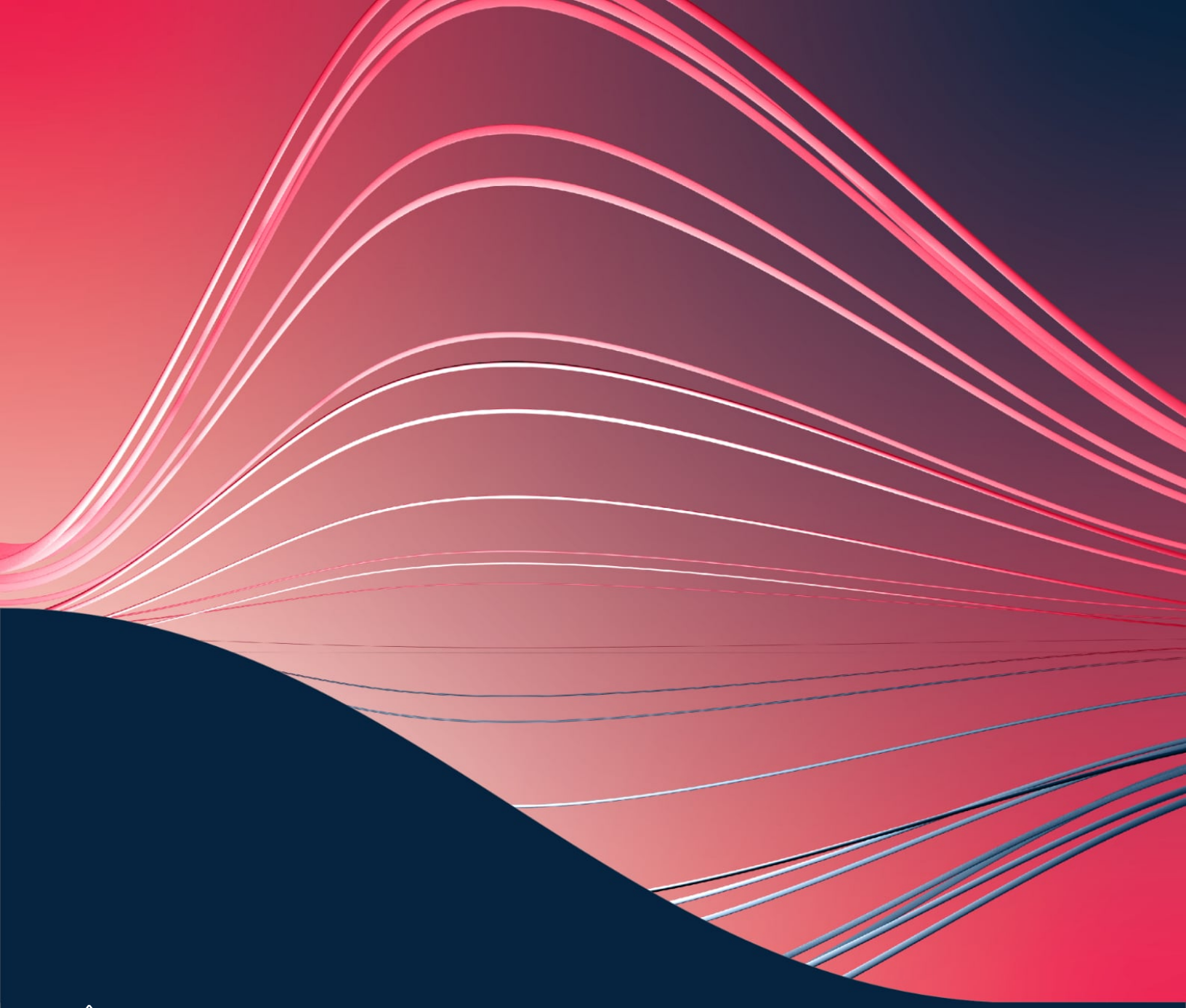

CÔTE D'IVOIRE

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 15th update of the Data Protection Laws of the World handbook. Data protection and privacy laws continue to evolve at pace, reflecting responses to technological change, increasing data-driven business models and heightened expectations around accountability and enforcement. Alongside jurisdiction-specific reform, a number of clear global trends are emerging, including increasing enforcement action, greater data localization and complexities with data transfers, and closer alignment between data protection, cybersecurity and wider digital regulation, all set within a backdrop of heightened geopolitical tensions. As a result, keeping track of developments across jurisdictions has become both more important and more challenging for organisations operating internationally.

Recent legislative and enforcement developments

This edition reflects another busy year for privacy and data protection, with new legislation taking effect in key markets such as India, while enforcement of established data protection laws, such as those in Europe, continues to be influenced by an increasingly complex geopolitical environment and escalating cyber threats.

Developments in the United States

In the United States, consumer privacy laws continue to rapidly develop at the state level, with the passage of more than 20 state comprehensive consumer privacy laws and increased state and multi-state enforcement. Recently, minor privacy laws have been passed and taken effect in a number of states, imposing privacy obligations and restrictions on websites and online services that provide services that are directed at minors under 18 years old or that collect personal information about known minors under 18 years old. In addition to increased regulator enforcement, privacy litigation is on the rise in the United States – key areas of focus for privacy litigation and class action risk include minor privacy and safety, online tracking, data breaches and cyber incidents, text marketing, and biometrics.

Responding to a rapidly evolving landscape

To support clients in navigating this fast-moving landscape, Data Protection Laws of the World will now be updated twice per year, reflecting the accelerating pace of reform within the data protection and privacy landscape and the growing need for up-to-date, practical insight.

Côte d'Ivoire

LAST MODIFIED 6 JANUARY 2025

Data protection laws

The data protection regime in Côte d'Ivoire is governed by the following laws and regulations:

- Law No. 2024-532 of June 6, 2024, on Electronic Communications
- Law no. 2013-546 of 30 July 2013 on electronic transactions
- Law no. 2013-451 of 19 June 2013 on the fight against cybercrime
- Law no. 2013-450 of 19 June 2013 on the protection of personal data
- Order no. 2012-293 of 21 March 2012 relating to telecommunications and information and communication technologies
- Decree No. 2015 -79 of 04 February 2015, laying down the procedures for filing declarations, submitting applications, granting and withdrawing authorizations for the processing of personal data
- Order No. 511/MPTIC/cab of 11 November 2014, defining the profile and setting the conditions of employment of the personal data protection correspondent
- Ratification of the African Union Convention on Cybersecurity and Protection of Personal Data

Definitions

Definition of personal data

According to Article 1 of the 2013-450 law on the protection of personal data, personal data is defined as:

> *'any information of any kind whatsoever and regardless of its medium, including sound and image relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, cultural, social or economic identification'.*

Definition of sensitive personal data

Article 1 of the 2013-450 law on the protection of personal data defines sensitive data as:

> *'any data relating to religious, philosophical, political or trade union opinions or activities, sexual or racial life, health, social measures, prosecutions or criminal or administrative sanctions.'*

National data protection authority

In Côte d'Ivoire, the Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) is the body responsible for protecting personal data. Created by Ordinance no. 2012-293 of 21 March 2012, ARTCI performs the duties of a personal data protection authority in accordance with Law no. 2013-450 of 19 June 2013.

According to Article 47 of this law, the ARTCI's main missions in terms of personal data protection are as follows:

- Inform data subjects and data controllers of their rights and obligations
- Respond to any request for an opinion on the processing of personal data
- Drawing up internal rules specifying the rules relating to deliberations, investigation and presentation of files
- Receive declarations and grant authorisations for the implementation of personal data processing or withdraw them in the cases provided for by law
- Receiving claims and complaints relating to the processing of personal data and informing the complainants of the action taken
- To inform the competent judicial authority without delay of any offences of which it becomes aware in the course of its duties
- To determine the essential guarantees and appropriate measures for the protection of personal data

- To carry out checks on any processing of personal data by sworn officials
- To impose administrative and financial penalties on data controllers who fail to comply with the provisions of the law
- To update and make available to the public a directory of personal data processing operations
- Advise persons and bodies carrying out personal data processing or carrying out tests or experiments in this area
- Giving its opinion on any draft legal text relating to the protection of freedoms and privacy
- To draw up rules of conduct relating to the processing and protection of personal data
- Participate in scientific research, training and study activities relating to the protection of personal data and, more generally, freedoms and privacy
- To authorise cross-border transfers of personal data, subject to certain conditions laid down by decree in the Council of Ministers
- Propose legislative or regulatory measures to adapt the protection of freedoms to developments in IT processes and techniques
- Set up cooperation mechanisms with the personal data protection authorities of other countries
- Participate in international negotiations on the protection of personal data
- To prepare and submit an annual activity report to the President of the Republic and the President of the National Assembly

Registration

These are the prior formalities that data controllers must complete before implementing certain types of data processing. These formalities may take the form of declarations or requests for authorisation, depending on the nature of the processing.

In principle, any processing of personal data is subject to prior declaration to the protection authority (article 5 of the 2013-450 Data Protection Act). The declaration must include detailed information about the processing, such as the identity of the person responsible, the purposes of the processing, the types of data processed, and the security measures put in place (article 9 of the aforementioned law).

However, certain types of processing are exempt from prior declaration under article 10 of the aforementioned law. These include:

- Processing carried out by a natural person in the exclusive context of his or her personal or domestic activities, provided that the data is not intended for systematic communication to third parties
- Processing for the sole purpose of keeping a register for exclusively private use
- Processing carried out by an association or non-profit-making body of a religious, philosophical, political or trade union nature, subject to certain conditions

- Processing of data concerning a natural person whose publication is required by law
- Processing operations for which the data controller has appointed a data protection correspondent, except in the event of data being transferred to a third country

As for Prior Authorisation in accordance with Article 7 of the aforementioned 2013 Act, it is required for Certain processing operations considered riskier for privacy. This concerns:

- Processing of genetic data and research in the field of health
- Processing of data relating to offences, convictions or security measures
- Processing of a national identification number or any other similar identifier, in particular telephone numbers
- Processing of biometric data
- Processing in the public interest, in particular for historical, statistical or scientific purposes
- The transfer of personal data to a third country
- The interconnection of files
- Processing carried out on behalf of the State: The processing of personal data carried out on behalf of the State, a public establishment or a local authority, or a legal person under private law managing a public service shall be decided by legislative or regulatory act adopted after a reasoned opinion from the national data protection authority (article 13)
- Transfers of personal data to a third country

Registration process

- The declaration or request for authorisation may be sent to the protection authority electronically, by post or by any other means against delivery of an acknowledgement of receipt (in accordance with Article 10 of the aforementioned Act).
- ARTCI must give its decision within one month of receipt of the declaration or request for authorization. This period may be extended by a further month. Failure to respond within the time limit is equivalent to a rejection 'Article 5 of Decree No. 2015 -79 of 04 February 2015, laying down the procedures for filing declarations, submitting applications, granting and withdrawing authorizations for the processing of personal data.
- For the most common categories of processing, the ARTCI may establish standards to simplify or exempt from the declaration obligation.
- Once the declaration has been made, the data protection authority issues a receipt, which may be issued electronically. The applicant may then begin processing but remains responsible for compliance with the law.

Data protection officers

Obligation to designate a CPDCP

- According to Article 5 of Law 2013-450, the processing of personal data is subject to a prior declaration to the ARTCI. However, this obligation to declare may be waived if the controller designates a CPDCP, except in the case of the transfer of personal data to a third country. The designation of a CPDCP is therefore a choice that exempts the declaration, and not a legal obligation (Article 6 of the aforementioned law).
- When the data controller opts to designate a CPDCP, it must notify the ARTCI of this designation (Article 6 of the Order on the correspondent's profile).
- The CPDCP is responsible for independently ensuring compliance with the legal obligations relating to the protection of personal data.

Qualifications required for the CPDCP

- Law no. 2013-450 stipulates that the CPDCP must have the necessary qualifications to carry out his or her duties.
- Order No. 511/MPTIC/CAB of 11 November 2014 specifies the profile required for the CPDCP, which differs depending on whether it is a natural or legal person:
  - For natural persons:
    - Be of Ivorian nationality (implied)
    - Have at least a BAC+4 level in the fields of legal sciences, computer science or telecommunications/ICT networks, or an equivalent diploma
    - At least two years' professional experience in these fields
    - Proven competence in personal data protection
    - Have a good knowledge of database management and operating systems, data storage methods and information systems security policies
    - Mastery of office automation tools and the internet
    - Excellent interpersonal and organisational skills
    - Not to have been the subject of a final criminal conviction or a ban on exercising an activity, handed down by an Ivorian or foreign court, or of a sanction handed down by ARTCI
  - For legal entities:
    - Be a legal person under Ivorian law
    - Prove that they are tax-compliant and that they are registered with social security institutions
    - Have been active for at least five years in the fields of legal sciences, information technology or telecommunications/ICT networks, and provide proof of this
    - Have insurance covering professional risks relating to the protection of personal data
    - Have staff with at least the profile of a CPDCP, natural person

It is important to note that the controller cannot be designated as a CPDCP.

A natural person CPDCP can only be designated by a single controller and carry out his duties only with the latter. On the other hand, a legal entity may be appointed by several data controllers.

Duties of the CPDCP

The CPDCP is responsible for ensuring, in an independent manner, compliance with the legal obligations relating to the protection of personal data.

Its main missions, defined by Law No. 2013-450, and specified by Order No. 511/MPTIC /CAB include:

- Maintaining the list of data processing carried out
- Keeping a copy of the codes and passwords required to access files relating to processing
- Provide access to data to any data subject who requests it in order to exercise their rights
- To ensure compliance with legislation on the protection of personal data
- To inform and advise the data controller and employees on legal obligations in relation to data protection
- Notify the data controller of any breaches of legislation observed
- Notify the ARTCI of uncorrected breaches within three months of reporting to the controller
- Notify the ARTCI of any difficulties encountered in carrying out its duties

Other important elements

- The appointment of the CPDCP must be notified to the ARTCI.
- The ARTCI has 30 days to object to the designation if the CPDCP does not meet the required profile.
- The CPDCP may not be sanctioned by his employer for the performance of his duties.
- The controller may replace the CPDCP for a legitimate reason, after informing the CPDCP and giving him/her the opportunity to present his/her observations. The replacement must also be notified to the ARTCI.
- Decree No. 2015-79 specifies that applications to file a declaration and authorisation for the processing of personal data must be submitted by a natural person resident in Côte d'Ivoire or a legal person under Ivorian law.

Collection and processing

Data collection

- Data must be collected in a lawful, fair and non-fraudulent manner Article 15 of Law 2013-450.

- Data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes.
- The controller must inform the data subject, at the latest at the time of collection of the data, of his identity, the purposes of the processing, the categories of data collected, the recipients, the storage period and his rights (Article 28).
- The consent of the data subject is generally required for the collection and processing of data (Article 14). This consent must be explicit, unequivocal, free, specific and informed.
- There are exceptions to consent where processing is necessary to comply with a legal obligation, to perform a task in the public interest, to perform a contract, or to safeguard the vital interests of the data subject.

Data processing

- Data processing must be carried out in accordance with established principles.
- Data must be adequate, relevant and not excessive in relation to the purposes for which it is collected.
- Data processing must be confidential and carried out exclusively by persons acting under the authority of the data controller and only on its instructions.
- The data controller must take all necessary precautions to prevent the data from being distorted, damaged or accessed by unauthorised third parties. He must also choose a processor who provides sufficient guarantees.
- Sensitive data is subject to specific rules. Their collection and processing are generally prohibited except in certain cases (explicit consent, safeguarding vital interests, etc.).
- Personal data must not be kept beyond the period necessary for the purposes for which it was collected and processed.
- The data controller must guarantee that the data can be used regardless of the technical medium used.

Data processing

- Data processing must be carried out in accordance with the established principles (Articles 14 et seq. of the 2013-450 Law).
- Data must be adequate, relevant and not excessive with regard to the purposes for which they are collected (Article 15).
- Data processing must be confidential and carried out exclusively by persons acting under the authority of the data controller and only on its instructions (Article 39).
- The data controller must take all necessary precautions to prevent the data from being distorted, damaged or accessed by unauthorised third parties. He must also choose a processor who provides sufficient guarantees (Article 40).
- Sensitive data is subject to specific rules. According to Article 13, Their collection and processing are generally prohibited except in certain cases (explicit consent, safeguarding vital interests, etc.).

- Personal data must not be kept beyond the period necessary for the purposes for which they were collected and processed (Article 16).
- The controller must ensure that the data can be used regardless of the technical medium used (Article 44).

Transfer of personal data

The principle in this area is that the transfer of data to a third country is only authorised if that State ensures a level of protection of privacy, freedoms and fundamental rights that is greater than or equivalent to that in force in Côte d'Ivoire (article 26 of Law 2013-450).

Article 26 also states that prior to any actual transfer of personal data to a third country, the data controller must obtain prior authorisation from ARTCI.

This authorization is required even if the third country is considered to have an adequate level of protection.

The application for authorization must be submitted by a legal entity under Ivorian law (Article 7 of the 2015 Decree).

According to the said Article 7, the authorization application must include several elements, including:

- The identity and address of the data controller and, where applicable, its representative
- The nature of the data involved
- The reason for and purposes of the transfer
- The guarantees of protection, conservation, confidentiality of the data and respect for the rights of the data subjects
- The name of the country hosting the transferred data and the legal framework relating to personal data applicable in that country
- The methods of transmission of the data concerned
- The guarantee of unhindered access to the transferred data by the data subject and by the Ivorian public authorities

According to Article 8 of the Decree, data transfers to third countries are subject to regular monitoring by ARTCI, particularly about their purpose. The ARTCI may set up cooperation mechanisms with the data protection authorities of the main host countries. The data controller must draw up and submit to ARTCI an annual activity report on the transfer of data to third countries.

Security

Law No. 2013-450 of 19 June 2013 on the Protection of Personal Data requires data controllers to implement appropriate security measures to safeguard personal data against any form of breach.

According to **Article 39** of the law, the processing of personal data must remain confidential and should only be carried out by individuals acting under the authority of the data controller or their processor, and strictly in accordance with their instructions.

Furthermore, **Article 40** specifies that the data controller is required to take all necessary precautions, taking into account the nature of the data and the risks posed by processing, to ensure the security of the data. This includes preventing them from being altered, damaged, or accessed by unauthorised third parties. The controller must also implement technical and organisational measures to protect the data against destruction, loss, alteration, unauthorised disclosure, or access. These measures include securing facilities, controlling access, verifying the identity of third parties, and backing up the data.

In the event of non-compliance with these obligations, the data controller may face various types of sanctions, as provided for in **Articles 49 and subsequent** of the 2013-450 law on the protection of personal data:

- **Warning**: The data protection authority may issue a formal warning to the controller for failing to meet their obligations.
- **Formal Notice**: The authority may serve notice on the controller to rectify the identified breaches within a set timeframe.
- **Administrative and Financial Sanctions**: If the controller fails to comply with the formal notice, the authority may revoke the authorisation temporarily or permanently and impose a financial penalty proportional to the severity of the breach.
- **Interruption of Processing, Locking of Data, or Prohibition of Processing**: In urgent cases where processing causes a violation of rights and freedoms, the authority may order the suspension of data processing, locking of specific data, or a ban on processing activities.
- **Criminal Sanctions**: Criminal penalties apply for serious breaches, such as processing sensitive data without authorisation (e.g., racial origin, political opinions, religious beliefs), direct marketing without prior consent, or obstructing the authority's work.
- **Civil Liability**: The controller may also be held liable for damages caused to affected individuals due to non-compliance with their obligations, as stipulated in **Article 5 of the African Union Convention on Cybersecurity and Personal Data Protection.**

Breach notification

There is no legal requirement to notify data breaches to ARTCI.

Enforcement

Here are some relevant decisions from the ARTCI:

- Decision No. 2024-1002 – GCB Cocoa Trading Côte d'Ivoire

- Decision No. 2024-1001 – GCB Cocoa Trading Côte d'Ivoire
- Decision No. 2024-0999 – GCB Cocoa Côte d'Ivoire
- Decision No. 2024-0998 – GCB Cocoa Côte d'Ivoire
- Decision No. 2024-0997 – GCB Cocoa Côte d'Ivoire
- Decision No. 2024-0996 – Ministry of Technical Education, Vocational Training and Apprenticeship and KAYDAN GROUP
- Decision No. 2023-0981 – OCEANA
- Decision No. 2023-0881 – Capital Asset Management West Africa
- Decision No. 2023-0970 – NSIA Banque CI
- Decision No. 2023-0964 – Blommer Chocolate Company

Electronic marketing

The data must be collected lawfully, fairly, and for specific, explicit, and legitimate purposes (Article 15 of the Law on the Protection of Personal Data).

The data subject may freely object to the use of their data for prospecting activities, including electronic marketing, in accordance with Article 30 of the Law on the Protection of Personal Data. This right must be explicitly brought to the attention of the data subject.

However, the data controller may refuse an objection if there are compelling legitimate reasons justifying the processing, as provided in Article 30 of the Law on the Protection of Personal Data.

Online privacy

The Law does not provide any specific rules for governing cookies and location data.

However, pursuant to Article 40 and sq. of the data law mentioned above, data controller must implement all appropriate technical and organizational measures to preserve the security and confidentiality of the data, including protecting the data against accidental or unlawful destruction, accidental loss, alteration, distribution or access by unauthorised persons.

Data protection lawyers

Louis Thierry Dadje
Senior Associate
Geni & Kebe
t.dadje@gsklaw.sn
View bio

Foungnigué Alassane Ouattara
Counsel
Geni & Kebe
a.ouattara@gsklaw.sn

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:

Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com