The Governing privacy Laws of this website are that of Federal Republic of Nigeria Privacy Law and the United State of America

Any claim relating to the Province of St. Joseph the worker Nigeria and Ghana, website shall be governed by the Privacy laws of the Federal Republic of Nigeria and the United State of America without regard to its conflict of law provisions.

Website Terms and Conditions of Use

1. Terms

By accessing this web site, you are agreeing to be bound by these web site Terms and Conditions of Use, all applicable laws and regulations, and agree that you are responsible for compliance with any applicable local laws. If you do not agree with any of these terms, you are prohibited from using or accessing this site. The materials contained in this web site are protected by applicable copyright law.

2. Disclaimer

1. The materials on the Province of St. Joseph the Worker Nigeria and Ghana website are provided "as is". Province of St. Joseph the Worker Nigeria and Ghana makes no warranties, expressed or implied, and hereby disclaims and negates all other warranties, including without limitation, implied warranties or conditions of merchantability, fitness for a particular purpose, or non-infringement of intellectual property or other violation of rights. Further, the Province of St. Joseph the Worker Nigeria and Ghana does not warrant or make any representations concerning the accuracy, likely results, or reliability of the use of the materials on its Internet web site or otherwise relating to such materials or on any sites linked to this site.

3. Limitations

In no event shall Dominican Province of St. Joseph the worker Nigeria and Ghana or its suppliers be liable for any damages (including, without limitation, damages for loss of data or profit, or due to business interruption,) arising out of the use or inability to use the materials on

Province of St. Joseph the Worker Nigeria and Ghana Internet site, even if Province of St. Joseph the Worker Nigeria and Ghana or a Province of St. Joseph the Worker Nigeria and Ghana authorized representative has been notified orally or in writing of the possibility of such damage. Because some jurisdictions do not allow limitations on implied warranties, or limitations of liability for consequential or incidental damages, these limitations may not apply to you.

4. Revisions and Errata

The materials appearing on this website of the St. Joseph the worker Nigeria and Ghana could include technical, typographical, or photographic errors. Province of St. Joseph the Worker Nigeria and Ghana does not warrant that any of the materials on its web site are accurate, complete, or current. St. Joseph the worker Nigeria and Ghana may make changes to the materials contained on its web site at any time without notice. Dominican friars of Nigeria and Ghana does not, however, make any commitment to update the materials.

5. Links

The Province of St. Joseph the Worker, Nigeria and Ghana has not reviewed all of the sites linked to its Internet web site and is not responsible for the contents of any such linked site. The inclusion of any link does not imply endorsement by Province of St. Joseph the Worker Nigeria and Ghana of the website. Use of any such linked web site is at the user's own risk.

6. Site Terms of Use Modifications

The Dominican Friars of Province of St. Joseph the Worker, Nigeria and Ghana may revise these terms of use for its web site at any time without notice. By using this website you are agreeing to be bound by the then current version of these Terms and Conditions of Use.

General Terms and Conditions applicable to Use of a Web Site.

Privacy Policy of this Website relates to the Province of St. Joseph the worker Nigeria and Ghana.

1. General

Your privacy is very important to us. Accordingly, we have developed this Policy in order for you to understand how we collect, use, communicate and disclose and make use of personal information. The following outlines our privacy policy.

- Before or at the time of collecting personal information, we will identify the purposes for which information is being collected.
- We will collect and use of personal information solely with the objective of fulfilling those purposes specified by us and for other compatible purposes, unless we obtain the consent of the individual concerned or as required by law.
- We will only retain personal information as long as necessary for the fulfillment of those purposes.
- We will collect personal information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.
- Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.
- We will protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
- We will make readily available to customers information about our policies and practices relating to the management of personal information.

We are committed to conducting our business in accordance with these principles in order to ensure that the confidentiality of personal information is protected and maintained.

2. Cookies

The Province of St. Joseph the worker Nigeria and Ghana and its service providers may use Cookies (as defined below), local browser storage, web beacons, pixels, tags and other automated information gathering technologies to track your behavior and interaction on this website and other Internet properties operated by us or by our service providers on our behalf.

For example, we and our service providers collect how, when, and which parts of our sites or Internet properties and their features you use.

A “Cookie” is a small amount of data a website operator, or a third party whose content is embedded in that website, may store in your web browser and that the website operator or, as applicable, the third party, can access when you visit the website. A Cookie may also refer to web-browser-based storage provided by Adobe’s Flash plugin (a “Flash Cookie”). A web beacon, pixel or tag is a small, usually-transparent image placed on a web page that allows the operator of that image, which may be the operator of the website you visit or a third party, to read or write a Cookie.

Your operating system and web browser may allow you to erase information stored in Cookies, Flash Cookies, and local browser storage. But if you do so, you may be forced to login to our website again and you may lose some preferences or settings. You may also be able to set your browser to refuse all website storage or to indicate when it is permitted, but some features of our websites may not function properly without it. We and our service providers may use Cookies to keep you logged in, save your preferences, collect information about how you use our websites, and improve our websites and services and your user experience.

In addition, we or our service providers may use Cookies or other automated information gathering technologies to associate your behavior or interaction on one website operated by us or on our behalf (for example, features or content that you view or click on) with what you do on another of our sites or properties, and we or our service providers may associate this information with personal information you have provided to us in order to better understand your interests and preferences and to send you e-mail and other communications that are tailored to your interests. You can stop this tracking across our sites by modifying your web browser’s settings, as mentioned earlier.

More information about managing Cookies is available here. Cookie management tools provided by your browser may not affect Flash Cookies. More information about managing Flash Cookies is available here. To learn how to manage privacy and storage settings for your local browser storage, please refer to the end user documentation for your browser.

Federal Republic of Nigeria Privacy Law

Principal regulation

Data Protection Act

The Act has been enacted to safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria. Among other things, the objective of the Act include: the protection of personal information; establishing the Nigeria Data Protection commission for the regulation of the processing of personal information; promoting data processing practices that safeguard the security of personal data and privacy of data subjects; protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights; and strengthening the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data etc. The Data Protection Act received Presidential assent on 13 June 2023.

Subsidiary legislation

Nigeria Data Protection Regulation

The personal and territorial scope of the NDPR is defined by citizenship and physical presence. It applies to residents of Nigeria, as well as Nigerian citizens abroad. The NDPR provides legal safeguards for the processing of personal data. Under the NDPR, Personal Data must be processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject.

Implementation Framework for the Nigeria Data Protection Regulation

The Framework builds on the NDPR to ensure a tailored implementation of the data protection regime in Nigeria. It serves as a guide to data controllers and administrators / processors to understand the standards required for compliance within their organisations. The Framework is to be read in conjunction with the NDPR and does not supersede the NDPR.

Guidelines for the Management of Personal Data by Public Institutions in Nigeria

The Guidelines apply to all public institutions (PIs) in Nigeria, including ministries, departments, agencies, institutions, public corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the Federal, State or Local levels, that process the personal data of a data subject. The Guidelines mandate all PIs to protect personal data in any incidence of processing of such data. Processing in this context retains the same meaning it has under the NDPR. All forms of personal data of a Nigerian citizen, resident or non-Nigerian individual that has interactions with PIs, or such PIs have access to the personal data in furtherance of a statutory or administrative purpose, are to be protected in accordance with the NDPR or any other law or regulation in force in Nigeria.

Sectoral laws

In addition to the principal legislation mentioned, the Constitution of the Federal Republic of Nigeria and various sector-specific laws make different provisions for privacy and data protection matters. Key provisions in the mentioned laws are outlined hereunder:

The laws

Constitution of the Federal Republic of Nigeria 1999 (As Amended)

The Nigerian Constitution provides Nigerian citizens with a fundamental right to privacy. Section 37 of the Constitution guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. The Constitution does not define the scope of "privacy" or contain detailed privacy provisions.

Child Rights Act 2003

The Child Rights Act 2003 reiterates the constitutional right to privacy as relates to children. Section 8 of the Act guarantees a child's right to privacy subject to parent or guardian rights to exercise supervision and control of their child's conduct. Some Nigerian states have also enacted Child Rights Laws. Under the Act / Laws, age of a child is any person under the age of 18.

Consumer Code of Practice Regulations 2007 (NCC Regulations)

The Nigerian Communications Commission (NCC) issued the NCC Regulations which requires all licensees to take reasonable steps to protect customer information against improper or accidental disclosure, and ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information to any party except to the extent agreed with the customer, as permitted or required by the NCC or other applicable laws or regulations.

Consumer Protection Framework 2016 (Framework)

The Consumer Protection Framework 2016 was enacted pursuant to the Central Bank of Nigeria Act 2007. The Framework includes provisions that prohibit financial institutions from disclosing customers' personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

Credit Reporting Act 2017

The Credit Reporting Act establishes a legal and regulatory framework for credit reporting by Credit Bureaus. Section 5 of the Act requires Credit Bureaus to maintain credit information for at least 6 years from the date that such information is obtained, after which the information must be archived for a 10-year period prior to its destruction. Section 9 of the Act provides the rights of data subjects (i.e. persons whose credit data are held by a Credit Bureau) to privacy, confidentiality and protection of their credit information. Section 9 further prescribes conditions under which the credit information of the data subject may be disclosed.

Cybercrimes (Prohibition, Prevention Etc) Act 2015

The Cybercrimes (Prohibition, Prevention Etc) Act provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. The Act

requires financial institutions to retain and protect data and criminalizes the interception of electronic communications.

Freedom of Information Act, 2011 (FOI Act)

The FOI Act seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc.).

National Identity Management Commission (NIMC) Act 2007

The NIMC Act creates the National Identity Management Commission (NIMC) to establish and manage a National Identity Management System (NIMS). The NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers to qualified citizens and legal residents. Section 26 of the NIMC Act provides that no person or corporate body shall have access to data or information in the Database with respect to a registered individual without authorization from the NIMC. The NIMC is empowered to provide a third party with information recorded in an individual's Database entry without the individual's consent, provided it is in the interest of National Security.

National Health (NH) Act 2014

The NH Act provides rights and obligations for health users and healthcare personnel. Under the NH Act, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NH Act further imposes restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NH Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

The NH Act provides rights and obligations for health users and healthcare personnel. Under the NH Act, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NH Act further imposes

restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NH Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011

Section 9 and 10 of the Nigerian Communications Commission Regulation provides confidentiality for telephone subscribers records maintained in the NCC's central database. The Regulation further provides telephone subscribers with a right to view and update personal information held in the NCC's central database of a telecommunication company in camera.

United States Privacy Law

United States privacy law is a complex patchwork of national, state and local privacy laws and regulations. There is no comprehensive national privacy law in the United States. However, the US does have a number of largely sector-specific privacy and data security laws at the federal level, as well as many more privacy laws at the state (and local) level. In recent years, beginning with California, states have begun to introduce their own comprehensive privacy laws, and other states are expected to follow and enact their own comprehensive state privacy laws. Although a bipartisan draft bill (the 'American Data Privacy and Protection Act') was introduced in 2022, several senators were in opposition of the bill, and comprehensive privacy law on the federal level is not expected to pass any time soon.

Federal and State Privacy Laws and Regulations

Federal laws and regulations include those that apply to financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, children's privacy, telemarketing, email marketing and communications privacy laws.

There are also a number of state privacy and data security laws that overlap with federal law—some of these state laws are preempted in part by federal laws, but others are not. US states have also passed privacy and data security laws and regulations that apply across sectors and go beyond federal law—such as data security laws, secure destruction, Social Security number privacy, online privacy, biometric information privacy, and data breach notification laws. Generally, each state's laws apply to personal information about residents of that state or activities that occur within that state. Thus, many businesses operating in the United States must comply not only with applicable federal law, but also with numerous state privacy and security laws and regulations.

For example, California alone has more than 25 state privacy and data security laws, including the California Consumer Privacy Act (CCPA) and its regulations as recently amended by the California Privacy Rights Act (CPRA), collectively referred to as the CCPA. The CCPA, as amended, introduced additional definitions and individual rights, and imposed additional

requirements and restrictions on the collection, use and disclosure of personal information. The CCPA is also unique among state comprehensive privacy laws in that, as of January 1, 2023, it applies to HR and B2B personal information. Enforcement of the CPRA amendments to the CCPA commenced on July 1, 2023 for violations of the new provisions that occur on or after that date.

Notably, updated CCPA regulations based on the CPRA amendments were finalized on March 29, 2023, with enforcement by the California Attorney General and the newly established California Privacy Protection Agency ('CPPA' or 'Agency') expected to begin on July 1, 2023. However, following a suit filed by the California Chamber of Commerce, the Sacramento district court ruled that the Agency was required to give businesses 12-months between finalizing a CCPA regulation and commencing enforcement, effectively delaying enforcement of the amended regulations to March 29, 2024. This delay does not affect the Agency or the California Attorney General's ability to enforce the version of the CCPA amended by the CPRA (effective July 1, 2023) or the existing (i.e., pre-2023-amendment) CCPA regulations (effective August 14, 2020).

In late 2022, the California legislature also passed the California Age-Appropriate Design Code, which was slated to take effect July 1, 2024 and would apply to companies that meet the definition of "business" under the CCPA and that provide online services that are likely to be accessed by individuals under 18 years of age. However, on September 18, 2023, a California District Court issued an injunction blocking the law from coming into effect on First Amendment grounds. Following an appeal to the Ninth Circuit by the California Attorney General's office, the fate of the law is currently uncertain. More information on the California Age-Appropriate Design Code can is available at ***https://www.dlapiper.com/en-us/insights/publications/2023/05/californias-age-appropriate-design-code-act***

Beyond California, Colorado's Attorney General finalized the Colorado Privacy Act (CPA) Rules on March 15, 2023, which add significantly to the CPA's obligations on businesses. Both the CPA and the CPA Rules went into effect July 1, 2023. Connecticut, Utah, and Virginia's privacy laws also took effect in 2023.

While not identical, the Colorado, Connecticut, Utah, and Virginia state privacy laws are substantially similar to each other in most key aspects. Further, unlike the CCPA, all are also generally inapplicable to personal information collected about, and processed in the context of, employee and business relationships. On the other hand, while the CCPA has some practical similarities with these state laws, it adopts more granular definitions, requirements, and restrictions that vary considerably from these laws, and, notably, applies to personal information collected from California residents in employment and B2B contexts.

2023 brought a significant development in the health data space, with Washington passing the My Health My Data Act (MHMD). The law ostensibly applies only to consumer health data, but its exceptionally broad definitions and scope combined with its private right of action may mean its enforcement touches on data many companies may not typically consider "health" data. More information on the MHMD Act is available at ***https://www.dlapiper.com/en/insights/publications/2023/04/washington-state-passes-my-health-my-data-act***

Finally, the pace of state privacy legislation accelerated in 2023 overall, with the following states passing their own comprehensive privacy laws or variations thereof:

- Florida (effective July 1, 2024)
- Oregon (effective July 1, 2024)
- Texas (effective July 1, 2024)
- Montana (effective Oct. 1, 2024)
- Delaware (effective Jan. 1, 2025)
- Iowa (effective Jan. 1, 2025)
- Tennessee (effective Jan. 1, 2025)
- New Jersey (effective Jan. 15, 2025)
- Indiana (effective Jan. 1, 2026)

More information on the US state privacy laws is available at ***https://privacymatters.dlapiper.com/state-privacy-laws/***

Enforcement of Unfair and Deceptive Trade Practices

In the United States, consumer protection laws, which prohibit unfair and deceptive business practices, provide another avenue for enforcement against businesses for their privacy and security practices.

At the federal level, the US Federal Trade Commission (FTC) uses its authority to protect consumers against unfair or deceptive trade practices, to take enforcement actions against businesses for materially unfair privacy and data security practices. The FTC uses this authority to, among other things, take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate or misleading privacy and security statements, including in privacy policies
- Failing to abide by applicable industry self-regulatory principles
- Transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or M&A transaction, in a manner not expressly disclosed on the applicable consumer privacy policy
- Violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of standards established in their prior enforcement precedents

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. State attorneys general also sometimes work together on enforcement actions against companies for actions that broadly affect the consumers of multiple states (such as data breaches).

Privacy class actions also continue to be a key risk area in the United States, including in the context of biometric privacy (under the Illinois Biometric Privacy Act), text messaging (under the federal Telephone Consumer Privacy Act) and call recording, wiretapping and related claims under the California Invasion of Privacy Act and other state laws. Online monitoring and targeting activities—including via cookies, pixels, chat bots, and so-called “session replay” tools—are an area of particular focus in the United States from a regulator and enforcement perspective and are also a developing litigation risk area.