are taken over by another service provider. trust guaranteeing an equivalent level of quality and security. This transfer of activities is carried out under the control of the National Electronic Certification Authority.

In the absence of a buyer, the service provider revokes, subject to sixty (60) days' notice days, the certificates granted to its holders.

Article 163.

The trust service provider that ceases its activities for independent reasons of its will or in the event of bankruptcy, immediately informs the National Electronic Certification Authority. It proceeds, where appropriate, to revoke the certificates issued.

TITLE VII: ADMINISTRATIVE SANCTIONS

Article 164.

Where the trust service provider fails to comply with the provisions of the this ordinance-law and the requirements set by the National Electronic Certification Authority, the latter pronounces against it, in compliance with the principle of contradictory, the following sanctions:

1. the injunction to cease for a period of ninety (90) to three hundred and sixty-five (365) years days the provision of trust services and/or the payment of a sum ranging from five hundred thousand to five million Congolese francs when the impact of the breach is limited to the holder;
2. the obligation for the trust service provider to immediately inform the holders of the qualified certificates that it has issued, of their non-compliance with the provisions of this Ordinance-Law and the payment of a sum ranging from ten million to fifty million Congolese francs when the impact of the failure affects the integrity of personal data of holders;
3. the ban on practicing in the Democratic Republic of Congo, when the breach affects national defense or state security.

Article 165.

When the National Electronic Certification Authority requires the service provider to qualified trust that it corrects a failure to comply with the requirements set out in this statutory order and the service provider does not act accordingly after expiry of a period reasonable set by the Electronic Certification Authority, the latter has the possibility, in taking into account the extent, duration and consequences of the breach, to withdraw the "qualified" status to the provider or trust service concerned, and informs the authority competent for the purposes of updating the targeted trusted lists.

The National Electronic Certification Authority also informs the service provider of qualified trust services from the withdrawal of its "qualified" status or from the withdrawal of the "qualified" status qualified" of the relevant trust service.

The withdrawal of qualified status from a trusted service provider overrides the services it provides.

The trust service provider has, prior to any legal action, of a right of appeal to the Certification Authority.

The legal remedy is exercised before the Court of Appeal in accordance with the organic law No. 16-027 of October 18, 2016 relating to the organization, competence and operation of administrative courts.

BOOK III: DIGITAL CONTENT

TITLE I: PURPOSE AND SCOPE OF APPLICATION

Article 166.

Without prejudice to specific legal and regulatory provisions, this Book sets out the rules relating to public data and the protection of personal data.

TITLE II: PUBLIC CONTENT

CHAPTER I: GENERAL PROVISIONS

Article 167.

Public data is that produced, received or processed within the framework of the missions of public service by the public administration, establishment, body and company or the legal entities under private law charged with such a mission and are stored in the public data registers of the Democratic Republic of Congo.

Article 168.

Public data registers are classified into several categories including:

1. **National Population Register :** identity register, civil status register, biometric register.
2. **Land and property register :** cadastral register, property register, register of notarial deeds of real estate, register of leases, register of mines, forest register, agricultural register.
3. **Register of permits and licenses :** register of concessions, register of commercial licenses and/or permits, personal register of licenses and/or permits, register of driving licenses.
4. **Invoice and payment register :** invoice register, point of sale register, e-commerce register and electronic payment register.
5. **Register of citizens and migrants :** register of natural persons, register of beneficial owners, and register of visas.
6. **Asset register :** motor vehicle register, telephone register, airport register.
7. **Judicial register :** register of decisions taken by the Courts and Tribunals of all levels of jurisdiction.
8. **Register of health, education, social activities,** etc.

In accordance with the provisions of this ordinance-law, the data extracted from these Registers are used in many administrative services, whether in the form of certificates or via direct access to this data when it is digital.

A Decree of the Prime Minister deliberated in the Council of Ministers and completed, on proposal of the Minister responsible for digital technology in collaboration with the Ministers sectors concerned, the list and categories of public data registers mentioned in this Article, the Personal Data Authority being consulted by written notice.

Article 169.

Administrations are required to publish online and/or communicate documents administrative data that they hold to persons who request them under the conditions provided for by this ordinance-law.

Article 170.

The right to communication only applies to final documents.

This right to communication does not concern:

- preparatory documents for an administrative decision while it is being prepared;
- documents deemed strategic by the State;
- documents relating to private life;
- documents relating to defence and national security;
- documents for which third parties hold the property rights.

An order from the Minister responsible for digital technology completes or modifies the list documents which are not subject to the right to communication depending on the circumstances by regulatory route.

CHAPTER II: ELECTRONIC IDENTIFICATION

Section 1: Principles and obligations

Article 171.

Electronic identification is a process that involves the use of data identity of a natural or legal person by electronic means which represent unequivocally the natural or legal person concerned.

Article 172.

The State carries out, by means of electronic identification, the general identification of the population and issues a national identity card with a unique identifier to nationals.

A unique identifier resident card is issued to foreigners residing in the Republic Democratic Republic of Congo.

A unique identifier refugee card is issued to persons in a refugee situation in Democratic Republic of Congo.

Article 173.

On the proposal of the Ministers responsible for the Interior and Digital Affairs, a Decree of the Prime Minister deliberated in the Council of Ministers determines the elements, the technical specifications of electronic identification means, diagrams electronic identification and their levels of guarantee certifying the identification as well as the interoperability framework.

Section 3: Electronic diagram

Article 174.

An electronic identification scheme determines the specifications of the warranty levels low, substantial and/or high electronic identification means issued within the framework of said diagram:

The low level of guarantee is that provided by an electronic identification means which grants a limited degree of reliability to a person's claimed or purported identity concerned. It is characterized on the basis of technical specifications, standards and related procedures, including technical controls aimed at reducing the risk of misuse or alteration of the identity of the data subject;

The substantial level of guarantee is that provided by an electronic means of identification which grants a substantial degree of reliability to the claimed or alleged identity of a person concerned. It is characterized on the basis of technical specifications, standards and related procedures, including technical controls, the aim of which is to reduce substantially the risk of misuse or alteration of the person's identity concerned;

The high level of guarantee is that provided by an electronic identification means which grants a higher level of reliability to a person's claimed or purported identity than a means of electronic identification with a substantial level of guarantee. It is characterized on the basis of technical specifications, standards and related procedures, including technical controls, the aim of which is to prevent misuse or alteration of identity.

Article 175.

The electronic identification scheme is eligible if:

1. means of identification covered by the electronic identification scheme may be used to access any service provided by an entity or public administration requiring electronic identification;
2. the electronic identification scheme and the means of identification electronic products delivered meet the requirements of at least one of the guarantee levels provided for in Article 174;
3. the electronic identifier is assigned to the data subject in accordance with the technical specifications, standards and procedures for the guarantee levels.

Article 176.

A Decree of the Prime Minister deliberated in the Council of Ministers on the proposal of the Minister having digital in its attributions sets the technical specifications, standards and minimum procedures on the basis of which the levels of guarantees low, substantial and high are ensured by the electronic identification means provided for in Article 175 of the present ordinance-law.

These technical specifications, standards and minimum procedures are set by reference to the quality and reliability of the following elements:

1. the procedure for verifying and proving the identity of natural or legal persons requesting the issue of electronic identification means;
2. the procedure for issuing the requested electronic identification means
3. the authentication mechanism by which the data subject uses/confirms his/her identity;
4. the entity issuing the electronic identification means;
5. any other body associated with the request for the issue of electronic identification means;
6. the technical and security specifications of the electronic identification means issued.

Article 177.

In the event of a security breach or alteration of the electronic identification scheme affecting the reliability of the authentication of this scheme, the National Certification Authority Electronics suspends and, where appropriate, the Supervisory Minister revokes this without delay authentication or altered elements.

Where the breach of security or alteration referred to in the first paragraph has been remedied, the competent authority re-establishes authentication.

Article 178.

The institution providing electronic identification is liable for damages caused intentionally or through his negligence to any user of the means of identification electronic in accordance with current legislation.

Article 179.

Electronic identification schemes are interoperable.

Article 180 :

Application measures ensure that this interoperability framework:

1. is technologically neutral and does not discriminate between special technical solutions intended for electronic identification;
2. follows international standards and recommendations;

3. facilitates the implementation of privacy principles from the conception ;
4. ensures that personal data are processed in accordance with the provisions of the law, in particular the provisions of this Ordinance-Law.

Article 181 :

The establishment of the interoperability framework meets the requirements:

1. a reference to the minimum technical requirements relating to the guarantee levels provided for in Article 174;
2. a table of correspondences between the guarantee levels of the notified electronic identification schemes and the guarantee levels provided for in Article 174;
3. a reference to the minimum technical requirements for interoperability;
4. of a reference, in the electronic identification scheme, to a set minimum amount of data allowing a natural or legal person to be uniquely identified;
5. procedural rules governing interoperability;
6. provisions governing the settlement of disputes;
7. common operational safety standards.

Section 4: Obligations relating to electronic identification means

Article 182.

The holder of an electronic means of identification is required to take all measures necessary to keep it under its exclusive control in order to prevent theft, loss or disclosure. In this case, the holder must immediately revoke the means of identification electronic.

When the electronic identification means expires or is revoked, its holder can't use it anymore.

TITLE III: PERSONAL DATA

CHAPTER I: GENERAL PROVISIONS

Article 183.

The following categories are considered personal data. These include:
of :

1. personal identification data including: first name, last name, last name, date and place of birth, age, marital status, national identification number, valid official identity document and any other biometric data including photograph, sound recording, image, fingerprints and irises.
2. correspondence data: telephone contact details, physical, postal and electronic addresses;
3. professional data: status, job held, employer, remuneration ;
4. billing and payment data: invoice amount and history, payment status, reminders, payment balances, collection date;
5. bank details: bank code, account and card number banking, bank name/address/contact details, transaction references;
6. data on legal entities under public or private law display personal data;
7. data on family situation;
8. data concerning court decisions.

Article 184.

The following are subject to the provisions of this Title:

1. the collection, processing, transmission, storage and use of personal data by the State, the Province, the Territorial Entities Decentralized and Deconcentrated, legal persons under public or private law and natural persons,
2. the automated or non-automated processing of data contained or intended to be included in a file;
3. data processing carried out on national territory or abroad;
4. the processing of data concerning public security, defence, investigation and prosecution of criminal offences or state security, subject to exceptions defined by specific provisions set out in other laws in force.

Article 185.

The following are excluded from the scope of this title:

1. the processing of data carried out by a natural person in the exclusively within the framework of his personal or domestic activities, provided that the data is not intended for systematic communication to third parties or for dissemination;
2. temporary copies made as part of technical activities of transmission and provision of access to a computer network, for the purpose of

automatic, intermediate and transient storage of data and for the sole purpose of allowing other recipients of the service the best possible access to the information transmitted;

3. processing of personal data carried out by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

CHAPTER II: CONDITIONS FOR DATA PROCESSING

PERSONAL

Article 186.

The processing of personal data is subject to a prior declaration to the Data Protection Authority.

The declaration is made by the data controller or his representative.

The declaration includes a commitment that the processing meets the requirements of this ordinance-law.

The Data Protection Authority issues a receipt in response to the declaration, where applicable if necessary by electronic means. The applicant implements the processing upon receipt of its receipt; he is not exempt from any of his responsibilities.

Processing carried out by the same body and having identical or related purposes they may be the subject of a single declaration. The information required under the declarations are provided for each of the treatments only to the extent that they are clean.

The conditions and procedure for the declaration are set by the Data Protection Authority. data.

Article 187.

Are subject to prior authorization from the Data Protection Authority before any implementation:

1. the processing of personal data relating to data genetics, medical and scientific research in these areas;
2. the processing of personal data relating to data relating to offences, convictions or security measures issued by the courts;
3. processing relating to a national identification number or any other identifier of the same nature, in particular telephone numbers;
4. the processing of personal data including biometric data;
5. the processing of personal data for reasons of public interest, in particular for historical, statistical or scientific purposes;
6. the intended transfer of personal data to a country tiers.

The request for authorization is submitted by the data controller or his representative.

The authorization does not exempt from liability towards third parties. The conditions and the authorization procedure are set by the Data Protection Authority.

Article 188.

The declaration and authorization requests contain:

1. the identity or business name, the full address of the data controller or, if the latter is not established in the territory of the Democratic Republic of Congo, the contact details of his duly authorized representative;
2. the purpose(s) of the processing and a general description of its functions;
3. the envisaged interconnections or any other forms of connection with other processing;
4. the personal data processed, their origin and the categories of persons concerned by the processing;
5. the service(s) responsible for implementing the processing as well as the categories of persons who, by reason of their functions or for the needs of the service, have direct access to the recorded data;
6. the recipients or categories of recipients authorized to receive the communication of the data;
7. the function of the person or service to whom the right of access is exercised ;
8. the measures taken to ensure the security of processing and data, the guarantees of which surround communication to third parties;
9. the indication of the use of a subcontractor;
10. the transfers of personal data envisaged to a Third State, subject to reciprocity;

11. the commitment that the treatments comply with the provisions of this title.

The Data Protection Authority defines other information that must be contained in requests for declaration and authorization.

Article 189.

The following are exempt from prior declaration formalities:

1. the processing of data used by a natural person exclusively for his or her personal, domestic or family activities;
2. the processing of data concerning a natural person the publication of which is prescribed by a legal or regulatory provision;
3. the processing of data for the sole purpose of maintaining a register which is intended for exclusively private use;
4. processing for which the controller has appointed a data protection officer responsible for ensuring, in an independent manner, compliance with the obligations provided for in this Title, except where a transfer of personal data to a third country is envisaged;

5. the processing of personal data implemented by the public or private organizations and companies for the maintenance of their general accounting;
6. the processing of personal data implemented by public or private bodies and companies relating to the management of their staff's remuneration;

7. the processing of personal data implemented by public or private bodies for the management of their suppliers;
8. the processing implemented by an association or any non-profit organization of a religious, philosophical, political or trade union nature provided that this data corresponds to the purpose of this association or organization, that it only concerns its members and that it must not be communicated to third parties.

Article 190.

The Data Protection Authority shall rule within thirty (30) days from of receipt of the request for declaration or authorization.

However, this period may be extended once, by thirty (30) days upon reasoned decision of the Data Protection Authority.

If the declaration or authorization requested from the Data Protection Authority is not delivered within the prescribed period, the silence of the Data Protection Authority constitutes acceptance.

In the event of refusal by the Data Protection Authority, the data controller is granted processing the right of appeal within fifteen days from notification of the decision of refusal.

Article 191.

The request for declaration or authorization can be addressed to the Data Protection Authority data by electronic means, by post or by any other means against delivery of a acknowledgement of receipt by the said Authority.

CHAPTER III: PROCESSING OF PERSONAL DATA

Article 192.

The processing of personal data is lawful only to the extent that the person concerned has consented to the processing of his or her personal data or if the processing is necessary for the performance of a legal obligation to which the controller is submitted.

The processing of personal data is carried out within the framework of respect for human dignity, of privacy and public freedoms.

The processing of personal data, whatever its origin or form, must not infringe the rights of persons protected by the laws and regulations in force and it is, in any case, it is prohibited to use this data to harm people or their reputation.

Article 193.

Personal data are:

1. processed lawfully, fairly and transparently:

- the person concerned gives his or her prior consent, If the person concerned is incapable, consent is governed by the principle of common law;

- data collection is carried out for specific, explicit and legitimate;
- the data collected are not further processed in a incompatible with the purposes referred to in the preceding point, taking into account all relevant factors, in particular the reasonable expectations of the person concerned and the applicable legal and regulatory provisions.
- the principle of transparency implies mandatory, clear and intelligible information from the data controller concerning personal data.

2. treated confidentially and protected, in particular when the processing involves transmissions of data over a network;
3. kept in a form that allows the identification of individuals concerned for a period not exceeding that necessary to achieve the purposes for which they are collected or for which they are processed. Personal data may be kept for longer periods to the extent that they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, provided that the appropriate technical and organizational measures required by the provisions of this Title are implemented in order to guarantee the rights and freedoms of the person concerned, subject to the provisions of Law No. 78-013 of July 11, 1978 on the general regime of archives;

4. processed in a manner that ensures appropriate security, including the protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Article 194.

The personal data collected must be reliable, adequate, relevant,

accurate, honest and not excessive.

All appropriate measures must be taken to ensure that inaccurate or

incomplete, with regard to the purposes for which they are collected or for which

they are processed later, either deleted or rectified.

Article 195.

The processing of personal data relating to information is prohibited

racial, ethnic, political opinions, religious or philosophical beliefs,

to refugee and stateless status, trade union membership, sexual life or more generally those relating to the state of health of the person concerned.

The prohibition on processing personal data referred to in paragraph 1 of this article does not apply in the following cases:

1. The processing of personal data relating to data which have been manifestly made public by the data subject;
2. The data subject has given his or her explicit consent to the processing of his or her personal data for one or more specific purposes, except where the legislation in force in the Democratic Republic of Congo provides that the prohibition referred to in paragraph 1 cannot be lifted by the data subject. Consent may be withdrawn at any time free of charge by the data subject;

3. The processing of personal data is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally unable to give consent;

4. The processing of personal data is necessary for reasons of public interest;

5. Processing necessary for the performance of a task carried out in the public interest or carried out by a public authority or is assigned by a public authority to the controller or to a third party to whom the data are communicated;

6. Processing carried out in execution of laws relating to public statistics;
7. Treatment necessary for the purposes of preventive medicine or life-saving medicine. work, medical diagnosis, the administration of care or treatment either to the data subject or to a relative, or the management of health services acting in the interests of the data subject and the processing is carried out under the supervision of a health professional;
8. Processing necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, for the purpose of ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices on the basis of applicable law, which provides for appropriate and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

9. Processing necessary for the achievement of a purpose determined by or under the provisions of this Book, for the application of social security;
10. Processing necessary for the performance of a contract to which the individual concerned is a party or to the execution of pre-contractual measures taken at the request of the latter during the pre-contractual period;
11. Processing necessary for compliance with a legal or regulatory obligation to which the controller is subject;
12. Processing necessary for the performance of specific obligations and rights of the controller under employment law;

13. Processing carried out by associations with legal personality or by public utility institutions whose main corporate purpose is the defence and promotion of human rights and fundamental freedoms, with a view to achieving this purpose, provided that such processing is authorised by the Data Protection Authority and that the data is not communicated to third parties without the written consent of the persons concerned, whether on paper, electronic media or any other equivalent medium;

14. Processing carried out in the context of legitimate activities and with appropriate guarantees of a foundation, association or any other non-profit organization with a political, philosophical, religious, mutual or trade union purpose. However, the processing must relate exclusively to members or former members of this organization or to persons maintaining regular contact with it related to its objectives and purpose, and the data must not be communicated to an external third party without the consent of the persons concerned;
15. Processing necessary for archiving purposes, in the public interest, for scientific or historical research purposes or for statistical purposes.

The personal data referred to in paragraph 1 are processed for the purposes provided for in paragraph 2, point 8, if these data are processed by a healthcare professional subject to to an obligation of professional secrecy in accordance with the law in the Democratic Republic of the Congo or to the rules established by the competent national bodies, or under its responsibility, or by another person also subject to an obligation of secrecy in accordance with the rights in force in the Democratic Republic of Congo or the rules determined by the competent national bodies.

Article 196.

In cases where processing is based on consent, the controller is in measure to demonstrate that the data subject has given consent to the processing of personal data concerning her.

In case the consent of the person concerned is given within the framework of a declaration written which also concerns other questions, the form on the request for consent is completed in a form that clearly distinguishes it from these other matters, understandable and easily accessible manner, and formulated in clear and simple terms.

No part of this statement that constitutes a violation of this Book is binding.

The data subject has the right to withdraw consent at any time, through the same means used to give it. Withdrawal of consent does not compromise the lawfulness of processing based on consent made before its withdrawal. The data subject in is informed before giving consent. It should be as easy to withdraw as it is to give consent.

When determining whether consent is freely given, it is important to take into account the following: taking into account, among other things, whether the performance of a contract, including the provision of a service, is subject to consent to the processing of data at personal data which is not necessary for the performance of the said contract.

CHAPTER IV: TRANSMISSION AND TRANSFER OF DATA PERSONAL

Section 1: Transmission of personal data

Article 197.

The transmission of personal data is lawful and legal. It is done between the managers of private law and/or public law processing.

Article 198.

The data controller transmits to one or more other data controllers personal data for prospecting purposes or any other lawful and legal need with the consent of the person concerned.

The data controller who transmits ensures that the data communicated does not are altered by anything.

It ensures the identity and quality of the data controller or his representative who receives the data.

The data controller who receives the data is required to use it only for reasons for which they were communicated to him.

A confidentiality agreement is concluded between the two data controllers.

Article 199.

For reasons of judicial investigation, the Public Prosecutor or the judge sends a requisition information or a request to the data controller for the purpose of communicating the personal data that it requires. The latter informs the Data Protection Authority data. After having ensured the authenticity and regularity of the request or the requisition, the data controller provides a response within a time limit which cannot exceed two days.

However, in the event that it is unable to respond to the request or requisition of the authority, the data controller informs the author of the request or the requisition the day after the deadline set in paragraph 2 and takes all measures to do so respond within a period which may not exceed eight (8) days.

For reasons of judicial investigation and national security, the Data Protection Authority data formulates a correspondence to the data controller so that it is transmitted all the necessary information.

Article 200.

When communicating personal data, this operation involves including the identity of the person responsible who transmitted the data to the partner and/or sub-processing, the rights of the data subject and in particular his right to object to the prospecting.

Section 2: Transfer of personal data

Article 201.

Personal data is stored and/or hosted in the Democratic Republic of Congo.

However, for digital sovereignty and security purposes, personal data Personal data may be transferred to a digital embassy, a host located in a third State or an international organisation when the Data Protection Authority finds that the State or International Organisation in question ensures a level of protection adequate and sufficient to that established by the provisions of this Book.

The equivalent and sufficient nature of the level of protection is assessed in the light of all the circumstances relating to a transfer of data. In order to determine this equivalent character and sufficient, account is taken in particular of:

1. The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, as well as the effective and enforceable rights enjoyed by data subjects and the administrative and judicial remedies that data subjects whose personal data are transferred may actually pursue.
2. The existence and effective functioning of one or more independent supervisory authorities in the third country, or to which an international organisation is subject, responsible for ensuring compliance with data protection rules and enforcing them, including through appropriate enforcement powers, and for assisting and advising data subjects in exercising their rights.

3. International commitments made by the third country or organisation international agreement in question, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, with regard to the protection of personal data.

Before any actual transfer of personal data to a third State or a international organization, the data controller must first obtain the authorization of the Personal Data Protection Authority. The transfer of personal data to third States or an international organization is subject to regular monitoring by the Personal Data Protection Authority.

Article 202.

The transfer of personal data to a third State or an international organisation not ensuring an adequate level of protection, is carried out in one of the following cases:

1. The data subject has expressly given his or her consent to the intended transfer after having been informed of the risks that such transfer may entail for him or her, in particular the lack of an adequate level of protection;
2. The transfer is necessary for the performance of a contract between the individual concerned and the controller or of the measures prior to the conclusion of this contract, taken at the request of the person concerned;
3. The transfer is necessary for the conclusion or performance of a contract concluded or to be concluded, in the interest of the data subject, between the controller and another natural or legal person;

4. The transfer is necessary or legally required for the safeguarding an important public interest, or for the establishment, exercise or defense of a legal right.
5. The transfer is necessary to protect the vital interests of the individual concerned or other persons where the concerned person is physically or legally incapable of giving consent.
6. The transfer takes place from a public register which, by virtue of legislative or regulatory provisions, is intended for the information of the public and is open to consultation by the public or any person justifying a legitimate interest, to the extent that the legal conditions for consultation are met in the particular case.

Points 1, 2 and 3 of this paragraph are not applicable to the activities of the authorities public in the exercise of their public authority prerogatives.

Without prejudice to the provisions of this article, the Council of Ministers may, after consulting compliant with the Data Protection Authority, authorize a transfer or a set of transfers of personal data to a third State or an organization international law ensuring an adequate and sufficient level of protection, when the person responsible for the processing provides sufficient guarantees with regard to the protection of privacy and fundamental rights and freedoms of individuals, as well as with regard to the exercise of rights correspondents.

CHAPTER V: PERSONAL DATA SUBJECT TO REGIMES INDIVIDUALS

Article 203.

The processing of personal data relating to offences, criminal convictions and to related security measures is prohibited. It can be implemented by:

1. public and/or judicial authorities, legal entities managing a public service within the framework of their legal attributions, in particular their judicial or administrative police missions;

2. legal assistants, for the strict needs of carrying out the missions assigned to them are entrusted by legal and regulatory provisions, in particular by lawyers or other legal advisers, insofar as the defense of their clients requires it;
3. other persons where processing is necessary for the achievement of purposes established by or under a legal or regulatory provision;
4. natural persons or legal entities under public or private law, provided that the management of their own disputes so requires.

The complete register of criminal convictions can only be kept under the control of the Data Protection Authority.

The persons concerned who may process personal data relating to Criminal convictions and related security measures are subject to secrecy professional.

Article 204.

Further processing of personal data for historical, statistical or scientists is forbidden.

The prohibition on processing personal data referred to in paragraph 1 does not apply not in the following cases:

1. the objective of the research cannot reasonably be achieved without these information is provided in a form that allows the individual to be identified;
2. the information is disclosed on the condition that it will not be used for the purpose of: contact someone to participate in a study;
3. the registered link does not cause harm to the data subject and the benefits arising from the registered link are clearly in the public interest;
4. the relevant data controller has approved all conditions relating to security and confidentiality, the removal or destruction of individual identifiers as soon as possible, the prohibition of any further use or disclosure of this information in a form that allows individuals to be identified without the express permission of the data controller;

5. the person to whom this information is communicated has signed a contract committing him to comply with the approved conditions, the provisions of this Book, the policies and procedures of the data controller relating to the confidentiality of personal information.

Further processing of personal data for historical, statistical or scientific research carried out using anonymous data is permitted.

Article 205.

In the event that the purposes for which personal data are processed do not impose not or no longer require the controller to identify a data subject, the latter is not required to retain, obtain or process additional information

to identify the data subject for the sole purpose of complying with the provisions of this title.

Where, in the cases referred to in paragraph 1 of this Article, the data controller is even to demonstrate that he is not able to identify the person concerned, he informs the person concerned, if possible. In such cases, Articles 224, 225, 226 and 227 are not applicable applicable, except where the data subject provides, for the purposes of exercising the rights that he provide these articles with additional information that allows it to be identified.

Article 206.

When processing personal data referred to in the articles of Chapter V of the this Title, the controller must take the following additional measures:

1. the categories of persons having access to personal data must be designated by the data controller or, where applicable, by the processor, with a precise description of their function in relation to the processing of the data concerned;
2. the list of categories of persons so designated must be kept at the disposal of the Data Protection Authority by the controller or, where applicable, by the processor;
3. he must ensure that the persons designated are required, by a legal or statutory obligation, or by an equivalent contractual provision, to respect the confidential nature of the data concerned;
4. when the information, due under this ordinance-law, is communicated to the person concerned or during the declaration, the data controller must mention the legal or regulatory basis authorizing the processing of personal data referred to in the articles of Chapter V of this Title.

Article 207.

Where the processing of personal data is exclusively permitted by consent written whether on paper, electronic media or any other equivalent medium, of the person concerned, the data controller must first communicate, to the person concerned, in addition to the information under the provisions of this book, the reasons for which these data are processed, as well as the list of categories of persons having access to personal data.

Article 208.

The controller or processor shall inform the data subject of the
possibility of defining the terms of management of personal data after death.

For this purpose, the person concerned indicates the terms and conditions relating to the conservation,
erasure, communication and, if applicable, transmission to a person of his choice.

The person concerned formulates either general directives which concern the whole
of his personal data or the special instructions which do not concern
that part of their personal data.

In the absence of instructions from the person concerned, the heirs of the person
concerned may at any time initiate the process of having their rights communicated to them.
related and, where applicable, to have data concerning the deceased transmitted to them,
in accordance with the relevant legislation.

CHAPTER VI: RIGHTS OF THE PERSON CONCERNED, OBLIGATIONS AND CONTROL OF THE DATA CONTROLLER, OF THE SUBCONTRACTOR AND THEIR AGENT IN DATA PROCESSING PERSONAL

Section 1: Rights of the data subject

Article 209.

The natural person whose personal data is processed may
ask the person responsible for this processing:

1. information allowing you to know and contest the processing of your personal data;
2. confirmation as to whether or not personal data concerning him/her are being processed, as well as information on:
    - the purposes of the processing;
    - the categories of data to which it relates and the categories of recipients to whom the data are communicated;
    - the recipients or categories of recipients to whom the personal data have been or will be communicated, where possible;
    - the existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the

underlying logic, as well as the significance and envisaged consequences of such processing for the data subject;

3. the communication in intelligible form of personal data concerning him/her as well as any available information as to the origin of these data;

4. where applicable, information relating to the transfers of personal data envisaged to a third State, after consultation with the Data Protection Authority;

5. where possible, the duration of retention of personal data envisaged personnel or, where this is not possible, the criteria used to determine this duration;
6. the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;

7. the right to lodge a complaint with the competent Authority;
8. any available information as to their source, when the data to personal data are not collected from the data subject.

Article 210.

In the case provided for in the preceding article, a copy of the information is communicated to him at later than sixty days of receipt of the request.

Payment of fees for any additional copies requested by the data subject must be fixed by service note from the structure responsible for processing on the basis of the significant administrative costs.

However, the Data Protection Authority, when contacted contradictorily by the controller of the file can grant it:

1. response times;
2. authorization to disregard certain requests which are clearly abusive due to their number, repetitive or systematic nature.

Where data relating to the health of the data subject are processed for the purposes of medical-scientific research, that it is clear that there is no risk that it will be carried invasion of that person's privacy and that the data is not used to take measures in respect of an individual data subject, the communication may, for

as long as it is likely to seriously harm the said research, be postponed as soon as possible late until the completion of the research. In this case, the person concerned gives prior written authorization to the data controller that the personal data personal data concerning her may be processed for medical-scientific purposes and the communication of this data may therefore be delayed.

Article 211.

Data subjects have the right to receive personal data concerning which they have provided to a data controller, in a structured format, commonly used and readable by a digital medium or other readable format, and have the right to transmit this data to another data controller without the data controller processing to which the personal data have been communicated prevents it, when :

1. the processing is based on consent or on a contract;
2. the processing is carried out using automated processes.

Where the data subject exercises his or her right to data portability pursuant to the first paragraph of this article, it has the right to obtain that the personal data personal data are transmitted directly from one data controller to another, when This is technically possible.

This right does not apply to processing necessary for the performance of a task carried out in the interest of public or relating to the exercise of public authority vested in the person responsible for the treatment.

The right referred to in paragraph 1 of this Article does not affect the rights and freedoms of third parties.

Article 212.

The person proving his identity has the right to contact the Data Protection Authority. data in order to know whether the different treatments carried out by the organs or services competent, relate to personal information concerning it and, where applicable, to get communication.

Article 213.

The natural person has the right to object, at any time, for legitimate reasons, to this that personal data concerning her be processed. She has the right, on the one hand, to be informed before data concerning them is used for first time communicated to third parties or used on behalf of third parties for purposes of exploitation, in particular commercial, charitable or political, and, on the other hand, to see themselves expressly offer the right to object, free of charge, to said communication or use.

This right must be explicitly offered to the person concerned in an intelligible and must be clearly distinguishable from other information.

Where an objection is upheld in accordance with this Article, the person responsible for the processing no longer uses or processes the personal data concerned.

To exercise his right of opposition, the interested party sends a dated and signed request, by postal or electronic, to the data controller or his representative. The data controller processing must communicate within thirty (30) days following receipt of the request provided for in the preceding paragraph, what follow-up he gave to the request of the person concerned.

When personal data is collected in writing, either on paper, on a medium digital from the person concerned, the data controller asks the person concerned, on the document through which it collects its data, if it wishes to exercise the right d'opposition.

In the event of a dispute, the burden of proof lies with the data controller. from which the right of access is exercised except when it is established that the contested data has been communicated by the person concerned or with his/her consent.

When personal data is collected from the data subject, otherwise than in writing, the data controller shall ask the latter whether it wishes exercise the right of opposition, either on a document that he communicates to him for this purpose at the latest no later than sixty (60) days after the collection of the personal data, or by any technical means which makes it possible to preserve proof that the person concerned had the possibility of exercising his right.

Article 214.

The natural person may require the data controller to, depending on the case, and as soon as possible, updated or locked personal data concerning, which are inaccurate, incomplete, ambiguous, outdated, irrelevant or whose collection, use, communication or conservation is prohibited. To exercise your right for rectification or deletion, the interested party sends a request, by post, by electronically or by bearer, dated and signed to the data controller or his representative.

Within thirty (30) days following receipt of the request provided for in the preceding paragraph, the data controller communicates the rectifications or deletions of the data made to the data subject himself/herself as well as to the persons to whom the data inaccurate, incomplete, ambiguous, outdated, irrelevant or the collection of which, use, communication or conservation is prohibited, have been communicated. When the data controller is not aware of the recipients of the communication and that notification to these recipients does not appear possible or involves efforts disproportionate, he notifies them within the time limit.

In the event of non-compliance with the deadline provided for in the preceding paragraph, a complaint shall be sent to the authority responsible for the protection of personal data by the author of the request.

In the event that information has been transmitted to a third party, its rectification or cancellation is notified to this third party, unless an exemption is granted by the authority responsible for the protection of personal data.

The beneficiaries of a deceased person who can prove their identity may, if the elements brought to their attention knowledge leads them to assume that personal data concerning them subject to processing have not been updated, require the controller of this processing that it takes into consideration the death and makes the necessary updates. consequence.

When the rights holders so request, the data controller shall provide justification, free of charge for the applicant, that he has carried out the operations required under the preceding paragraph.

Article 215.

The data subject has the right to obtain from the controller the erasure, within a period of thirty (30) days, personal data concerning him. The person responsible for the processing has an obligation to erase them when one of the following grounds applies:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2. to comply with a legal obligation to which the controller is subject submitted;
3. to carry out a task carried out in the public interest or in the exercise of official authority vested in the controller;
4. the personal data have been unlawfully processed;
5. the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing.

Article 216.

Where the controller has made public the personal data of the person concerned, it takes all appropriate measures, including measures techniques, with regard to data published under its responsibility, with a view to informing third parties who process the said data that a data subject requests them to erase all link to such personal data, or any copy or reproduction thereof.

Where the controller has authorised a third party to publish personal data personnel of the person concerned, he is deemed responsible for this publication and takes all appropriate measures to implement the right to digital oblivion and to the erasure of personal data.

The data controller shall put in place appropriate mechanisms ensuring the implementation work to respect the right to digital oblivion and the erasure of personal data personal or periodically reviews the need to retain such data, in accordance with to the provisions of this Title.

When the erasure is carried out, the controller does not carry out any other processing of such personal data. Paragraphs 1, 2, 3 and 4 above do not do not apply to the extent that such processing is necessary:

1. to the exercise of the right to freedom of expression and information;
2. compliance with a legal obligation which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
3. for reasons of public interest in the area of public health;
4. for archival purposes in the public interest, for research purposes scientific or historical or statistical purposes to the extent that the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of said processing;
5. to the establishment, exercise or defense of legal rights.

Article 217.

The Data Protection Authority adopts, without prejudice to the provisions of this Book, measures or guidelines for the purpose of specifying:

1. the conditions for deleting links to personal data personal, copies or reproductions thereof existing in publicly available electronic communications services;
2. the conditions and criteria applicable to the restriction of the processing of personal data.

Article 218.

With regard to processing relating to state security, defence and security public, the request is addressed to the Data Protection Authority which designates one of its members to carry out all useful investigations and make any modifications necessary. The latter may be assisted by another member of the said authority. The Authority of Data Protection forwards the verification report to the requesting services that it has been carried out the checks.

Where the Data Protection Authority finds, in agreement with the data controller, processing, that the communication of the data contained therein does not call into question the purposes, state security, defense or public safety, this data may be communicated to the applicant.

Where the processing is likely to include information the communication of which does not call into question the purposes assigned to it, the Data Protection Authority provides that this information is communicated to the applicant by the file manager directly seized within thirty days of receipt of the request.

Section 2: Obligations of those responsible for processing personal data

Article 219.

The data controller or his representative is required in particular to:

1. Keep up to date any inaccurate, incomplete or irrelevant data, as well as any data obtained or processed in breach of the provisions of this Book;

2. Ensure that, for persons acting under his authority, access to data and processing possibilities are limited to what these persons need for the exercise of their functions or to what is necessary for the requirements of the service;
3. Inform persons acting under his authority of the provisions of this Book and its implementing measures, as well as any relevant provisions relating to the protection of privacy with regard to the processing of personal data;
4. Ensure the compliance of software used for automated processing of personal data with the terms of the declaration referred to in Article 186 and the regularity of their application;
5. Implement all appropriate technical and organisational measures to ensure the protection of the data it processes against accidental or unlawful destruction, accidental loss, alteration, dissemination or unauthorised access, in particular when the processing involves data transmissions over a network, as well as against any other form of unlawful processing;

6. Provide training to agents who deal with the daily processing of personal data;

7. Prevent any unauthorized person from accessing the facilities used for data processing;
8. Prevent data carriers from being read, copied, modified or moved by an unauthorized person;
9. Prevent unauthorized entry of any data into the system computer science, as well as any unauthorized knowledge, modification or deletion of recorded data;
10. Prevent data processing systems from being used for money laundering and terrorist financing;
11. Prevent data from being read, copied, modified, altered or deleted in an unauthorized manner during data communication and the transport of data carriers;

12. Ensure that when using an automated data processing system, data, authorized persons can only access data relevant to their authorization;

13. Ensure that the identity of third parties to whom data may be transmitted via transmission facilities is verified and confirmed;
14. Ensure that the identity of the persons who have had access to the computer system containing personal data, the nature of the data that have been entered, modified, altered, copied, deleted or read in the system, and the time at which these data were manipulated are verified and established retrospectively;

15. Back up data by creating protected backup copies.

Article 220.

The data controller or his representative must provide the person whose data are subject to processing, at the latest, upon collection and whatever the means and media used, including the following information:

1. Identity and contact details of the controller or data controller data protection and, where applicable, the representative of the controller;

2. The specific purposes of the processing for which the data are intended when the processing is based on legitimate interests pursued by the controller or by a third party;
3. The categories of data concerned;
4. The recipients to whom the data may be communicated;
5. The ability to request to no longer appear on the file;
6. The existence of a right to object, upon request and free of charge, to the processing of personal data concerning her envisaged for prospecting purposes, in particular commercial, charitable or political;
7. The mandatory or optional nature of the response, the regulatory or contractual nature and the possible consequences of a failure to respond;
8. The existence of a right of access to information and data concerning him/her and request to update their data;
9. Where processing is based on the existence of the right to withdraw consent, consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
10. The right to lodge a complaint with the Authority;
11. The duration of data retention;
12. The existence of automated decision-making, including profiling and, in such cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject;
13. the possibility of any transfer of data to third countries.

Article 221.

The data controller implements the necessary means to guarantee security personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, backup and restoration. He is also civilly liable for the employees processing this data.

It also implements all appropriate means to ensure that, by default, only the personal data necessary for each specific purpose of the treatment are processed.

Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers of the processing. The controllers processing partners transparently define their respective obligations in order to to ensure compliance with the requirements of this ordinance-law, in particular with regard to concerns the exercise of the rights of the data subject, and their respective obligations by by agreement between them. A contact point for the persons concerned may be designated in this agreement.

The agreement referred to in paragraph 3 shall duly reflect the respective roles of the joint managers of the processing and their relations with data subjects. The main points of the agreement are made available to the person concerned.

Irrespective of the terms of the agreement referred to in paragraph 1, the data subject may exercise the rights conferred on him by this ordinance-law with respect to and against each of the data controllers.

Article 222.

The data controller appoints a data protection officer personnel to ensure that processing is not likely to harm the rights and freedoms of the persons concerned. The delegate is responsible in particular for:

1. Ensure, in an independent manner, the internal application of the provisions of this ordinance-law;
2. Keep a record of the processing carried out by the data controller, containing the information referred to in Article 168 of this Ordinance-Law.

Article 223.

Personal data is processed and stored confidentially and protected,

particularly when the processing involves data transmissions over a network.

Article 224.

Where processing is entrusted to a processor, the controller or, where applicable

where applicable, its representative in the Democratic Republic of Congo:

1. Ensures that the selected subcontractor meets all required conditions by the law in force on subcontracting;
2. Ensures that the selected subcontractor provides sufficient guarantees with regard to security, ethical and organizational measures relating to processing as well as technical and operational measures in accordance with the laws in force, in particular for the implementation of security and confidentiality measures, so that the processing meets the requirements of this Book and guarantees the protection of the rights of the persons concerned.
3. Ensures compliance with the measures in point 1 above, in particular by: stipulation of specific mentions in contracts entered into with subcontractors;
4. Sets out in the contract the subcontractor's liability to the data controller and the subcontractor's obligations regarding the protection of data security and confidentiality;
5. Agrees with the subcontractor that the latter acts only on the sole instructions of the controller and is bound by the same obligations as those to which the controller is bound;
6. Record in writing or on electronic media the elements of the contract referred to in this article.

Article 225.

The data controller shall ensure and assist the data protection officer in

associated, appropriately and in a timely manner, with all matters relating to the protection

personal data and carries out the tasks assigned to it.

The data controller shall ensure that the data protection officer receives

no instructions regarding the exercise of its missions.

The data protection officer may not be relieved of his duties or penalized by the

controller or processor for the exercise of its duties. The data controller

Data Protection reports directly to the highest level of management of the
controller or processor.

Data subjects may contact the Data Protection Officer.
on all matters relating to the processing of their personal data
and to the exercise of the rights conferred on them by the provisions of this Book.

The data protection officer is subject to professional secrecy with regard to
the exercise of its missions.

The Data Protection Officer performs other tasks and duties. The Data Protection Officer
processing or the subcontractor ensures that these missions and tasks do not give rise to a conflict
of interest.

Article 226.

The duties of the data protection officer are as follows:

1. Inform and advise the controller or processor and employees carrying out the processing of their obligations under the provisions of this Book on data protection.

2. Monitor compliance with the provisions of this Book on data protection and the internal rules of the controller or processor on the protection of personal data, including with regard to the allocation of responsibilities, awareness-raising and training of personnel involved in processing operations, and related audits;

3. Provide advice, upon request, regarding the data protection impact assessment and verify its execution in accordance with the provisions of this Book;

4. Cooperate with the authority responsible for the protection of personal data personnel ;
5. Act as a focal point for the authority responsible for the protection of personal data on matters relating to processing, including prior consultation in accordance with the provisions of this Book, and conduct consultations, where appropriate, on any other matter.

The data protection officer takes into account, in carrying out his duties,
of the risk associated with the processing operations taking into account the nature, scope,
context and purposes of the processing.

Article 227.

The controller shall keep a record of the processing activities carried out under their responsibility. This register contains all of the following information:

1. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.
2. The purposes of the processing.
3. A description of the categories of persons concerned and the categories of personal data.
4. The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations.
5. Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation.
6. The deadlines provided for the erasure of the different categories of data.
7. A general description of technical and organizational security measures.

Article 228.

The data controller and, where applicable, his representative, shall make the register available to the provision of the Data Protection Authority.

The obligations to keep a register and appoint a delegate do not apply to small and medium-sized enterprises as well as start-ups, unless the processing they carry out is likely to pose a risk to the rights and freedoms of the persons concerned, if it is not occasional or if it relates in particular to special categories of data or on personal data relating to criminal convictions.

Section 3: Obligations of the subcontractor

Article 229.

The subcontractor is required to process the data only within the limits of the contract which binds it with the Data Controller.

Processing by a processor is governed by a contract between the processor and the controller. of the processing, defines the object and duration of the processing, the nature and purpose of the processing, the

type of personal data and the categories of persons concerned, and the obligations and rights of the controller.

This contract provides, in particular, that the subcontractor:

- only processes personal data on documented instructions from the controller, including with regard to transfers of personal data to a third country or to an international organisation;

- ensures that persons authorised to process personal data staff undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality;
- takes into account the nature of the processing, assists the controller, by appropriate technical and organisational measures, to the extent possible, in fulfilling his obligation to respond to requests made by data subjects to exercise their rights under this Title;

- assists the data controller in ensuring compliance with the obligations provided for in this Title, taking into account the nature of the processing and the information available to the processor;
- makes available to the data controller all information necessary to demonstrate compliance with the obligations under this Article and to enable audits, including inspections, to be carried out by the controller or another auditor appointed by it, and contributes to such audits.

The Subcontractor shall not recruit another Subcontractor without prior written permission, specific or general, of the data controller. In the case of written authorization general, the processor informs the controller of any planned changes regarding the addition or replacement of other subcontractors, thereby giving the controller processing the possibility of raising objections to these changes.

Article 230.

The processor shall keep a record of all categories of processing activities carried out on behalf of the data controller, including:

1. the name and contact details of the processor(s) and of each controller on whose behalf the processor acts, as well as, where applicable, the names and contact details of the representative of the controller or processor and those of the data protection officer;
2. the categories of processing carried out on behalf of each controller of the treatment;

3. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers, documentation attesting to the existence of appropriate safeguards;
4. a general description of technical and organizational security measures.

The registers can be in materialized or dematerialized form.

Article 231.

The subcontractor or its representative, where applicable, makes the register available to the Personal Data Protection Authority upon request.

The obligations to keep a register and appoint a delegate do not apply to small, medium-sized enterprises and start-ups unless the processing they carry out is likely to pose a risk to the rights and freedoms of the persons concerned, if it is not occasional or if it relates in particular to particular categories or data to personal data relating to criminal convictions.

Article 232.

Without prejudice to Book III, trust service providers referred to in the aforementioned Book are subject to the personal data protection requirements provided for by the provisions of this book.

Section 4: Obligations of the agent

Article 233.

The person having access to personal data and acting under the authority and control of the data controller, is required to follow the latter's instructions for process personal data.

Section 5: Control of the processing of personal data

Article 234.

Control of the processing of personal data carried out by a data controller processing or its delegate, the subcontractor as well as the administrative sanctions for their non-

compliance with this Book, are the exclusive responsibility of the Data Protection Authority.
personal data.

This prerogative cannot be delegated to a third party body, unless the body fulfils the
conditions below:

1. demonstrates, to the satisfaction of the data protection authority, that:
   staff, its independence and its expertise;
2. establishes procedures enabling it to assess whether those responsible for the
   processing and the subcontractors concerned meet the conditions for monitoring compliance
   with the provisions and periodically reviewing its operation;
3. establishes procedures and structures to handle complaints about breaches by a
   controller or processor;
4. demonstrates, to the satisfaction of the authority responsible for the protection of
   personal data, that its tasks and missions do not entail a conflict of interest.

The Data Protection Authority revokes the approval of the body if the conditions
approval are no longer met or if the measures taken by the body constitute a violation
of the provisions of this Book.

Article 235.

Where personal data has not been collected from the individual
concerned, the controller or his representative provides the data subject with:
unless already informed, the following information:

1. The identity and contact details of the controller and, where applicable,
   of the data protection officer;
2. The purposes of the processing;
3. The existence of a right to object, on request and free of charge, to the
   processing of personal data concerning him/her for direct marketing
   purposes, in particular commercial, charitable or political. In this case, the data
   subject is informed before personal data are communicated to third parties
   for the first time or used on behalf of third parties for marketing purposes;

4. Other additional information as follows:

   • The categories of data concerned;
   • The recipients or categories of recipients;
   • The duration of data retention;

- The possibility of any transfer of data to third countries, where the processing is based on the legitimate interests pursued by the controller or by a third party;
- The existence of a right of access to data concerning them and of rectification or erasure of this data;
- The existence of the right to withdraw consent at any time, without undermine the lawfulness of processing based on consent given before its withdrawal;
- The right to lodge a complaint with the Authority;
- The source from which the personal data comes and, where applicable where applicable, a statement that they come from publicly available sources;

- The existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

The above mentioned information must be provided when registering the data or, if the communication of data to a third party is envisaged, at the latest at the time of the first communication of data.

The data controller provides the information referred to in the first paragraph:

1. within a reasonable period after obtaining the personal data, but not exceeding thirty (30) days, having regard to the particular circumstances in which the personal data are processed;
2. whether the personal data are to be used for the purposes of the communication with the data subject, at the latest at the time of the first communication to the data subject; or
3. if it is intended to communicate the information to another recipient, later when the personal data is first communicated.

When it intends to carry out further processing of personal data for a purpose other than that for which the personal data were obtained, the data controller shall provide the data subject with prior information on this other purpose and any other relevant information referred to in paragraph 1.

Article 236.

In accordance with the provisions of this Book, the data controller is exempt from provide the information when:

1. Informing the data subject proves impossible or involves disproportionate effort for processing for statistical, historical or scientific purposes or for screening motivated by the protection and promotion of public health;

2. The person concerned already has this information;
3. The recording or communication of personal data is carried out for the purpose of applying a legal or regulatory provision.

Article 237.

The controller shall take appropriate measures to provide any information required to carry out the communication, with regard to the processing of the person concerned in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms, especially for any information concerning a minor.

Information is provided in writing or by other means, including, where it is appropriate, electronically.

However, the person concerned may make a written request; in this case the information will also be provided to him in writing, provided that the identity of the person concerned is demonstrated by other means.

Article 238.

The data controller facilitates the exercise of the rights granted to the data subject. In this case, the data controller does not refuse to comply with the request of the data subject to exercise the rights conferred by this Book, unless the controller demonstrates that he is unable to identify the person concerned.

Article 239.

The controller shall provide the data subject with information on the measures taken following a request made as soon as possible and in any event in a period of thirty days from receipt of the request. If necessary, this period may be extended by sixty days, taking into account the complexity and number of requests.

The data controller shall inform the data subject of this extension and of the reasons for the postponement within thirty days of receipt of the request.

Where the data subject submits his or her request in electronic form, the information is provided electronically where possible, unless the person concerned does not request otherwise.

If the data controller does not respond to the request made by the person concerned, he informs the latter without delay and at the latest within thirty days of from receipt of the request for reasons for its inaction.

The person concerned has the possibility of lodging a complaint with the authority having responsible for the protection of personal data and to lodge an appeal jurisdictional.

Article 240.

No payment is required to provide information to proceed with any communication.

Article 241.

Without prejudice to the provisions relating to the protection of personal data, criminal convictions, and related security measures, when the person responsible for the processing has reasonable doubts as to the identity of the natural person presenting the special request, he may ask that information be provided to him additional information necessary to confirm the identity of the data subject.

Article 242.

Information to be communicated to individuals can be provided accompanied by icons standardized to provide a good overview, easily visible, understandable and

clearly legible, of the intended treatment. When the icons are presented by way electronic, they are machine readable.

Article 243.

Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, including the degree of probability and severity varies, that the processing presents for the rights and freedoms of natural persons, the data controller implements, both at the time of the determination of the means of treatment at the time of the treatment itself, measures appropriate technical and organizational measures, such as pseudonymization, which are intended to implement data protection principles, such as the data minimization, effectively and to match the processing of guarantees necessary to meet the requirements of this Book and to protect the rights of the person concerned.

The data controller implements technical and organizational measures appropriate to ensure that, by default, only personal data that are necessary in relation to each specific purpose of the processing are processed. These measures apply to the amount of personal data collected, the extent of their processing, their retention period and their accessibility. In particular, these measures ensure that, by default, personal data is not made accessible to an indefinite number of natural persons without the intervention of the natural person concerned.

Article 244.

The data controller must notify the Data Protection Authority without delay and to the data subject any personal data breach affecting the personal data of the data subject.

The subcontractor must notify the data controller without delay of any breach of the security affecting the personal data it processes on behalf of and in the name of of the data controller.

The notification referred to in paragraph 1 must, at the limit:

1. Describe the nature of the security breach affecting personal data including, where possible, the categories and approximate number of individuals affected by the breach and the categories and approximate number of personal data records affected;

2. Communicate the name and contact details of the data protection officer or other contact point from whom further information may be obtained;

3. Describe the likely consequences of the security breach;
4. Describe the measures taken or that the controller proposes to take take to address the security breach, including, where appropriate, measures to mitigate any adverse consequences.

Communication to the data subject referred to in paragraph 1 is not necessary if one or one of the following conditions is met:

1. The controller has implemented the protective measures appropriate technical and organisational measures and such measures have been applied to the personal data affected by the said breach, in particular measures which render the personal data incomprehensible to any person who is not authorised to access them, such as encryption
2. The controller has taken further measures to ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

3. It would require a disproportionate effort. In this case, a public communication or similar measure shall instead be taken to enable the persons concerned to be informed in an equally effective manner.

Article 245.

When treatment, in particular through the use of new technologies, and taking into account of the nature, scope, context and purposes of the processing, is likely to generate a high risk for the rights and freedoms of natural persons, the person responsible of the treatment carries out, before the treatment, an analysis of the impact of the operations of processing envisaged on the protection of personal data. One and the same analysis may relate to a set of similar processing operations that have similar similar high risks.

When carrying out a data protection impact assessment, the data controller
processing request advice from the data protection officer, if such a officer has been appointed
designated.

The data protection impact assessment referred to in paragraph 1 is, in particular,
required in the following cases:

1. the systematic and in-depth evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on the basis of which decisions are taken which produce legal effects concerning a natural person or similarly significantly affect him or her;

2. large-scale processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

3. large-scale processing of data relating to criminal convictions and offences;

4. systematic large-scale monitoring of an area accessible to the public.

The Data Protection Authority shall establish and publish a list of the types of operations
processing for which a data protection impact assessment is
required in accordance with paragraph 1.

It establishes and publishes a list of the types of processing operations for which no
no data protection impact assessment is required.

Article 246.

The data controller shall consult the Data Protection Authority prior to the
processing when a data protection impact assessment carried out under
of the previous article indicates that the processing would present a high risk if the controller
treatment did not take steps to mitigate the risk.

Where the Data Protection Authority is of the opinion that the intended processing referred to in
paragraph 1, would constitute a violation of the provisions of this Book, in particular when
the controller has not sufficiently identified or mitigated the risk, the Authority

data protection provided in writing, within a maximum period of eight (8) weeks to from receipt of the request for consultation, written notice to the person responsible for the processing and, where applicable, to the subcontractor, and may use its powers. This period may be extended by four weeks, depending on the complexity of the treatment envisaged.
The Data Protection Authority shall inform the controller and, where appropriate, the subcontractor of the extension of the deadline and the reasons for the delay, within a period of fifteen days from receipt of the consultation request. These deadlines may be suspended until the Data Protection Authority has obtained the information which she requested for the purposes of the consultation.

Article 247.

As regards the direct provision of information society services to minors, the processing of personal data relating to a minor is lawful only in the to the extent that consent is given by the holder of parental responsibility in respect of of the minor.

The data controller shall verify, in such cases, that consent is given or authorized by the holder of parental responsibility for the child, taking into account the available technological means.

Article 248.

In the event of incapacity of an adult within the meaning of the family code duly certified by a health care professional, the rights, as set out in the provisions of this Book, of a major person concerned, are exercised by the spouse or any person committed to the protection of the interests of this adult in accordance with the family code.

The person concerned is involved in the exercise of his rights as far as possible and given his ability to understand.

Article 249.

Without prejudice to any other administrative or legal remedy, the person concerned has the right to lodge a complaint with the Data Protection Authority, if it

considers that the processing of personal data concerning it constitutes a violation of the provisions of this Book.

The Data Protection Authority informs the author of the complaint of the status progress and outcome of the claim, including the possibility of an appeal jurisdictional under the following article.

Article 250.

The data subject has the right to an effective remedy before the courts competent administrative authority when the authority responsible for data protection personal character does not process a complaint or inform the data subject, within sixty (60) days of the progress or outcome of the claim which it introduced under the previous article.

Article 251.

The data subject has, against the data controller or its processor, right to an effective legal remedy before the peace court of its jurisdiction if it considers that the rights conferred on it by the provisions of this Book have been violated fact of processing of his personal data carried out in violation of the provisions of this book.

Article 252.

The person who has suffered material or moral damage as a result of a violation of the provisions of this Book has the right to obtain from the controller or the processor dealing with compensation for the damage suffered.

The data controller who participated in the processing is liable for the damage caused by processing which constitutes a violation of the provisions of this Book. A subcontractor is only liable for damage caused by the processing if it has not complied with the obligations provided for by the provisions of this Book which are specifically incumbent on subcontractors or if he has acted outside the lawful instructions of the controller or unlike these.

The controller or processor is exempt from liability under
paragraph 2, if he proves that the fact which caused the damage is in no way attributable to him.

Where there are several data controllers or processors or where, at the same time, one
controller and a processor participate in the same processing and, when, at
under paragraphs 2 and 3, they are liable for damage caused by the processing, each
controllers or processors are jointly and severally liable for the
damage (in its entirety) in order to guarantee the person concerned effective compensation.

Where the controller or processor has, in accordance with paragraph 4, repaired
fully compensate for the damage suffered, he is entitled to claim from the other persons responsible for the
processing or subcontractors having participated in the same processing the share of the repair
corresponding to their share of responsibility for the damage, in accordance with the conditions
fixed in paragraph 2.

Article 253.

Joint controllers shall define their obligations transparently
respective for the purposes of ensuring compliance with the requirements of this Book, in particular with regard to
concerns the exercise of the rights of the data subject, and their respective obligations regarding
to the communication of information, by agreement between them.

A point of contact for data subjects may be designated in the agreement.

The agreement referred to in paragraph 1 shall duly reflect the respective roles of the joint managers of the
processing and their relations with data subjects. The main points of the agreement
are made available to the person concerned.

Article 254.

The interconnection of personal data files allows legal objectives to be achieved
or statutory ones presenting a legitimate interest for the data controllers. It cannot
not lead to discrimination or reduction of rights, freedoms and guarantees for
persons concerned or be accompanied by inappropriate security measures and must furthermore
take into account the principle of relevance of the data being interconnected.

CHAPTER VII: ADMINISTRATIVE MEASURES

Article 255.

In particular, breaches under this Book include:

1. carry out unfair collection of personal data;
2. communicate personal data to an unauthorized third party;
3. collect sensitive data, strategic data,
   data relating to offences or a national identification number without complying with legal requirements;
4. collect or use personal data in a manner that seriously undermines the fundamental rights or privacy of the natural person concerned;
5. prevent the Data Protection Authority from carrying out an on-site inspection mission or obstruct the carrying out of such a mission.

Article 256.

The Data Protection Authority may issue a warning to the controller who fails to comply with the obligations arising from the provisions of the present Book.

It may also order the data controller to stop the processing.
failure noted within a fixed period which cannot exceed eight days.

Article 257.

Where the data controller fails to comply with the provisions relating to the implementation in default of this Book, the Data Protection Authority may pronounce on its against, in compliance with the principle of adversarial proceedings, the following sanctions:

1. payment of eight million to two hundred million Congolese francs if the violation had no serious impact on the State and/or the persons concerned;
2. payment of 5% of its annual turnover excluding tax for the past financial year, if the violation led to the death or attempted murder of one or more persons;
3. injunction to cease processing of personal data, if the violation endangered national security and safety and/or led to mass murder or genocide.

The State reserves the right to bring criminal proceedings against the data controller and claim damages against him and the persons concerned.

Article 258.

The sanction imposed by the Data Protection Authority may be accompanied by a injunction to proceed, within a period which may not exceed eight (8) days, with any modification or deletion useful in the operation of personal data processing, object of the sanction.

Article 259.

The sanctions provided for in the provisions of this Book are imposed on the basis of a report drawn up by the Data Protection Authority. This report is notified to the controller of the treatment, who may make written or oral observations within a period of fifteen (15) days from receipt of the notification from the Data Protection Authority and which may be attended or be represented at the working sessions at the end of which the Authority data protection statute.

The decisions taken by the Data Protection Authority are justified and notified to the data controller.

Article 260.

Decisions imposing a sanction may be appealed before the court. competent administrative authority.

Article 261.

The sanctions imposed are made public by the Data Protection Authority.

TITLE IV: DATA PROTECTION AUTHORITY

Article 262.

A data protection authority, called the Data Protection Authority, is hereby established. data in acronym “APD”, hereinafter referred to as “Data Protection Authority”, responsible to monitor compliance with the provisions of this Book and those relating to the protection of privacy and any foreign action affecting data or data processing public and personal data hosted in the Democratic Republic of Congo.

The Data Protection Authority is an independent administrative authority with the legal personality and enjoying administrative and financial autonomy.

A decree of the Prime Minister deliberated in the Council of Ministers, on the proposal of the Minister having digital in its attributions, establishes the organization and the functioning of the Authority data protection.

Article 263.

The Data Protection Authority is responsible for ensuring that the processing of public and personal data is implemented in accordance with the provisions of Book III of this ordinance-law.

In this capacity, the Data Protection Authority is responsible for:

1. Respond to any request for advice or recommendations relating to the processing of public and personal data;
2. Issue on its own initiative reasoned opinions or recommendations on any question relating to the application of the fundamental principles of the protection of privacy within the framework of this Book, as well as laws containing provisions relating to the protection of privacy with regard to the processing of public and personal data;
3. Inform the persons concerned and the data controllers of their rights and obligations;
4. Allow or refuse file processing in a number of cases, including sensitive files;
5. Receive the formalities prior to the creation of personal data processing and, where applicable, authorize these processing operations;
6. Receive, by post or electronically, claims, petitions and complaints relating to the implementation of the processing of personal data and inform their authors of the follow-up given to them, in particular if a further investigation or coordination with another national protection authority is necessary;
7. Carry out, without prejudice to any action before the courts, investigations, either on its own initiative or following a complaint or at the request of another National Protection Authority, and inform the person concerned, if it has submitted a complaint to it, of the outcome of its investigations within a reasonable time;
8. Inform the judicial authority without delay for certain types of offences of which it is aware;
9. Inform the Public Prosecutor without delay, in accordance with the provisions of the penal code, violations of the provisions of this Book, constituting criminal offences;

10. Inform the National Assembly, the Government or other political institutions, as well as the public, of any issue relating to the protection of public and personal data;

11. Conduct frequent consultations with stakeholders on issues that the Authority considers may undermine the effective protection of personal data for services, facilities, devices or directories under this Book;

12. Require sworn experts or agents to participate in the implementation of verification missions relating to any processing of personal data on the territory of the Democratic Republic of Congo;
13. Ensure compliance with prior authorizations and consultations;
14. Pronounce the rectification, erasure or destruction of all data when they have been processed in violation of the provisions of this Book and the notification of these measures to third parties to whom the data have been disclosed;
15. Request the controller or processor to comply with requests to exercise the rights provided for in the provisions of this Book submitted by the data subject;

16. Impose administrative and financial sanctions on data controllers;

17. Update a directory of personal data processing and make it available to the public;

18. Monitor relevant developments as they impact on the protection of public and personal data, including developments in information and communications technologies and business practices;

19. Authorize and monitor data monetization operations;
20. Inform the controller or processor of an alleged breach of the provisions governing the processing of personal data and, where appropriate, order the controller or processor to remedy the breach by specific measures, in order to improve the protection of the data subject;

21. Advise natural or legal persons who carry out processing of personal data or tests or experiments likely to result in such processing;

22. Authorise or refuse cross-border transfers of personal data to third countries;

23. Raise public awareness of the risks, rules, guarantees and rights relating to the processing of personal data. Activities specifically aimed at children, the elderly or seriously ill or anyone who may not be able to understand the scope of the activities offered to them are given special attention;

24. Make proposals for legislative or regulatory changes likely to simplify and improve the legislative and regulatory framework with regard to data processing;
25. Approve codes of conduct and collect and authorize, where appropriate, the projects, modifications or extensions of said codes;

26. Establish cooperation mechanisms with public and personal data protection authorities of third States for information sharing and mutual assistance;
27. Participate in international negotiations on the protection of public and personal data;
28. Ensure capacity building for data controllers or their delegates, subcontractors and their agents.

In order to carry out its missions, the Data Protection Authority may proceed by way of recommendations and take individual decisions in the cases provided for by the present ordinance-law.

Article 264.

The bodies of the Data Protection Authority are:

1. The Plenary Assembly;
2. The Office;
3. The Standing Committees.

The Data Protection Authority has a Technical Secretariat responsible for issues administrative, legal and financial. It has an antenna in each capital of province, each city and the territorial capital.

Article 265.

The Plenary Assembly comprises all members of the Data Protection Authority. data. It is the body of design, orientation, decision and control of the Authority. Its decisions are taken by consensus or, failing that, by majority vote.

Article 266.

The Plenary Assembly is composed of nine (9) members chosen for their skills and/or techniques as follows:

1. A person appointed by the President of the Republic;
2. Three personalities appointed by the National Assembly;
3. Two career magistrates appointed by the High Council of the Judiciary;
4. A lawyer appointed by the National Bar Association;
5. A delegate appointed by the National Human Rights Commission, CNDH for short;

6. A representative of employers' organizations from the digital ecosystem, subject to the provisions of Article 268 of this Ordinance-Law.

The appointment of members takes into account their expertise in the digital sector and national representation, as well as that of women.

Article 267.

No one may be appointed as a member of the Plenary Assembly of the Data Protection Authority. data if it does not meet the following conditions:

1. Be of Congolese nationality;
2. Enjoy his civil and political rights;
3. Hold at least a bachelor's degree or an equivalent qualification and provide proof of professional experience of 5 years or more in a field that may be of interest to the Data Protection Authority;
4. Not be in one of the cases of incompatibility referred to in Article 268 of the present ordinance-law.

Article 268.

The members of the Plenary Assembly are appointed by Order of the President of the Republic on the proposal of the Minister responsible for digital technology for a duration of 5 years, renewable once, and are subject to parliamentary control.

Members of the Plenary Assembly enjoy complete immunity for opinions issued in the exercise of their functions. They are subject to the jurisdiction of the Court of Cassation.

The quality of the members of the Plenary Assembly is incompatible with the quality of the members of the Government, of the Deputies and Senators, of the exercise of the functions of leader of companies, of holding interests in companies in the digital sector, banking or telecommunications.

Article 269.

The Office is the management and coordination body of the Data Protection Authority. It is composed of four members: a President, a Vice-President, a Rapporteur and a Deputy Rapporteur. The members of the Bureau of the Plenary Assembly are elected by their peers by a simple majority of votes.

Article 270.

The Commissions are technical bodies responsible for dealing with issues relating to the mission of the Data Protection Authority.

Each Commission is headed by a member of the plenary other than the members of the Plenary Office.

The number of commissions, their composition, organization and operation are determined by decree of the Prime Minister referred to in Article 262 of this ordinance-law.

BOOK IV: ON THE SECURITY AND CRIMINAL PROTECTION OF SYSTEMS COMPUTERS

TITLE I: PURPOSE AND SCOPE OF APPLICATION

Article 271.

The provisions of this Book set out the rules applicable to cybersecurity and the procedures to combat cybercrime.

They also establish the institutional framework, rules and procedures for using the cryptology in the Democratic Republic of Congo.

Article 272.

This Book applies to:

1. To the means of ensuring the protection and integrity of computer systems, operators of vital importance and digital data;

2. Specific offences relating to digital activities and services, as well as those committed on and by means of a computer system;
3. To offences committed in cyberspace and the effects of which occur on the national territory;
4. To the collection of electronic evidence of any offence;
5. To the institutional framework and procedural rules specific to the cybersecurity and cybercrime in the Democratic Republic of Congo.

Article 273.

The provisions of this book do not apply to:

1. To the means of encryption used by diplomatic missions and consular in accordance with regularly ratified treaties and conventions as well as those relating to internal and external security.
2. To digital applications and systems used by the specialized defense and national security services of the Democratic Republic of Congo.

TITLE II: INSTITUTIONAL FRAMEWORK

Article 274.

The institutional framework of the cybersecurity sector is the National Cybersecurity Agency, “ANCY”, in acronym.

The National Cybersecurity Agency is the national authority in charge of cybersecurity and of computer systems security in the Democratic Republic of Congo.

CHAPTER I: THE NATIONAL CYBERSECURITY AGENCY

Article 275.

The National Cybersecurity Agency is a public body with the personality legal. It falls under the authority of the President of the Republic.

An Order of the President of the Republic deliberated in the Council of Ministers fixes the organization and operation of the National Cybersecurity Agency.

As part of its missions, the National Cybersecurity Agency collaborates in particular with the Ministries responsible for the following matters:

1. interior and security;
2. national defense;
3. to justice;
4. digital;
5. posts and telecommunications;
6. human rights.

Article 276.

The Agency is the national authority in charge of Cybersecurity and systems security. computers in the Democratic Republic of Congo.

It ensures regulation in matters of Cybersecurity, compliance and auditing of systems computer systems and electronic communications networks, the approval of cybersecurity service and product providers.

The operator of a computer system, public or private, informs the National Agency of Cybersecurity from all attacks, intrusions and other penetrations that may hinder the operation of another computer system or network to enable it to take the necessary measures to deal with it, including the isolation of the computer system concerned and this until these disturbances cease.

The operator is required to comply with the measures issued by the National Agency for Cybersecurity to stop these disruptions.

Article 277.

It guides the national cybersecurity strategy and proposes the security policy for the State's IT systems.

The National Cybersecurity Agency provides its expertise and technical assistance to administrations as well as to both public and private companies, with a mission strengthened for the benefit of critical and essential infrastructures and important operators vital (OIV).

Article 278.

The National Cybersecurity Agency is responsible in particular for the following missions:

- pilot, coordinate and monitor the implementation of the National Strategy Cybersecurity;
- implement measures to prevent, protect and defend data, critical and essential infrastructures as well as electronic communications networks against the risks of cyber threats in Democratic Republic of Congo;
- drive national risk management, cyber measures resilience, cyber incident management, business continuity, cyber crisis management;

- ensure compliance of cybersecurity procedures for public bodies and institutions;
- ensure the national inclusion mechanism of the different stakeholders in the implementation of the national Cybersecurity strategy;
- identify, in collaboration with Ministries and sector regulators, vitally important organizations and essential services, and ensure that they are updated;

- monitor performance indicators in cybersecurity and security computer systems;
- establish and maintain cyber vulnerability databases;
- participate in the development of digital trust;
- ensure the audit and technological monitoring of computer systems and electronic communications networks in the Democratic Republic of Congo ;
- certify and approve Cybersecurity and cryptology products and services in the Democratic Republic of Congo;
- support and collaborate in the fight against cybercrime with other public organizations and institutions;
- collaborate and participate in awareness raising, training and investigations in cybersecurity;
- ensure the management of the Sovereign Fund;
- contribute, with regard to its missions, to the application of agreements, treaties and conventions relating to Cybersecurity and the fight against Cybercrime ratified by the Democratic Republic of Congo;
- ensure the implementation of legal and regulatory provisions relating to the security of computer systems and electronic communication networks;
- centralize requests for assistance following security incidents on the computer systems and electronic communications networks.

Article 279.

A sovereign fund for cybersecurity and computer systems, called "Sovereign Fund".

The Sovereign Fund participates in the financing of the National Cybersecurity Strategy and supports the activities of the National Cybersecurity Agency.

A Decree of the Prime Minister deliberated in the Council of Ministers, on the proposal of the Minister having digital in its attributions, defines the operating methods of the Fund sovereign and its financing.

Article 280.

Public sector IT systems are subject to an audit regime
mandatory and periodic IT security check.

Criteria relating to the nature of the audit, its frequency and the application procedures
recommendations contained in the audit report, conditions and procedures
identification of experts are set by order of the Minister responsible for digital technology
attributions. To carry out the audit referred to in this article, the National Cybersecurity Agency
and/or the Experts appointed by it to carry out said audit, have the right to consult all
databases, documents, files and folders relating to computer security in order to
to accomplish their missions.

The sworn agents of the National Cybersecurity Agency responsible for the investigation have the quality of judicial police officer with limited competence. They take an oath according to the provisions of common law applicable in this matter.

In this respect, apart from the administrative report addressed to the hierarchical authority, they address the judicial report to the relevant Public Prosecutor.

TITLE III: COMPUTER SYSTEMS SECURITY

CHAPTER 1: GENERAL AND SPECIFIC OBLIGATIONS

Section 1: General obligations

Article 281.

The natural or legal person operating and/or having knowledge in the sector of
digital is required to cooperate in the detection of cyber attacks in accordance with
legal and regulatory provisions applicable in the Democratic Republic of Congo.

Article 282.

The online service provider is required to hold and retain data of a nature to
allow the identification of anyone who has contributed to the creation of the content or one of the contents of the services they provide.

It is also required to provide persons who publish a communication service to public online guarantees allowing them to meet the identification conditions provided for by this ordinance-law.

The Public Prosecutor or the Data Protection Authority may request from online service providers, in accordance with the relevant law, the conservation and the protection of the integrity and the communication of the data mentioned in paragraph 1 of the this article.

Article 283.

The online service provider is not responsible for the content of the information they transmit and to which they give access if it satisfies the following conditions:

1. not be the originator of the transmission;
2. not selecting the recipient of the transmission;
3. not to modify the information being transmitted;
4. inform their subscribers of the existence of technical means enabling them to restrict access to certain services or to select them and offer at least one of these means.

The internet access provider and the online service provider referred to in paragraph 1 include in particular the automatic, intermediate and transient storage of information transmitted, provided that this storage serves exclusively for the execution of the transmission over the communications network and that its duration does not exceed the time necessary to the transmission.

Article 284.

The Internet access provider and the online service provider do not commit their civil and/or criminal liability arising from the activities or information stored at the request from a recipient of their services, if they were not actually aware of their illicit nature or of facts and circumstances revealing this nature or if, from the when they became aware of it, they acted promptly to remove this data or make access impossible.

The preceding paragraph does not apply when the recipient of the service acts under the authority or control of the online service provider.

Article 285.

Knowledge of the disputed facts is presumed to have been acquired by the service provider in line, when notified of one of the following:

1. the date of the notification;
2. if the notifier is a natural person: his/her first name, last name, post-name, profession, address, nationality, date and place of birth;
3. if the notifier is a legal person: its legal form, its corporate name and its registered office as well as the body which legally represents it;
4. the name and address of the recipient or, if it is a legal entity, its business name and registered office;
5. the description of the disputed facts and, if possible, their precise location;
6. the reasons why the content should be removed, including a reference to the legal provisions and factual justifications;
7. a copy of the correspondence addressed to the author or publisher of the disputed information or activities requesting their interruption, withdrawal or modification, or justification that the author or publisher could not be contacted.

Article 286.

The Internet access provider and the online service provider are not subject to the obligation to monitor the information they transmit or store, nor the obligation to to seek facts or circumstances revealing illicit activities unless, in a manner temporary, this obligation is made at the request of the Public Prosecutor, the National Cybersecurity Agency, security and public order services.

Article 287.

The Internet service provider and the online service provider compete in the fight against the offences provided for in this ordinance-law.

To this end, they are setting up an easily accessible and visible system allowing anyone person to bring to their attention the facts constituting these offences.

They are also required, on the one hand, to promptly inform the competent authorities of any illicit activities mentioned which are reported to them and which are carried out by the

recipients of their services, and, on the other hand, suspend any content likely to cause attack on morality.

The judicial authority may order, in accordance with the law, any service provider in line, and failing that, to any Internet access provider, all measures likely to prevent a damage or to stop damage caused by the content of an online service.

Article 288.

The person whose activity is to publish an online public communication service is required to make available to its subscribers, in an open standard, the names of the director of publication and of the person responsible for the editorial, the company name, the address electronic and telephone number of the online service provider.

Article 289.

The Internet access provider and the online service provider are required to obligation of confidentiality for all matters relating to the disclosure of these elements identification or any information allowing the identification of the person concerned,

This obligation of confidentiality is not enforceable against the judicial authority or the services investigation by the judicial police, nor to the National Cybersecurity Agency, the Authority of data protection, as well as security services when required for the needs public order.

Section 2: Specific obligations

Article 290.

The cache provider is not responsible for the data and information it processes in the framework of its activities.

However, he becomes liable under the following conditions if he:

1. modifies the information;
2. does not comply with the conditions of access to information;

3. does not comply with the rules regarding the updating of information, indicated in a manner widely recognized and used in the sector;
4. hinders the lawful use of technology, widely recognized and used by the sector, for the purpose of obtaining data on the use of information;
5. fails to act promptly to remove stored information or to make access to it is impossible as soon as he actually becomes aware of the fact that the information at the origin of the transmission has been removed from the network or that access to the information has been made impossible, or that an administrative or judicial authority has ordered the information to be removed or access to it to be made impossible.

Article 291.

The hyperlink provider is responsible for the information it provides.

access, provided that:

1. it does not promptly remove or prevent access to the information after receiving an injunction from the judicial authority to remove the hyperlink;
2. he has not become aware or conscious of specific illegal information stored or of illegal activities that the recipients of their services may be carrying out, other than by an injunction from the judicial authority;
3. he failed to promptly inform the judicial authorities to enable them to assess the nature of the information or activities and, if necessary, to order the removal of the content.

Article 292.

The search engine provider which, automatically or on the basis of the

entries made by others, presents an index of online content or makes available

electronic means to search for information provided by third parties, is responsible

search results, provided that it:

1. either at the origin of the transmission;
2. selects the recipient of the transmission;
3. selects or modifies the information contained in the transmission.

Article 293.

The host is responsible for the information stored at the request of a user of the

service it provides, provided that:

1. when he has not become aware of specific illegal information, stored or illegal activities carried out by the recipients of the service, it immediately informs the judicial authority.
2. It does not remove, disable or impede access promptly access the data after receiving an injunction from the judicial authority to remove the data.

Paragraph 1 of this Article does not apply where the recipient of the service acts under the authority or control of the host.

Article 294.

The seller of products and/or provider of information technology and communication is required to request, from the Minister having digital in his attributions, a certificate of conformity after analysis of the vulnerability and evaluation of the security guarantee by IT security experts approved by the said Minister.

It is also required to inform consumers of any vulnerabilities detected in information and communication technology products and services as well as solutions deployed to address this.

Article 295.

The digital service provider is required to implement qualified systems of detection of events likely to affect the security of their computer systems.

The qualifications of detection systems and service providers operating these systems are delivered by the Ministry responsible for digital technology, the Agency National Cybersecurity heard.

Article 296.

The digital service provider subjects its IT system to checks intended to verify the level of security and compliance with security rules.

These checks are carried out by the National Cybersecurity Agency. The cost of the checks is the responsibility of the digital service provider.

Article 297.

For the purposes of IT system security and service providers digital, the National Cybersecurity Agency can obtain from suppliers, the identity, the postal address and email address of users or system owners vulnerable, threatened or attacked computers, in order to alert them to the vulnerability or compromise of their system.

CHAPTER II: CRYPTOLOGY:

Section 1: General provisions

Article 298.

The use, supply, import and export of cryptographic means ensuring exclusively authentication or integrity control functions are free, under subject to the obligations provided for in this Book.

However, when cryptology means allow functions to be ensured confidentiality, the principle of free use referred to in paragraph 1 applies only if the means are based on agreements managed by an approved service provider.

Cryptology service provision is reserved for service providers of cryptology, in accordance with the terms determined under this chapter, except in the case where encryption is done for its own data.

Section 2: Legal regime

Article 299.

No one may carry out a cryptology activity without submitting to one of the legal regimes provided for in this Book.

The exercise of cryptology activities and services is subject to the authorization or declaration, in accordance with the terms and conditions of grant set out in Book 1 of the this ordinance-law and by order of the Minister responsible for digital technology.

The instruction of requests for authorization or declaration, as well as the preparation of the notebook The charges are the responsibility of the National Cybersecurity Agency.

The National Cybersecurity Agency has created a Cryptology Commission within its ranks.

Article 300.

The supply or importation of cryptographic means not exclusively ensuring authentication or integrity control functions are subject to a prior declaration with the Cryptology Commission of the National Cybersecurity Agency, subject to any exemptions from reporting under a legal or regulatory provision.

Article 301.

The provider or person carrying out the supply, import or export of a means of cryptology keeps at the disposal of the Cryptology Commission a description technical characteristics of the cryptology means used.

Article 302.

The export of cryptographic means not exclusively ensuring functions authentication or integrity control is subject to the authorization of the Minister having the digital in its attributions, the Cryptology Commission of the National Agency of Cybersecurity heard.

Section 3: Cryptology Service Providers

Article 303.

The cryptology service provider is required to obtain prior authorization from of the Cryptology Commission of the National Cybersecurity Agency.

The conditions for issuing approval to cryptology service providers as well as that their obligations are defined by order of the Minister responsible for digital technology attributions.

Article 304.

The Cryptology Commission of the National Cybersecurity Agency, on the instructions of the Minister responsible for digital technology provides for exceptions to this obligation prior authorization for the provision of cryptology services including technical characteristics or the conditions of supply are such that, with regard to the interests of national defence and the internal or external security of the State, this supply may be exempt from any prior formality.

Article 305.

The cryptology service provider is liable for damage caused to persons:

1. entrusting them with the management of their secret agreements in the event of an attack the integrity, confidentiality or availability of data transformed using these conventions;
2. who have relied on the cryptology service provided. Any contractual clause to the contrary is deemed unwritten.

The cryptology service provider releases or limits its liability if it manages to demonstrate the absence of negligence or intentional fault.

The cryptology service provider is exempt from any liability with regard to persons who make unauthorized use of their services, provided that the conditions of use contained in a written statement are accessible to users and clearly present the permitted and unauthorized uses.

The cryptology service provider must take out a policy insurance covering the risks associated with the exercise of their activities.

Section 4: Administrative sanctions

Article 306.

When a provider of cryptology services, even free of charge, does not comply with the obligations to which it is subject under this Book, the National Agency for Cybersecurity may, after hearing the person concerned, pronounce:

1. the prohibition on using or putting into circulation the means of cryptology concerned. This means may be put back into circulation as soon as the obligations previously not respected have been satisfied, under the conditions provided for in the provisions of this Chapter;
2. the temporary withdrawal of the authorization granted for a period of between one and twelve months;
3. the definitive withdrawal of the authorization granted;
4. the payment of fines, the amount of which is set according to the seriousness of the breaches committed and in relation to the advantages or profits derived from these breaches.

Article 307.

The ban on placing into circulation provided for in the preceding article is applicable to all of the national territory. It also entails for the supplier the obligation to carry out the withdrawal :

1. with commercial broadcasters, cryptology means whose implementation traffic was banned;
2. materials constituting means of cryptology whose circulation has been prohibited and which have been acquired for a fee, directly or through commercial distributors.

The relevant cryptographic means is put back into circulation as soon as the obligations previously unfulfilled obligations will have been satisfied.

TITLE IV: CRIMINAL PROTECTION OF COMPUTER SYSTEMS

CHAPTER I: GENERAL PRINCIPLES

Section 1: Criminal liability

Article 308.

The State, provinces, decentralized territorial entities, administrative authorities independent and public institutions do not incur criminal liability.

State agents or public officials working for the State, provinces, entities decentralized territorial authorities, independent administrative authorities and establishments

Public authorities incur individual criminal liability when they commit offences punishable by this ordinance-law in the exercise of their functions.

Article 309.

The legal person under private law is liable for the offences provided for by the provisions of this ordinance-law when they are committed on their behalf by one of their representatives.

The directors of private legal entities incur criminal liability individual when they commit offences in the same circumstances and in the exercise of their functions.

Section 2: Penalties

Article 310.

Without prejudice to the provisions of the Congolese Penal Code, the penalties applicable in matters of cybercrime-related offences are:

1. Penal servitude;
2. The fine;
3. Special confiscation.

Article 311.

The penalties incurred by legal persons for the offences referred to herein ordinance-law, are as follows:

1. A fine the maximum amount of which is equal to five times that provided for for individuals by the law which punishes the offence;
2. Dissolution when it is an offence which affects security and to state security;
3. A permanent ban or a ban for a period of two to five years from exercising directly or indirectly one or more professional or social activities;
4. The permanent closure or closure for a period of two to five years of one or more several of the company's establishments used to commit the incriminated acts;

5. Permanent exclusion from public markets for a period of two (2) to five (5) years;
6. A permanent ban or a ban for a period of two to five years on appealing public savings;
7. A ban for a period of two to five years on issuing checks other than those which allow the withdrawal of funds by the drawer from the drawer or those which are certified, or on using payment cards;
8. Confiscation of the tool used to commit the offence and of the proceeds of l'infraction.

Article 312.

Without prejudice to the provisions of the Congolese Penal Code, in the event of conviction for one of the offences provided for in this Book, the competent court may pronounce the confiscation of materials, equipment, instruments, computer systems or computer data as well as cash assets, benefits or products resulting from l'infraction.

The decisions of conviction taken under the preceding paragraph are published in the Official Journal of the Democratic Republic of Congo.

Article 313.

Without prejudice to the provisions of the Congolese Penal Code, in the event of conviction for one of the offences provided for in this ordinance-law, the competent court pronounces the prohibition in accordance with the terms provided for in this article.

This penalty includes a ban on sending electronic communications messages. and the prohibition, temporarily or permanently, of access to the site used to commit the infringement or any other site whatsoever, for a period of five (5) to ten (10) years.

The competent court may order any person responsible for the site to: used to commit the offence and/or any other person qualified to implement the technical means necessary to ensure the prohibition of access, accommodation or the cutting off access to the offending site.

Article 314.

The competent court may rule against the convicted person for the offences provided for in this Book, the prohibition permanently or for a period of five to ten years, to carry out any activity related to the electronic communications sector or to exercise a public function, an elective mandate or a function in a company of which the State is totally or partially the owner or a socio-professional activity, when the acts were committed in the exercise or on the occasion of the exercise of functions.

The competent court may prohibit in whole or in part the exercise of civil rights and following civilians:

- Right to vote;
- Right of eligibility;
- Prohibition of access to public and parastatal functions of any kind the level;
- Right to be an expert or witness in civil status documents;
- Right to give evidence in court, other than to provide simple information.

Violation of the prohibitions provided for in this ordinance-law and pronounced by the courts and tribunals is punishable by a term of penal servitude of six months to three years and a fine of three hundred thousand to five million Congolese francs.

Conviction decisions taken under this article are published in the Journal official of the Democratic Republic of Congo.

Section 3: Criminal participation and punishable attempt

Article 315.

Is punishable by the same penalty as the offence committed, in accordance with the Penal Code. Book I, any criminal participation and any attempt to violate this order- law.

Section 4: Repeat offenses and aggravating circumstances

Article 316.

When one of the offences provided for in this ordinance-law is committed within five years following the pronouncement of the conviction which has become irrevocable for one of these

offences, the penalty provided by law is doubled, the maximum of penal servitude is not
which may exceed twenty years.

Article 317.

When an offence is committed by a member of a criminal organisation or a
organized gang with a view to committing offences punishable by this ordinance-law, the
The initially planned sentence is doubled, the maximum penal servitude cannot exceed
twenty years.

Where one of the offences provided for under this Ordinance-Law undermines State security, computer data and/or computer systems linked to
strategic or sensitive infrastructures and applications, the judge pronounces the sentence of servitude life imprisonment and a fine of one to twenty billion Congolese francs.

CHAPTER II: RULES OF PROCEDURE AND JURISDICTION JURISDICTIONS

Section 1: On the observation of violations of digital legislation

Article 318.

Violations of digital legislation are noted by police officers
judicial with limited jurisdiction or with general jurisdiction as the case may be.

When judicial police officers are notified or note the facts of an offence under
provisions of this ordinance-law, they inform the officer of the Public Prosecutor's Office competent in accordance with the provisions of the Code of Criminal Procedure.

Article 319.

Violations of digital legislation are noted in reports drawn up
in accordance with the Code of Criminal Procedure.

Section 2: Searching data stored in a computer system

Article 320.

When data stored in a computer system or on a medium allowing
keeping data on the national territory is useful for the manifestation of the truth,
the Public Prosecutor, in accordance with the provisions of Articles 22 and 23 of the
Code of Criminal Procedure, may carry out a search or access a computer system
or any part thereof, or to any other computer system or medium and to data
present in the latter as long as this data is accessible from the system
initial or available for the initial system.

If it is previously proven that this data, accessible from the initial system or
available to the initial system, are stored in another computer system located in
outside the national territory, they are collected by the officer of the Public Prosecutor's Office, by means
of international letters rogatory.

Article 321.

When the Public Prosecutor discovers data in a computer system
stored which are useful for the manifestation of the truth, but that the seizure of the medium does not
does not appear desirable, these data, as well as those which are necessary for the
understand, are copied onto computer storage media that can be seized and
placed under seal, they can also be made inaccessible or removed from the system
computer in question by decision of the judge.

Section 3: Data interception

Article 322.

The Public Prosecutor may, when the needs of the information so require, prescribe
the interception, recording and transcription of correspondence in accordance with

provisions of this Ordinance-Law, including data relating to the content,
issued by electronic communications.

The interception may not concern a line belonging to a lawyer, a lawyer's office or
from his home, unless there are reasonable grounds to suspect him of having committed or
attempted to commit, as an author or accomplice, the offence which is the subject of the proceedings
or a related offence, provided that the measure is proportionate in relation to the
nature and seriousness of the facts. The interception is authorized by decision of the Attorney General
near the Court of Appeal, seized by requisition of the prosecuting Magistrate, the national bar association
informed or the president of the bar as the case may be.

Article 323.

The National Cybersecurity Agency authorizes:

1. interceptions of correspondence sent by electronic communications, in accordance with the provisions of this ordinance-law;
2. the conservation and protection of the integrity as well as the collection, including in real time in accordance with the procedures provided for in Articles 25 et seq. of the Code of Criminal Procedure, of data and information on personal data and in Article 273 of this Ordinance-Law.

The methods of implementing the provisions of this article will be specified by
regulatory.

Article 324.

The interception operations referred to in this ordinance-law are authorized by
the National Cybersecurity Agency when necessary:

1. to the maintenance of national sovereignty, territorial integrity or national defense;
2. to the preservation of the major interests of the foreign policy of the Republic Democratic Republic of Congo;
3. to safeguard major economic, industrial and scientific interests of the Democratic Republic of Congo;
4. to the prevention of terrorism, collective violence likely to lead seriously damaging public order or organized crime and delinquency.

Section 4: Prosecutions

Article 325.

Violations of digital legislation are prosecuted in accordance with the Code of criminal proceedings and proven by any legal means.

Article 326.

Public action against breaches of digital legislation is taken in accordance with the Code of Criminal Procedure and the provisions of this ordinance-law.

Section 5: Termination of public action

Article 327.

Public action to suppress violations of digital legislation is time-barred in accordance with the Congolese Code of Criminal Procedure.

Limitation periods begin to run from the day the criminal act is committed. or, if it has been concealed, from the day of its discovery or revelation.

Section 6: Competent jurisdictions

Article 328.

The rules of jurisdiction and procedure applicable to breaches of legislation digital are those provided respectively by organic law n°13/011-B of April 11 2013 on the organization, operation and jurisdiction of the courts of the judicial system and the Code of Criminal Procedure.

However, the commercial court has jurisdiction over all offences provided for by the this ordinance-law which infringe economic and commercial legislation, whatever whatever the rate of penal servitude or the amount of the fine.

Article 329.

Without prejudice to the Code of Criminal Procedure, the courts referred to in the preceding article are competent when:

1. The offence was committed on the Internet in the territory of the Democratic Republic of Congo, or when the illegal content is accessible from the Democratic Republic of Congo;
2. The natural or legal person has been guilty, in the territory of the Democratic Republic of Congo, as an accomplice of an offence committed abroad if the offence is punishable by both Congolese law and foreign law;

3. The offence was committed by Congolese people outside the territory of the Democratic Republic of Congo and that the acts are punishable by the legislation of the country where they were committed.

CHAPTER III: QUALIFICATION OF OFFENSES

Article 330.

Constitutes an infringement of digital legislation, any violation of which is punishable of a penalty provided for by this ordinance-law.

This Ordinance-Law defines the charges and penalties for specific offences. related to digital.

Section 1: Common law offences committed by means of or on a network electronic communication or a computer system

Article 331.

Common law offences committed using a communications network electronic or computer system are punishable in accordance with the Criminal Code Congolese and the specific criminal provisions in force.

Section 2: Attacks on computer systems

Paragraph 1: On illegal access and maintenance

Article 332.

Anyone who fraudulently and without right gains access to or maintains, in whole or in part, of a computer system, with fraudulent intent is punishable by a term of imprisonment criminal sentence of three to five years and a fine of fifty million to one hundred million francs Congolese, or one of these penalties only.

Whoever, with fraudulent intent or with the aim of causing harm, exceeds his authority legal access to a computer system, is punishable by a term of penal servitude of two to five years and a fine of fifty million to one hundred million Congolese francs, or one of these penalties only.

Article 333.

Where the facts referred to in the preceding article result in the deletion, obtaining or modification of data contained in the computer system, or an alteration of the operation of this computer system, the penalties provided for are increased from five to ten years of penal servitude and a fine of one hundred million to three hundred million Congolese francs or one of these penalties only.

When the acts referred to in the preceding article are committed in violation of security measures, The perpetrator of these acts is punished by a term of penal servitude of ten to twenty years and a fine of three hundred million Congolese francs to five hundred and fifty million francs Congolese or one of these penalties only.

Paragraph 2: Attacks on data in a computer system

Article 334.

Is punishable by penal servitude of five to ten years and a fine of fifty to one hundred millions of Congolese francs, whoever intercepts, discloses, uses, alters or diverts intentionally and without right by technical means, data during their non-public transmission to, from or within a system computer science, including electromagnetic emissions from a system computer carrying such data.

Article 335.

Is punishable by penal servitude of six months to three years and a fine of five million to one hundred million Congolese francs, the one who transfers, without the authorization of the person concerned, personal data of the latter from a computer system or from one data storage medium to another.

The penalty provided for in the preceding paragraph may be increased from three to ten years of penal servitude, if this offence is committed with fraudulent intent, or in connection with a system computer connected to another computer system, or bypassing the measures protections put in place to prevent access to the content of non-public transmission.

However, the following does not constitute an offence within the meaning of this article:

1. Interception carried out in accordance with a court warrant;
2. Communication sent by or intended for a person who has consented to the interception;
3. Interception carried out by a legally authorized legal person for the needs of public security or national defense;
4. Interception carried out by a legal or natural person legally authorized under the legal and regulatory provisions in force in the Democratic Republic of Congo.

Article 336.

Whoever, intentionally and without right, directly or indirectly damages, erases, damages, alters or deletes data, will be punished by a term of penal servitude of six months to five years and a fine of fifty million to one hundred million Congolese francs, or of one of these penalties only.

If the offence referred to in paragraph 1 is committed with fraudulent intent or with the aim of harm, the penalty of penal servitude is two to five years and a fine of fifty million to one hundred million Congolese francs, or one of these penalties only.

Paragraph 3: Attacks on the integrity of the computer system

Article 337.

Is punishable by a term of penal servitude of five to ten years and a fine of two hundred million to two hundred and fifty million Congolese francs, or one of these penalties only, he who, intentionally and without right, directly or indirectly, causes by any technological means an interruption of the normal functioning of a system computer science.

Any person who, as a result of committing the acts referred to in paragraph 1, causes damage to data in the relevant computer system or in any other computer system, will be

punished by a term of penal servitude of ten to fifteen years and a fine of two hundred million to two hundred and fifty million Congolese francs or one of these penalties only.

Any person who, as a result of committing the acts referred to in paragraph 1, causes a disturbance serious or prevented, totally or partially, the normal functioning of the system computer system concerned or any other computer system, will be sentenced to the penalty of penal servitude of fifteen to twenty years and a fine of two hundred million to two hundred fifty million Congolese francs or one of these penalties only.

Where the commission of the acts referred to in paragraph 1 affects one or more infrastructures sensitive or critical, within the meaning of this ordinance-law, the responsible person is sentenced to penal servitude of fifteen to twenty years and a fine of three hundred million to five hundred million Congolese francs or one of these penalties only.

The penalty of penal servitude and the fine are applicable even if the consequences on the or the computer systems referred to in the preceding paragraphs are temporary or permanent.

Paragraph 4: Abuse of devices

Article 338.

Whoever intentionally and without right produces, sells, imports, exports, distributes or made available in any other form, any electronic device or equipment, including data or computer programs, primarily designed or adapted to enable the commission of one or more offences provided for herein ordinance-law, will be punished by a term of penal servitude of two to five years and a fine from two hundred and fifty million to five hundred million Congolese francs or one of these only penalties.

Whoever, intentionally and without right, possesses within the meaning of this order-law, any device, including data, primarily designed or adapted for allow the commission of one or more offences provided for in this order-law is punishable by a term of penal servitude of six months to five years and a fine of five one hundred thousand to two million Congolese francs or one of these penalties only.

Is punishable by a term of penal servitude of two to five years and a fine of five hundred one thousand to two million Congolese francs or one of these penalties only, any officer or public official, custodian or agent of the public force who, during the exercise of his functions, except in cases provided for by law or without respecting the formalities it prescribes, unduly, possesses, produces, sells, obtains for use, imports, distributes or makes available provision in another form of a device, including data, primarily designed or adapted to enable the commission of one or more offences referred to herein ordinance-law.

Paragraph 5: On the falsification of data or forgery in IT

Article 339.

Whoever commits forgery by intentionally and without right introducing into a system computer or electronic communications network, by modifying, altering or erasing data that is stored, processed or transmitted by a computer system or an electronic communications network, or by modifying by any other means technological, the possible use of data in a computer system or network electronic communication, and thereby modifies the legal scope of such data, is punished by penal servitude of three to five years and a fine of twenty to fifty million million Congolese francs, or one of these penalties only.

Anyone who uses the data referred to in the preceding article, knowing that they are false, is punishable by penal servitude of five to ten years and a fine of twenty million to fifty million Congolese francs, or one of these penalties only.

Paragraph 6: Computer fraud

Article 340.

Whoever, intentionally and without right, causes or seeks to cause harm to another with the intention of providing an illegal economic advantage to oneself or a third party,

shall be punished by a term of penal servitude of five to ten years and a fine of fifty to one hundred million Congolese francs:

1. If he has introduced into a computer system, by modifying, altering or erasing data that is stored, processed or transmitted by a computer system;
2. If it disrupts the normal operation of a computer system or the data contained therein.

Section 3: Attacks in the area of the National Cybersecurity Agency

Article 341.

Anyone who fails to comply with the following requirements shall be punished with a fine of five to ten million Congolese francs:

complies with the obligation to communicate to the National Cybersecurity Agency a description of the technical characteristics of the cryptology means under the conditions provided for by the provisions of Title II of this ordinance-law and its texts d'application.

Article 342.

Anyone who provides or imports a means of cryptology that does not exclusively provide functions authentication or integrity control without meeting the reporting requirement prior to the National Cybersecurity Agency.

Is punishable by five to ten years of penal servitude and a fine of fifty to one hundred million Congolese francs, anyone who has provided cryptology services without having obtained previously obtained the approval certificate from the National Cybersecurity Agency.

Article 343.

Is punishable by five to ten years of penal servitude and a fine of five to ten million Congolese francs, or one of these penalties only, anyone who exports a means of cryptology not exclusively providing authentication or control functions integrity without having first obtained authorization from the National Agency for Cybersecurity.

Article 344.

Is punishable by five to ten years of penal servitude and a fine of five to ten million Congolese francs, or one of these penalties only, whoever has made available of another by the sale or rental of a means of cryptology which has been the subject of a administrative ban on use and circulation.

Article 345.

Is punishable by five to ten years of penal servitude and a fine of fifty to one hundred million Congolese francs, or one of these penalties only, whoever by any means of cryptology, will have obstructed the progress of investigations within the meaning of the Code of Procedure criminal and this Ordinance-Law or refused to provide information or documents therein related.

Article 346.

Where a means of cryptology has been used to prepare or commit an offence or to facilitate its preparation or commission, the maximum penalty provided for by the Code penal servitude is doubled, penal servitude cannot exceed twenty years.

Article 347.

Is punishable by three years of penal servitude and a fine of five million to forty million. of Congolese francs, anyone having knowledge of the secret decryption convention of a means of cryptology likely to have been used to prepare, facilitate or commit an offence, refuses to hand over the said agreement to the judicial authorities or to put it in works on the requisitions of these authorities issued in application of the Code of Procedure criminal.

If the refusal is made while the delivery or implementation of the agreement allows to prevent the commission of an offence or to limit its effects, the penalty is increased to five years of penal servitude and a fine of five million to twenty million Congolese francs.

Section 4: Offences related to the use of personal data

Paragraph 1: Sending unsolicited messages

Article 348.

Any unsolicited electronic message sent based on the collection of data from personal character must contain a link that allows the beneficiary to unsubscribe.

Failure to comply with this provision exposes the offender to a fine of five hundred thousand to two million Congolese francs.

Paragraph 2: On deception

Article 349.

Is punishable by a term of penal servitude of six months to two years and a fine of twenty-five million Congolese francs, or one of these penalties only, anyone who uses the identification elements of a natural or legal person for the purpose of deceiving recipients of an electronic message or users of a website with a view to leading them to communicate personal data or confidential information.

Paragraph 3: Unauthorized processing

Article 350.

Anyone who has carried out a transfer of personal data either without having previously informed individually the person concerned of their right of access, rectification or opposition, the nature of the data transmitted and the recipients of these, despite the opposition of the person concerned, will be punished by a penalty of penal servitude of six months to two years and a fine of two million to five million Congolese francs, or one of these penalties only.

Paragraph 4: Identity theft

Article 351.

Is punishable by penal servitude of one to five years and a fine of twenty million to one hundred millions of Congolese francs, whoever usurps, by phishing or any other means, intentionally and without right through a computer system, the identity of others, one or more data allowing one to falsely and illicitly attribute oneself the identity of others with the aim of disturbing their peace, of harming their honour, their consideration or to its interests.

Anyone who, by intentionally wrongly relying on a legitimate motive or justification and by using a computer system at any stage of the offence, shall have transferred, possessed or used a means of identifying oneself to another person with the intention of committing, assisting or to encourage illegal activity, is punishable by penal servitude of two to five years and a fine of five to one hundred million Congolese francs or one of these penalties only.

Will be punished with a term of penal servitude of five to ten years and a fine of one hundred million to two hundred million Congolese francs, or one of these penalties only, whoever commits pass for an institutional, trusted or other third party, through a system computer, with the aim of inciting or forcing the victim to communicate data to him personal.

Article 352.

Anyone who has used personal data or confidential information communicated for the purpose of embezzling public or private funds, will be punished by a penalty of penal servitude of five to ten years and a fine of fifty million to one hundred million Congolese francs.

Section 5: Bank card fraud and offences relating to advertising on internet

Paragraph 1: Bank card fraud

Article 353.

Without prejudice to the other provisions set out in Article 123 of Law No. 18/019 of 9 July 2018 relating to payment systems and securities regulations, is punishable by a term of servitude criminal sentence of two to five years and a fine of fifty to five hundred million francs Congolese or one of these penalties only, the fact for any person of:

1. counterfeit or falsify a payment or withdrawal card by means of or on a electronic communications network or a computer system;
2. knowingly use a counterfeit or falsified payment or withdrawal card by means of or on an electronic communications network or computer system;
3. knowingly agree to receive payment by means of a counterfeit or falsified payment card by means of or on an electronic communications network or computer system.

Article 354.

Is punishable by a term of penal servitude of five to ten years and a fine of fifty million to five hundred million Congolese francs or one of these penalties only, the fact for any person to manufacture, acquire, hold, transfer, offer or make available provision of equipment, instruments, computer programs or any data, designed or specially adapted to commit the offences provided for in the preceding article.

Confiscation for the purpose of destruction of counterfeit or falsified payment cards is mandatory in the cases provided for above. The confiscation of materials, machines, tools, devices, instruments, computer programs or any data having been used or intended to be used or intended to be used in the manufacture of said objects, except when they have been used without the owner's knowledge.

In all cases provided for in the above paragraphs, the judicial authority may pronounce, in the event of repeat offense, the prohibition of civil rights as well as the prohibition, for a period of two years, moreover, to exercise a professional or social activity.

Paragraph 2: Offences relating to advertising on the Internet

Article 355.

Advertising by means of or on an electronic communications network or a computer system in favor of unauthorized online gambling and games of chance is forbidden.

Any person who contravenes the prohibition set out in paragraph 1 shall be punished by a fine of twenty to fifty million Congolese francs.

The competent court may increase the amount of the fine to four times the amount of the advertising expenditure devoted to the illegal operation.

Section 6: Abusive Content

Paragraph 1: On the dissemination of tribalist, racist and xenophobic content through of an electronic system

Article 356.

Anyone who intentionally creates, downloads, distributes or makes available to the public through a computer system of writings, contents, messages, photos, sounds, videos, drawings or any other representation of ideas or theories of a racist, tribalist or xenophobic or in any form whatsoever, within the meaning of this ordinance-law and in accordance with the provisions of Ordinance-Law No. 66-342 of June 7, 1966 relating to repression of racism and tribalism, will be punished by penal servitude of one month to two years and a fine of one million to ten million Congolese francs or one of these penalties only.

Paragraph 2: Child pornography

Article 357.

The act of producing, distributing, broadcasting, importing, exporting, offering, making available, to sell, to obtain or to provide to others, to possess any material child pornography through a computer system or a electronic communications network, is punishable by five to fifteen years of penal servitude. principal and a fine of two thousand to one million Congolese francs.

Paragraph 3: Harassment through electronic communication

Article 358.

Anyone who initiates electronic communication that coerces, intimidates, harasses or causes emotional distress in a person, by using a computer system with the aim of encouraging hateful, tribal and hostile behavior against good morals and patriotic values is punishable by penal servitude of one month to two years and a fine of five hundred thousand to ten million Congolese francs.

Article 359.

Anyone who has harassed, through a computer system or a network of electronic communication, a person when he knew or should have known that he would seriously affect the peace of the person concerned by this behavior, will be punished of penal servitude of one month to two years and a fine of five hundred thousand to ten million of Congolese francs, or one of these two penalties only.

Article 360.

Anyone who initiates or relays false information against a person through the networks social, computer systems, electronic communication networks or any form of electronic support, is punishable by penal servitude of one to six months and a fine of five hundred thousand to one million Congolese francs, or one of these penalties only.

Paragraph 4: On the negation, gross minimization, approval or justification of international crimes or sexual violence

Article 361.

Is punishable by penal servitude of ten to twenty years and a fine of one million to ten million of Congolese francs, anyone who distributes or makes available through a system computer or electronic data communications network that denies, minimize, approve or justify acts constituting the crime of genocide, crimes of war, crimes against humanity, crimes of aggression and/or sexual violence such as as defined by international instruments and the Congolese Penal Code and recognized as such by a final and conclusive decision of a national or international court.

Paragraph 5: Incitement or provocation to commit terrorist acts and Apology for terrorist acts

Article 362.

Anyone who, by means of a computer system or communications network electronic, incited or directly provoked acts of terrorism, will be punished in accordance with to the provisions of Articles 157 to 160 of the Congolese Military Penal Code.

Paragraph 6: Junk mail or junk mail or spam

Article 363.

Will be punished by penal servitude of two to five years and a fine of ten to fifty million Congolese francs or one of these penalties only any person who,

intentionally and without legitimate motive or justification, or by wrongly relying on a motive or a legitimate justification:

1. triggers the transmission of erroneous, unwanted or contrary to the law messages law, multiple e-mails from or through a computer system;
2. uses a computer system or electronic communications network protected to relay or retransmit email messages multiple for the purpose of deceiving or misleading users or any e-mail or internet access service provider as to the origin of these messages;
3. seriously falsifies header information in email messages multiple electronic devices and intentionally triggers the transmission of these messages.

Section 7: Offences against the Internet access provider

Article 364.

The Internet service provider that does not inform its subscribers of the existence of means techniques for restricting access to certain services is punishable by a fine of five million to twenty million Congolese francs.

In the event of a repeat offence, the fine is ten million to twenty million Congolese francs.

Article 365.

The person who reports content or activity to an online service provider as being illicit, with the aim of obtaining its withdrawal or stopping its distribution, then that she knows that this information is inaccurate, is punished by six to twelve months of servitude criminal and a fine of three to five million Congolese francs or one of these penalties only.

Article 366.

The natural person or any manager of a legal person, de jure or de facto, exercising the activity of an internet access provider or online service provider, which does not does not meet the obligations inherent in its legal status as set out in Book I of this ordinance-law, is punishable by penal servitude of six to twelve months and a fine of ten to fifty million Congolese francs or one of these penalties only.

The same penalties provided for in the preceding paragraph apply to any natural person or any manager of a legal entity, de jure or de facto, carrying out the activity of service publisher online communication which does not meet the obligation of vigilance provided for in Book III of this ordinance-law.

Article 367.

The legal entity, de jure or de facto, carrying out the activity of internet access provider or of an online service provider, which does not meet the obligations inherent to its status legal as provided for in Book I of this ordinance-law, is punishable by a fine of one hundred million to five hundred million Congolese francs.

Section 8: Online press offences and disclosure of details of a investigation

Paragraph 1: Press offences by means of electronic communication and right of reply

Article 368.

Anyone who commits acts constituting a press offence, through a computer system or an electronic communications network, will be punished in accordance with the legal provisions applicable to the press and communication.

Article 369.

Without prejudice to the legal provisions applicable to the press and the press and to the communication, anyone who has been the subject of a publication by means of or on a

electronic communications network or a computer system, has a right to
response, without prejudice to requests for correction or deletion of the message that it may
contact the department.

The request for correction or deletion must be submitted no later than three
months from the date the message justifying it was made available to the public.

The Director of Publication is required to insert within three days of their receipt, the
responses from any person named or designated in the online communications services.

Failure to comply with the requirements of the preceding paragraph will result in the publication manager being
punished with a fine of two million to five hundred million Congolese francs.

Paragraph 2: On the disclosure of details of an investigation

Article 370.

Is punishable by penal servitude of one month to two years, or a fine of two million to
five million Congolese francs or one of these penalties only anyone, in the
in the context of a criminal investigation, receives an injunction explicitly stating that confidentiality
must be maintained, or where such an obligation is stated by law, and which, without reason or
legitimate justification, or by wrongly relying on a legitimate motive or justification,
discloses through a computer system or communications network
electronically, intentionally:

1. the fact that an injunction has been issued;
2. any action taken under the injunction;
3. any data collected or recorded under the injunction and investigation.

Section 9: Cyber Espionage

Article 371.

Will be punished by penal servitude of five to fifteen years and a fine of five to ten billion billion Congolese francs, or one of these penalties only, anyone who has the intent or knowledge that the offense benefits a foreign government or business foreign, to a foreign intermediary, or to a foreign agent qualified as a spy through of a computer system:

1. steals, or, without authorization, appropriates, takes, carries away, or hides, or fraudulently, or artificially, or by deception, obtains information likely to undermine the security and safety of the State such as provided for by criminal provisions, or a commercial or industrial secret;
2. without permission, copy, duplicate, illustrate, draw, photograph, download, modifies, destroys, photocopies, reproduces, transmits, delivers, sends, addresses by mails, communicates or transfers a trade secret;
3. receives, purchases, or possesses a trade secret, knowing that it has been stolen or appropriated, obtained or transformed without authorization;
4. attempts to commit an offence described in any of paragraphs 1 to 3;
5. conspires with one or more persons to commit an offence described in one of paragraphs 1 to 3 and that one or more of these persons act in such a way as to obtain the object of the conspiracy.

Any organization that commits an offense described in the preceding paragraph is punishable by a fine of fifteen to twenty billion Congolese francs.

Section 10: Recording of images relating to the commission of offences and of the diffusion of elements to manufacture destruction engines

Paragraph 1: Recording of images relating to the commission of offences

Article 372.

Constitutes an act of complicity in intentional attacks on the integrity of the person, the knowingly recording, by any means whatsoever, on any medium whatsoever, images relating to the commission of offences.

Is punishable by penal servitude of one to five years and a fine of twenty to twenty-five million Congolese francs, any person who knowingly disseminates such images.

This Article does not apply where the recording or broadcasting results from the normal exercise of a profession whose purpose is to inform the public either when it is made to serve as evidence in court.

Paragraph 2: On the dissemination of elements for manufacturing destruction devices

Article 373.

Anyone who disseminates, by means of an electronic communications network or a computer system, processes enabling the manufacture of sophisticated destruction devices from powder or explosive substances, nuclear, biological or chemicals, or from any other product intended for domestic, industrial or agricultural, will be punished by five to ten years of penal servitude and a fine of twenty-five millions of Congolese francs.

When these procedures have allowed the commission of murder or assassination, the penalty is twenty years of penal servitude and a fine of fifty to one hundred million francs Congolese.

Paragraph 3: Failure to maintain the protective devices of a system computer science

Article 374.

Is punishable by a fine of ten to fifty million Congolese francs, the act for the responsible for computer systems, failing to maintain the devices in good condition protection of a computer system.

Section 11: Infringement of copyright and intellectual and industrial property as well as related rights

Article 375.

Whoever deliberately commits, on a commercial scale and by means of a system computer science, an infringement of copyright, intellectual and industrial property as well as than to neighboring rights defined by the legislation in force in the Democratic Republic of Congo, is punishable by six months to five years of penal servitude and a fine of fifty to one hundred million Congolese francs, or one of these penalties.

Anyone who infringes the property rights or the copyright of a creation computer science, namely a computer program, is punishable by six months to five years of penal servitude and a fine of fifty to one hundred million Congolese francs or one of these penalties.

Paragraph 1: Counterfeiting of trademarks, trade names, designations of origin, geographical indication, software and preparatory design material

Article 376.

Counterfeiting and/or piracy of trademarks, trade names, designations, software, preparatory design and geographical indication materials is punishable by a penalty of penal servitude of five to ten years and a fine of fifty to one hundred million Francs Congolese or one of these penalties only.

Counterfeiting constitutes the act, without the authorization of the author or his successors in title, of reproduce, use, sell, denigrate, distort a brand, a trade name, a designation of origin or a geographical indication belonging to another by means of a or on an electronic communications network or computer system.

Paragraph 2: Counterfeiting of designs and models

Article 377.

Is punishable by penal servitude of three to five years and a fine of fifty to one hundred million Congolese francs or one of these penalties only anyone who, without authorization of the author or his successors in title, to reproduce, represent or make available from the public, a design or model protected by copyright or a related right by means of of an electronic communications network or a computer system.

Paragraph 3: On infringement of patent property rights

Article 378.

An infringement of intellectual property constitutes the act, with full knowledge of the facts, without right to sell or make available to the public by reproduction or representation, a good or product protected by a patent for invention by means of a computer system. Those who, with full knowledge of the facts, sell, exhibit for sale, rent out, hold or introduce into the territory of the Democratic Republic of Congo for the purpose commercial, objects or works or software or protected computer hardware by a patent are punishable by the same penalties provided for in Article 14 of the Penal Code.

Without prejudice to the penalties provided for in Article 14 of the Penal Code, the following shall be punished by five to ten years of imprisonment: penal servitude and a fine of two hundred to two hundred and fifty million francs Congolese.

Paragraph 4: On the attack on the configuration diagrams of a digital system protégé

Article 379.

Constitutes an infringement of intellectual property, the act, with full knowledge of the facts, without right to sell or make available to the public by reproduction or representation a configuration diagram of a digital system using a communication network electronic.

Paragraph 5: From the infringement to an effective technical measure

Article 380.

The act of:
undermine, for purposes other than scientific research, an effective technological measure in order to alter the protection of a material by decoding, decryption or any other

personal intervention intended to circumvent, neutralize or suppress a mechanism of protection or control, when this infringement is carried out by means other than the use of a technological application or device.

Is punishable by six months to one year of penal servitude and a fine of two to five hundred thousand Congolese francs or one of these penalties only, the act of procuring or proposing knowingly to others, directly or indirectly, means designed or specially adapted to undermine an effective technical measure, by one of the following methods:

1. by manufacturing or importing a technological application or device for purposes other than research;
2. by holding for sale, loan or rental, by offering for these same purposes or by making available to the public in any form whatsoever, an application technological, a device or a component;
3. by providing a service for this purpose;
4. by inciting the use or by ordering, designing, organizing, reproducing, distributing or disseminating advertising in favour of one of the processes referred to in points 1 to 3 by means of an electronic communications network.

These provisions do not apply to acts carried out for computer security purposes.

Paragraph 6: Deletion of an element of information on the rights regime to infringe copyright

Article 381.

The act of:
delete or modify, knowingly and for purposes other than scientific research, any information element on the rights regime, by personal intervention, with the aim of to infringe, conceal or facilitate copyright infringement.
Is punishable by penal servitude of two to six months and a fine of two to five million of Congolese francs, or one of these penalties only, the act of procuring or proposing knowingly to others, directly or indirectly, means designed or specially adapted to delete or modify, even partially, an element of information on the

rights regime, with the aim of infringing a copyright, concealing or facilitate such an attack, by one of the following methods:

1. by manufacturing or importing a technological application, device or a component, for purposes other than research;
2. by holding for sale, loan or rental, by offering to these same purposes or by making available to the public in any form whatsoever either a technological application, device or component;
3. by providing a service for this purpose;
4. by encouraging the use, ordering, designing, organizing, reproducing, distributing or broadcasting an advertisement in favor of one of the precedents referred to in points 1 to 3 using a computer system.

Article 382.

Is punishable by penal servitude of two to six months and a fine of two to five million million Congolese francs, or one of these penalties only, the fact of importing, distribute, make available to the public in any form or communicate to the public, directly or indirectly, a work of which an element information on the rights regime has been removed or modified with the aim of undermining to a copyright, to conceal or facilitate such infringement. These provisions are not applicable to acts carried out for the purposes of scientific research or computer security.

BOOK V: MISCELLANEOUS, TRANSITIONAL, REPEAL AND REPEAL PROVISIONS FINALS

CHAPTER I: FISCAL, PARAFISCAL, CUSTOMS AND CHANGER

Article 383.

Legal entities and individuals carrying out digital activities and services evolving in the digital sector from or to the Democratic Republic of Congo, are subject to the common law regime in tax, parafiscal and customs matters and exchange rates in force.

Article 384.

Digital startups with entrepreneurial status are eligible for tax benefits,
parafiscal, customs and exchange duties provided for by the legislation relating to entrepreneurship and startups.

Furthermore, and without prejudice to the provisions of Ordinance-Law No. 69-006 of February 10, 1969 relating to the actual tax as amended to date and other applicable texts in the matter
tax :

1) It is granted to startups, entrepreneurs as well as small and medium-sized enterprises
operating in the digital sector, a total exemption from taxes, duties, fees and
royalties for a period of twelve months, renewable twice, with the exception of taxes,
duties, taxes and charges for which they are legally liable or those collected in return
services rendered;

2) It is granted to digital service providers that those listed in the point above,
a 50% reduction in corporate income tax and customs duties
the importation of equipment intended for the operation of digital services, rights
excise duties on digital services, taxes, duties, fees and charges as well as
other indirect taxes, duties, fees and charges for a period of five years. Exception
made from professional taxes on salaries and furniture.

An interministerial decree of the Ministers responsible for finance, small and medium-sized enterprises and digital in their attributions defines the eligibility criteria for the special regime
provided for in paragraph 1 of this article.

Article 385.

Admission to one of the legal regimes provided for in this ordinance-law is not
effective only after payment by the supplier or provider of digital services, as the case may be, of the duties, taxes and fees owed to the State.

An annex relating to duties, taxes and fees owed to the digital sector is added in addition to Ordinance-Law No. 18/003 of March 13, 2018 establishing the nomenclature of central government duties, taxes and charges, worded as follows:

32 Numerically

N°	WORDING OF DUTIES, TAXES AND FEES	GENERATING FACT
01	Tax on the authorization for the provision of digital services Application for authorization	
02	Tax on the declaration for a certificate of approval for the operation and provision of digital services	Declaration of operation of digital services
03	Tax on approval for the provision of digital services to public entities	Application for approval
04	Royalty on the turnover of companies Cybersecurity and computer systems security	Exploitation

An interministerial decree of the Ministers responsible for digital technology and finance attributions fixes the rates of duties, taxes and fees to be collected at the initiative of the ministry digital.

CHAPTER II: PUBLIC PROCUREMENT

Article 386.

The award of a public contract is, in addition to the provisions of this ordinance-law, governed in accordance with Law No. 10/010 of April 27, 2010 relating to public procurement.

Article 387.

The establishment of a public-private partnership in the digital sector is, in addition to the provisions of this ordinance-law, governed in accordance with law n°18/016 of July 9 2018 relating to public-private partnership.

CHAPTER III: TRANSITIONAL, REPEAL AND REVIVAL PROVISIONS FINALS

Article 388.

Digital service providers operating on the basis of titles obtained prior to this ordinance-law are required to comply with the new provisions of the this ordinance-law within six months of its entry into force.

Article 389.

All previous provisions contrary to this ordinance-law are repealed.

Article 390.

This ordinance-law comes into force on the date of its promulgation.

Done in Kinshasa, March 13, 2023

DETAILED PLAN OF THE CODE