| | |
|---|---|
| Jurisdiction | Côte d'Ivoire |
| Date | September 29th 2022 |
| Law Firm | Chauveau & Associés |
| Name and Position of the person in charge | Johana N'DIA-KRA, jurist |
| Contact Information | j.ndiakra@jfchauveau.com |

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

## Questionnaire

### I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the **private sector** at the present or in the near future?

Personal data processing in Côte d'Ivoire is governed by the Law n°2013-450 of 19 June 2013 on the protection of personal data and its implementing decree (the **"Personal Data Law"**).

The following are particularly subject to the provisions of the Personal Data Law, any collection, processing, transmission, storage and use of personal data by a natural person, the State, local authorities, legal persons under public or private law. The law applies to both the private and public sectors.

ii. Does your country have a general law concerning protection of personal information in the **public sector** at the present or in the near future?

See i. above.

iii. Does your country have laws concerning protection of personal information **which apply in individual (specific) sectors** at the present or in the near future? (If yes, please describe outline.)

Not applicable.

**Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.**

### II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I..( please add a reply column as necessary,)

The title of the law ： Law n°2013-450 of 19 June 2013 on the protection of personal data

| | |
|---|---|
| ① The definition of "Personal Information" | Any information that is related either to an identified or identifiable natural person by reference to either an identification number or specific elements that are peculiar to his/her physical, physiological, genetic, psychological, cultural, social or economic identity |
| ② The scope in which the law applies | - any collection, processing, transmission, storage and use of personal data by a natural person, the State, local authorities, legal persons governed by public or private law;<br>- any automated or non-automated processing of data contained or intended to be included in a file ;<br>- any data processing carried out on national territory ;<br>- any data processing concerning public security, defense, research, criminal offences investigation and prosecution or State security, subject to exemptions defined by specific provisions provided for by other law in force |
| ③ The territorial scope | Côte d'ivoire |
| ④ URL (please provide the URL officially posted by the government, English page is preferred, if available) | https://www.artci.ci/images/stories/pdf/lois/loi_2013_450.pdf |
| ⑤ The **effective** date * | 13 August 2013 |

* If the law has been amended, please fill in the effective date of the amended law.

ii. If there are any special instructions about the laws, please describe them.

Not applicable.

## III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

The collection, recording, processing, storage, transmission and interconnection of files of personal data must be done in a lawful and fair means (Art 15 of the Personal Data Law).

The processing of personal data is considered legitimate if the data subject expressly gives consent. However, this requirement of prior consent may be waived when the controller is duly authorized and the processing is necessary for:

- compliance with a legal obligation to which the controller is subject ;
- the performance of a task carried out in the public interest or within the exercise of public authority, which is entrusted to the controller or in a third party to whom the data are communicated ;
- the performance of a contract to which the data subject is a party or the performance of pre-contractual measures taken at the request of the data subject ;
- safeguarding the interests or fundamental rights and freedoms of the data subject ;

(Art 14 of the Personal Data Law)

The data controller is required to provide the person whose data are being processed, at the latest, at the time of collection and regardless of the means and supports used, with the following information:

- his or her identity and, where appropriate, that of his or her duly authorized representative ;
- the specific purpose(s) of the processing operation for which the data are intented ;
- the categories of data concerned ;
- the recipient(s) to whom the data may be disclosed ;
- the possibility of refusing to be included in the file in question ;
- the existence of a right of access to data concerning the person and a right to rectify such data ;
- the length of time the data will be kept ;
- the possibility of any transfer of data to third countries.

(Art 28 of the Personal Data Law)

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

Data must be collected for specific legitimate purposes and may not be further processed in a manner incompatible with these purposes.

Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.

Data must be kept for a period which does not exceed the period necessary for the purposes for which they were collected or processed.

Beyond this required period, the data may only be stored and kept only for the specific purpose of processing for historical, statistical or research purposes in accordance with legal provisions.

(Art 16 of the Personal Data Law)

The data collected must be accurate and, if necessary, updated.

Every reasonable measure must be taken to ensure that inaccurate or incomplete data, with regard to the purposes for which they are collected and further processed, are deleted or rectified.

(Art 17 of the Personal Data Law)

The principle of transparency implies compulsory and clear information from the data controller on personal data.

(Art 18 of the Personal Data Law)

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

See (b) above.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (c) Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

See (a) and (b) above.

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Personal data must be treated as confidential and protected, in particular where the processing of such data involves the transmission of data in a network.

(Art 19 of the Personal Data Law)

The data controller is required to take all precautions with regard to the nature of the data and, in particular, to prevent them from being distorted or damaged or that unauthorized third parties have access to it.

(Art 40 of the Personal Data Law)

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

The data controller shall keep a list of the processing operations carried out, which shall be immediately accessible to any person on request. The appointment of the correspondent by the controller shall be notified to the Data Protection Authority. It shall also be brought to the attention of the staff representative bodies, where appropriate.

(Art 12 of the Personal Data Law)

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;

at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Any natural person whose personal data are being processed may request in the form of questions and obtain from the person in charge of the processing:

- information enabling him/her to know about and challenge the processing ;
- confirmation as to whether or not personal data relating to him/her are being processed ;
- communication of the personal data concerning him or her and of any available information as to the origin of the data ;
- information as to the purposes of the processing, of the categories of personal data processed and the recipients or categories of recipients to whom the data are disclosed.

(Art 29 of the Personal Data Law)

Every natural person concerned has the right :

- to object, on legitimate grounds, relating to his or her particular situation, to the processing of personal data relating to him/her, except where the processing is expressly provided for by law. In the event of a legitimate objection, the processing carried out by the controller may not relate to the data in question;
- to object, at his/her request and free of charge, to the processing data concerning him/her for the purpose of canvassing ;
- to be informed before data relating to him/her are disclosed to third parties or used on behalf of third parties for canvassing purposes and to be expressly granted the right to object, free of charge, to such communication or use.

(Art 30 of the Personal Data Law)

Any natural person who can prove his identity may demand from the controller of a processing operation that, be rectified, completed, updated, blocked or deleted, as the case may be, if the personal data concerning them are

inaccurate, incomplete, equivocal, or outdated, or the collection, use, communication or conservation thereof is prohibited.
(Art 31 of the Personal Data Law)

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.
The Data Protection Authority may impose the following measures on data controllers

- a warning to the controller who does not comply with the obligations arising from the law

- a formal notice to cease the breaches observed within the time specified by the Authority

(Art 49 of the Personal Data Law)

The Data Protection Authority may, after having heard the data controller or his processor who does not comply with the provisions of the Personal Data Law and the formal notice sent to him, impose the following sanctions on him:

- the temporary withdrawal of the authorization granted,
- the definitive withdrawal of the authorization,
- a financial penalty proportional to the seriousness of the breaches committed and the benefits derived from the breach, the amount of which may not exceed XOF 10,000,000.

In the event of a repeated breach within 5 years of the date on which the financial penalty previously imposed became final, it may not exceed XOF 100,000,000 or, in the case of a company, it may not exceed 5% of the turnover excluding tax of the last financial year closed, up to a limit of XOF 500,000,000.

These administrative and financial sanctions are applied without prejudice to criminal sanctions.

(Art 51 of the Personal Data Law)

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle
Not applicable.

(b) Data Quality Principle
Not applicable.

(c) Purpose Specification Principle
Not applicable.

(d) Use Limitation Principle
Not applicable.

(e) Security Safeguards Principle
Not applicable.

(f) Openness Principle
Not applicable.

(g) Individual Participation Principle
Not applicable.

(h) Accountability Principle
Not applicable.

## IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as **comprehensive government access (e.g., limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the attorney-client privilege)** to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

Regarding the comprehensive government access, the requirement of prior consent of a data subject for processing his or her personal data may be waived where the controller is duly authorized and the processing is necessary for the performance of a task in the public interest or within the exercise of public authority, which is entrusted to the controller or the third party to whom the data are communicated (Art 14 of the Personal Data Law);

Please also note that the right to erasure of the data subject's personal data is not an absolute right and that it does not apply when data processing is necessary to comply with legal obligation or for the performance of a task carried out in the public interest or

in the exercise of official authority. (Art 14 of the Personal Data Law)
We are not aware of any safeguard for data subjects against each above and of any other law that allow public authorities to comprehensively access personal data held by the private sector or the public sector, which have an impact on the rights of data subjects.

Regarding Data Localization, our understanding of the Personal Data Law is that data must in principle be stored in Côte d'Ivoire. However, the Personal Data Law authorizes data controllers to transmit personal data to third countries, subject to such third countries providing a level of protection for personal data (especially protection of privacy, fundamental rights and freedoms) which is at least comparable (or higher) to the one granted by Ivorian laws. Please note that prior to any effective data transmission, the relevant data controller would need to obtain the Data Protection Authority (ARTCI)'s approval. (Art 26 + 7 of the Personal Data Law).

## V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Name: ARTCI
Address: 18 BP 2203 Abidjan 18 – Côte d'Ivoire
Telephone: +225 27 20 34 43 73
Website: www.autoritedeprotection.ci
Other information if any: Email: info-apdcp@artci.ci