



DATA PROTECTION AND CYBERSECURITY TOOLKIT

Supported by CIPESA





About Tech Hive™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm that works with private and public organisations on issues involving technology, business, and law. As an innovation partner, we help our clients get ready for and adjust to how new technologies change and affect long-standing practices.

Our experience and capability extend across Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Regulatory Intelligence, Start-Up Advisory, and Digital Health. We make sure that our advice helps our clients by knowing their business and the markets in which they work. We do this by keeping track of policy and legislative changes and gathering accurate intelligence on them.

Contact: contact@techhiveadvisory.org.ng



About Ikigai Innovation Initiative

The Ikigai Innovation Initiative, or "Ikigai," is a non-profit organisation that was set up to be Africa's one-stop shop for technology policy. We promulgate diverse research on technology policy and legal frameworks across Africa. We also talk to the right people about how the law, business, and technology interact and push for better policies for the ecosystem as a whole.

As a research centre focused on emerging technologies, policy, and research, we often collaborate with leading research institutes, academia, organisations, civil society, and individuals on policy affecting technology. We also publish whitepapers, reports, policy briefs, infographics, how-to guides, academic journals, and other publications, and we contribute to them.

Contact: policy@ikigaination.org



About CIPESA

The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) is one of two centres established under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was funded by the UK's Department for International Development (DfID). CIPESA focuses on decision-making that facilitates the use of ICT in support of development and poverty reduction.

Since inception, CIPESA has positioned itself as a leading centre for research and analysis of information aimed to enable policy makers in the region to understand ICT policy issues, and for various multi-stakeholders to use ICT to improve livelihoods. We produce and publish commentaries, briefing papers and newsletters that are widely circulated. Our commentaries – short and informative pieces aimed at sparking thinking and dialogue – provide an overview of selected international ICT policy and Information Communication Technology for Development (ICT4D) issues relevant to African stakeholders.

Disclaimer - Usage of the Toolkit

This toolkit is both general and educational. It is not meant to be a source of legal or technical advice, and you should not use it as such. The toolkit's information and materials may not apply in all (or any) situations. So, you should not act on them without getting specific legal or technical advice based on your situation.

The tools suggested in this toolkit are merely suggestions on how to improve your privacy and security posture as a business.

The absence of any trademark or service mark from this list does not waive Tech Hive and Ikigai's intellectual property rights in that name, mark, or logo.

All rights reserved. © 2022 Tech Hive Advisory and Ikigai Innovative Initiative.

Copyright © Tech Hive Advisory Limited and Ikigai Innovation Initiative 2022. This publication is the copyright of Tech Hive Advisory and Ikigai Innovation Initiative. Without Tech Hive and Ikigai's permission, no part of this document may be copied, reproduced, scanned into an electronic system, sent, forwarded, or distributed.

Acknowledgement

This toolkit was developed with the support of the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

We thank all the contributors for their valuable contributions towards the development of this toolkit.



Table of Contents

Content
Introduction
Section A - Data Protection
Legal Framework
Definition of terms
Obligations under the law
Privacy Implementation Tips
Conclusion
Section B - Cybersecurity
Legal Framework
Definition of terms
Cybersecurity Threats
Cybersecurity Vulnerabilities
What to do to ensure you are cybersmart?
Conclusion
Resources

Introduction

Tech Hive Advisory and Ikigai Innovation Initiative made this toolkit to help private businesses in Nigeria, especially those run by women, learn about data protection and cybersecurity and find resources that they can use.

According to the Global Entrepreneurship Monitor, Nigeria has the highest number of female entrepreneurs globally. There are over 41 million small and medium-sized enterprises (SMEs), with women accounting for 40% of this total. Globally, nine out of every ten businesses fail because of problems like lack of business and leadership skills, lack of family support, lack of access to resources, poor infrastructure, discrimination, fraud attacks, and lack of information.

Because of this, female entrepreneurs in Nigeria often face business stagnation, problems with not following the rules, phishing, targeted online fraud and scams, and data breaches, among other problems. For example, it is common for businesses on social media sites like Facebook, Instagram, and Twitter to lose access to their accounts after being phished, or tricked into clicking on a link they did not know about. In the same way, businesses process their clients' data, sometimes without knowing or caring about the rules of data processing. This makes it easy for people's online rights to be violated by accident. Based on this, they are likely to be targets of cyberattacks because of their lack of security infrastructure.

Through this toolkit, we hope to raise awareness of compliance requirements and encourage better online business practices and interactions between businesses and customers. This will help the digital economy grow and help women-owned businesses grow on a larger scale.

While using this toolkit, keep in mind that every situation and circumstance differs. You will need to be able to ascertain what works for you and applies to your business at any point in time.



Section A – Data Protection

The first thing you need to understand is the concept of data protection. What does “data protection” mean?

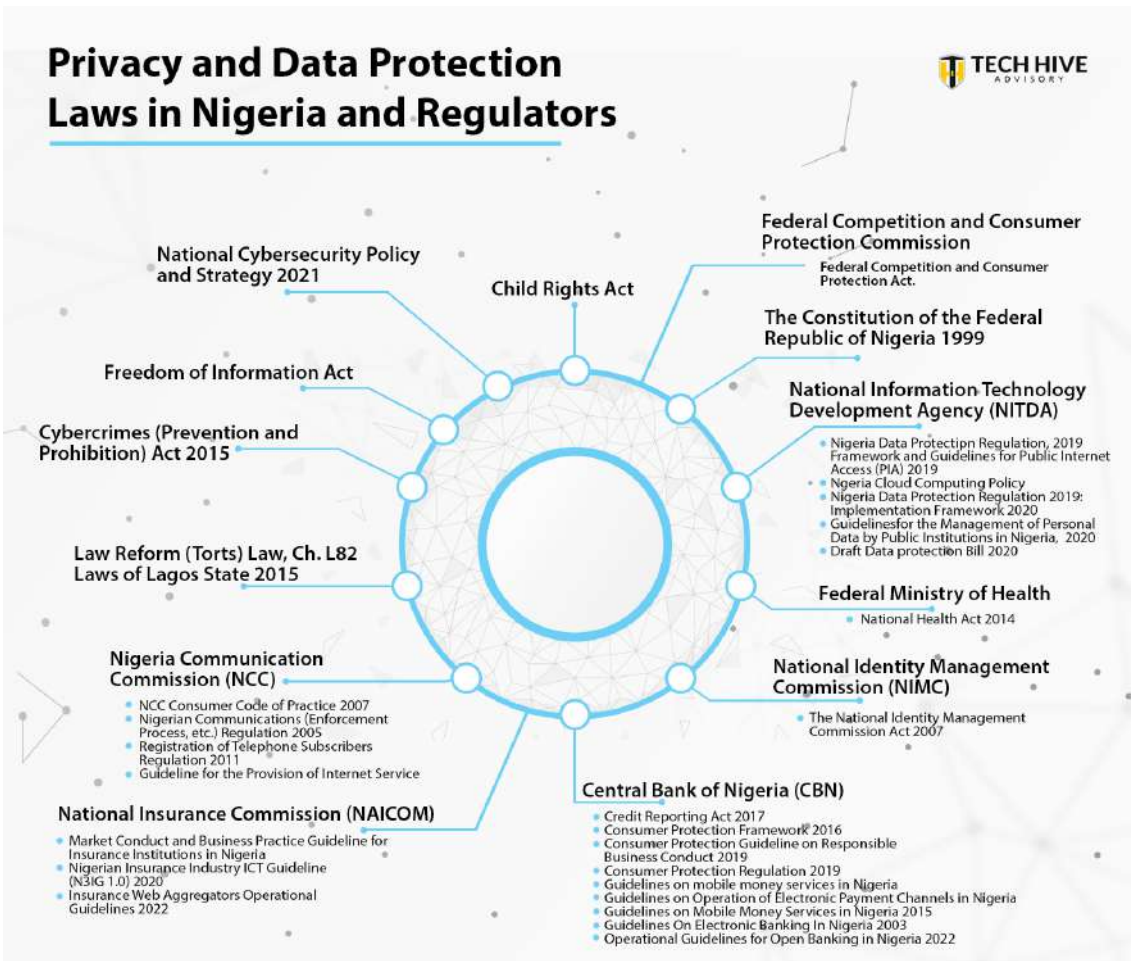
Data protection means keeping people's personal information safe from things like loss, corruption, compromise, abuse, or misuse, among other risks or harms. It is a human right. For instance, let's say Tomi, a person or customer, buys something from you, the business owner. In the process, Tomi gives you her home address (personal data) because she prefers to have the item delivered rather than pick it up from your store. It is your job to make sure that Tomi's information (like her home address), which she gave you, is kept safe from people who might want to use it maliciously or stalk her. You cannot use her phone number, email address, or other information she has given you to send her advertisements unless she has given you permission to do so.

This part of the toolkit will explain the meaning of some of the most important terms in data protection. It will also tell you what your legal responsibilities are as a data controller and give you some useful tips for implementing privacy in your business.

Legal Framework

This part of the toolkit is based on parts of Nigeria's data protection laws, which you can read about below:

- [The Nigeria Data Protection Regulations \(NDPR\), 2019](#)
- [The Nigeria Data Protection Regulations \(NDPR\): Implementation Framework](#)



Definition of terms

Personal Data: Any information that could be used to identify an individual directly or indirectly. Examples include: name, address, date of birth, phone number, identification number, email address, etc.

Sensitive Personal Data: These are special categories of personal data that require extra protection because there could be potential harm to the data subject (individual who owns the data) if the data gets into the wrong hands. These types of personal data include biometric data, genetic data, sexual orientation, racial or ethnic data, religious beliefs, political opinions, and trade union membership.

Processing: is any operation performed on personal data. This could include, but is not limited to, collecting, storing, changing, and sending personal information. Consider this as any and all things that you do to personal information throughout its entire life cycle.

Data Controller: is an individual or organisation that determines the why and how of processing personal data. You are a data controller if you decide the purpose and means of processing. For example, Chino decides to start a fashion business for profit and has a website set up (not necessarily by her) to display her wares and to create an avenue for customers to make purchases. The purpose of processing is to make a profit (she could have more reasons) and the means of processing is through the website.

Data Processor: is an individual or organisation that processes on behalf of the data controller. You are a data processor if you act on the instructions of a data controller. Example: Flowing from the example above, Silverstar Payment offers payment services. Chino partners with them to process payments on her website. Silverstar Payment, in this case, is a data processor.

Data Subject: is a human being that has been identified or is identifiable or is the subject of personal data. For example, customers, clients, patients, employees, and ex-employees, among others.

Third parties : are individuals or organisations that you may enter into an agreement with to provide specific services that are intended to further the aims and objectives of your business.

Example: The human resources department of PayUs Limited has engaged Chai Foods to deliver lunch weekly to its employees who work remotely. Chai Foods is providing a service to PayUs Limited and has been provided the relevant personal data to perform such a service. In this instance, Chai Foods is a third-party service provider.

Data Breach: occurs where personal data gets into the wrong hands. In other words, personal data is accessed, disclosed to, copied, transmitted to, or stolen by a person who should not have access to such personal data.

Example: An unknown individual hacks into Waterworks Limited's network system and steals sensitive information which includes personal data or when you wrongfully send an attachment or document to a wrong person.

Obligations under the law (what the law expects you to do)

1. Knowing why you collect and process data? and whether it is legal to collect the data that you do.

You cannot avoid processing personal data if you run a business that deals with customers. It is important to know why you collect the data that you do and whether you have a legal basis to do so. But first, identify the purpose of processing. It could be to complete a transaction, respond to a customer complaint, resolve a dispute, prevent fraud, deliver goods to the customer, or complete a transaction on behalf of a customer, among other things.

You may process personal data for whatever reason you have decided to set up your business. However, under the GDPR, every reason or purpose must have a corresponding lawful basis. Note that all the lawful bases may not apply at once or in all circumstances. You are provided with five (5) lawful bases under the law, which are:

- **Consent:** You may rely on this lawful basis where the data subject agrees to your processing of their data. This “agreement” must be clear and leave no room for doubt. It may be given orally, in writing, or by clicking an option, among other measures.

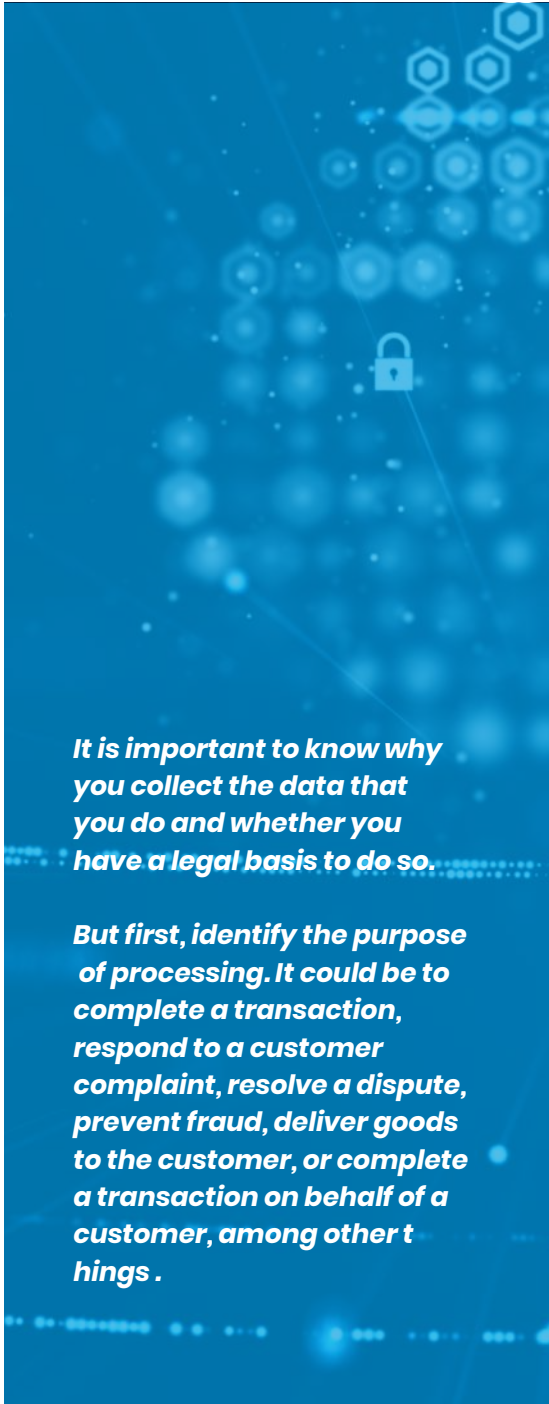
For example, Didi, a customer, may say, “I give you permission to publish my image and feedback on your website” before you can do so to display a customer review.

- **Performance of a contract:** Where there is a contract between two or more parties, or to complete a contract on behalf of another party (customer). For example, a service provider and a customer may each process personal data in order to fulfil their obligations under the contract.

For example, when Busola places an order for a wig, the disclosure of her address for delivery, phone number for confirmation, you sharing your account information, or processing of the order will be on the basis of the performance of a contract between you and Busola.

- **Compliance with a legal obligation:** The law often imposes obligations on data controllers. In such situations, you may need to process the personal data of individuals.

For example, if Lola is an employee of Halo Dynamics, for tax purposes (which is a legal obligation), Halo Dynamics would have to process Lola’s personal data to file tax returns. In addition, implementing measures to fulfil Know Your Customer (KYC) or Anti-Money Laundering (AML) obligations is a legal obligation.



It is important to know why you collect the data that you do and whether you have a legal basis to do so.

But first, identify the purpose of processing. It could be to complete a transaction, respond to a customer complaint, resolve a dispute, prevent fraud, deliver goods to the customer, or complete a transaction on behalf of a customer, among other things.

- **To protect the vital interests of the data subject:** you may rely on this lawful basis where one is acting in the interest of a data subject who, at the time, is unable to make decisions on their own.

For example, Ngozi has just had an accident at work and was taken to the hospital unconscious. The hospital is unable to reach out to the next of kin but needs to perform some emergency care on Ngozi. The hospital may rely on this lawful basis when processing her personal data.

- **Performance of a task carried out in the public interest:** processing of personal data will be lawful under this basis where it is done for the benefit of the public.

For example, the government imposing the requirement to wear a face mask is done under public health.

2. Principles that should guide your processing of personal data

Implementing the principles of data processing can help your business stay on the right side of the law. The following are principles you should rely on:

- **Transparency:** You are expected to have a privacy notice (refer to the part where it is defined) or provide information to the customer about how you process data. **For example, say briefly on your website what the purpose of processing is and any other relevant information.** This will be accomplished by posting a privacy notice on your digital platforms.
- **Purpose limitation:** You are not expected to use customers' information for other purposes you have not disclosed to them. If you need to, inform them. **For example,** if Hauwa buys her Zara make-up kit from you, it would be wrong for you to start sending her unsolicited newsletters or advertisements about unrelated products.
- **Data minimisation:** The personal data that you collect must be as minimal and reasonable as possible. You should not collect personal data that you do not need. **For example,** do not ask for a customer's maiden name or sexual orientation because you want to deliver a product to the individual's home.
- **Accuracy:** You must ensure that the personal data you process is accurate and kept up-to-date. You should give data subjects the opportunity to correct any inaccuracies.
- **Storage limitation:** You are only to keep personal data for as long as you need it or for as long as you are required by law to keep it. See section 8.
- **Integrity and confidentiality:** You are to ensure the security of the personal data that you process. See section 7.

3. Dealing with data subjects:

Data subjects have certain rights under the law when it comes to their personal data that you process. You will need to have a process in place to respond to these requests as they come. This **Guide** may prove useful in doing so.

4. Information Provision Obligations/Publishing a Privacy Notice:

As a business that processes the personal data of individuals, you are required to let them know why and how you use it. This notice is often published on a website, mobile application, or any digital medium, and should be simple, accessible, and straightforward. Your notice may look like [this](#).

5. Documenting your processing activities.

When running your business, it is important to know and understand your processing activities for the sake of transparency. When you work with personal information, you have to keep a record of everything you do with that information. This document is referred to as a "Record of Processing Activities" (RoPA). In this document, there would be information about storing data in the cloud, disclosure of data to other parties, and the legal basis and goals of processing. and so on.

It may seem daunting to document this. However, depending on your business, it does not have to be. A RoPA looks like [this](#). You may also refer to this [Guide](#).

6. Sending personal data outside Nigeria:

There may be instances where your clients, customers, or employees' personal data may "travel" across borders (outside the country). When this needs to happen, you have to ensure that you put in place measures to protect the data you are sending out. For such a transfer of data, you must also have a legal reason to do so, as set out by the law.

Here is an example of a situation where personal data "crosses borders": Lola runs SuperFlair, a fashion business headquartered in Nigeria. She decides to open branches of her business across Africa. Cross-border transfers would be when SuperFlair Nigeria sends personal information to the other countries where SuperFlair is present. Another example is when SuperFlair uses different service providers who don't actually process the data in Nigeria. For example, the use of communication, analytics, and cloud storage tools.

7. Keeping personal data safe:

As a data controller, you are responsible for keeping the personal information you handle safe. This obligation requires you to set up effective mechanisms to safeguard personal data from being hacked or even accidental loss or damage. Also, this means that you won't be able to say "it was an accident" as an excuse if you lose, get hacked, or destroy personal information. The obligation to safeguard personal data covers both physical, organisational and electronic security. For example, if you have paper documents containing personal information about customers, you would store them in a locked file cabinet and limit access to them to only those who need to use or know them, as well as ensure that you and your employee(s) log off computers after work. You will also be expected to keep your password strong, safe and not shared with anyone. Part of security is using two-factor authentication so your online account does not get hijacked.

In guiding you on how to keep the personal data you process safe, section B of this toolkit will show you how to safeguard personal data and how to identify online activities that could jeopardise the safety of personal data and ways to avoid them.

Please see the section on cybersecurity.

8. Retaining personal data:

You are required to keep personal data only as long as it is needed. That is, you cannot hold people's personal data forever—"just in case..." For example, if you made a deal with Madam Joyce five (5) years ago to deliver fabrics to her house, you cannot keep her home address forever "just in case she wants to place another order." In other words, there is a limit to how long you can hold personal data, after which you must delete it.

In deleting personal data, do not let your trash become another person's treasure. You must dispose of personal data properly, such that it can not be retrieved by anyone else. For example, do not just crumple up documents with personal information and throw them away because it's easy to get them back. Instead, shred it properly. If the personal data is in an electronic format, use an electronic shredder. When disposing of devices such as flash drives and hard drives, wipe out the data from them. The same is true for computers. To keep deleted files from being recovered, they must be wiped and written over.

You should pay attention to the considerations in determining the retention period. A retention period can be set by law, by a contract, by a business need, in the case of a legal claim, for archiving, or for some other reason.

Understanding Data Retention

Storage limitation is one of the principles of data protection provided under the Nigeria Data Protection Regulation (NDPR). The principles provides that personal data should not be kept in an identifiable form for no longer than it is necessary for the purposes for which the personal data are processed.

Personal data must be deleted or anonymised as soon as they are no longer needed for purposes for which they were collected.

What is a data retention policy?

A data retention policy is an organization's system of rules for holding, storing, and deleting the information it generates and otherwise handles."

Duty of the data controller

Consequently, it becomes the duty of the controller to find out, from various national legislations, the retention periods applicable to each type of data it processes, in order to formulate retention schedule and time limits.

Importance of storage limitation

Data retention assist businesses to reduce the burden of record management, enables efficient management of records stored and control unrestrained growth of record volume, reduce storage cost, improve the ability to locate and retrieve record when required, limit exposure to liabilities, improve utilisation of resources, and also to comply with the provision of the law.

Implication of excess retention

Lack of a viable basis to keep record longer or shorter timeline exposes an organisation to risk, such as litigation and sanction from the data protection authority. Storing record in excess imposes difficulty in location and identification of records when required for reference and legal compliance.

What is a data retention schedule?

"Retention schedules establish guidelines regarding how long important information must remain accessible for future use or reference, as well as when and how the data can be destroyed when it is no longer needed." The schedule outlines the type of data, the business reason or decision for retaining the data, and the retention period.



SOME OF THE STATUTORY DATA RETENTION SCHEDULE UNDER THE NIGERIAN LAW

Law	Duration
Money Laundering Act	5 years
Cybercrimes Act	2 years
Regulation on Consumer Protection (2007) – Nigeria	12 months
Guidelines for the Provision of Internet Service	12 months
Framework for Mobile Payments Regulation (CBN)	5 - 7 years
Regulation for Direct Debit Scheme (2018) - CBN	6 years
Guideline on International Money Transfer Services in Nigeria (2014) - CBN	7 years
Guideline on Point of Sale (POS) Card - CBN	10 years
Guideline on Documents and Record Retention by the Medical Laboratory Science Council of Nigeria	Contains different retention time for different health record
Labour Act	3 years
Credit Reporting Act	6 years
Minimum Wage Act	3 years
Dangerous Drugs Regulations	2 years
Deep Offshore and Inland Basin Production Sharing Contracts Act	5 years
Foreign Exchange (Monitoring and Miscellaneous Provisions)	7 years
Companies and Allied matters Act (CAMA)	6 years
The Police Act	Permanently (in case of recording)
Lawful Interception of Communications Regulations, 2019	3 years

Examples of the retention periods under Nigerian law.

9. Use privacy-preserving tools:

When it comes to prioritising the protection of personal data, it is advisable to use certain recommended tools that have high privacy settings by default. See the infographic below for some of the suggested tools:

TECH HIVE ADVISORY

SUGGESTED PRIVACY TOOLS

Search Engine

- DuckDuckGo
- Startpage
- SearchEncrypt
- Qwant
- Swisscows

Browser

- Brave
- Tor Browser
- Ghostery
- DuckDuckGo
- Bromite
- Firefox Focus
- Jive Search

Email

- ProtonMail
- Hushmail
- StartMail
- PGP/GPG

Social Network

- Mastodon
- Diaspora
- Friendica
- PixelFed
- Pleroma
- Minds

Ad Blockers

- Ad Guardian
- uBlock Origin
- Adblock Plus

Tracker Blockers

- Privacy Badger
- Ghostery
- uMatrix
- Disconnect
- Cookies Auto Delete

Secure Messaging

- Signal
- Threema
- Off-the-Record

Password Manager

- KeePassXC
- Bitwarden
- Enpass
- Blur
- 1Password
- Mitro

Productivity/Collaborative tools

- CryptPad
- Etherpad
- Dudle
- Framadate
- Matrix
- Rocket.chat

Encrypted DNS

- Https 1.1.1.1.

Web Hosting

- Bahnhof
- Njalla
- DataCell
- Orange Website

File Sharing

- Syncthing
- SparkleShare

Drive / File Storage

- Tresorit
- Cryptomator
- SpiderOak

Free SSL

- Let's Encrypt

File Shredder

- Eraser

Apps Permission Manager

- Dock

Privacy Policy

- Terms of Service; Didn't Read (ToS;DR)

Secure Operating System

- Tails OS
- Debian
- Arch Linux
- Qubes OS

Encrypted Voice Calls

- Silent Circle
- Mumble
- Linphone

File encryption

- VeraCrypt
- PeaZip
- Hat.sh

File sharing

- Onion Share
- Croc
- Magic Wormhole

10. Audits:

As a business that deals with people's personal information, you must have your privacy practises checked every year. This helps to assess your compliance with the law. The NDPR mandates all organisations that process the personal data of more than 1000 data subjects in a period of 6 months or 2000 data subjects in a period of 12 months to submit a Data Protection Audit report no later than March 15th every year.

Other compliance considerations

In addition to the above obligations, you must also take other steps to build your privacy program.

Obligations	Explainer
Use a contract when dealing with third parties.	Use a data protection clause or agreement when you engage other people or organisations with data processing. Consider those you share personal data with.
Notify the data subject in the event of a data breach.	When there is a data breach that can cause high risk to people, you need to notify them. For example, if you wrongfully send a patient's test result to another patient.
Notify the data protection authority.	When there is a data breach, you should notify the appropriate authorities within 72 hours of finding out about the breach.
Appoint a data protection officer or a privacy champion.	Designate someone within your enterprise to be responsible for the privacy function. As a small business, you can engage a privacy champion for this purpose,
Data protection by design and default.	Think about privacy from the design stage, and embed it into your process and business.
Data Protection Impact Assessment. (DPIA)	You may need to conduct a DPIA for high risk processing. Mainly to identify these risks and mitigate them. For example, deploying AI in your process will mean assessing the risk to people. You will find this Guide useful.
Keep documentation of policies, procedures, and guidelines.	Maintain policies and procedures that support privacy.
Training and awareness	<i>"If you don't train them, you can't blame them."</i> Train or attend training and awareness sessions on data protection and online security.



Privacy Implementation Tips

Considering how significant data protection has become in recent times, with businesses being fined for violating data protection principles and the reputational damage such violations cause for businesses, we have included the following data protection implementation tips:

- **Take stock of your data.**

It is impossible to protect what you don't know. Therefore, you need to know how much personal data you collect, the source, where and how you store it, and to whom you disclose it. For this activity, make a list of the devices, servers, browser extensions, cloud services, apps, and communication tools you use to collect, store, and send personal information. See how to curate a [data inventory](#).

- **Reduce the data you collect.**

Reduce your data collection to only what you need. For example, if there is no reason you need to have their mother's maiden name, do not ask for it. Also, do not collect unnecessary personal data. By collecting as little information as possible, your personal information is less likely to be hacked. The data you do not have cannot be stolen.

- **Verify the privacy practices of the third-parties with whom you share personal data.**

If you share your client's personal data with other service providers or any other third party, you need to verify the existence of their data protection and security measures to prevent them from introducing risk or harm into your environment. For example, if you use logistics and shipping companies (third parties) to run your business, make sure that these companies have privacy policies in place. This is necessary because if they mishandle the data you gave them, you may still bear the commercial and reputational damage. So, before you give them your personal data, have them sign a data processing agreement that says how they will handle your personal data or input a standard data protection clause in your service level agreements (SLA) or in the main agreement.

Here's a template of a standard data protection clause between "B" and "X" (third-party vendor):

"Both parties acknowledge and agree that all data provided by the Parties, or to which the Parties may be exposed, shall constitute Confidential Information and where applicable, intellectual property belonging to the disclosing Party.

i) "X" hereby warrants to "B" that it shall at all times strictly comply with all applicable laws and with all the provisions and requirements of both Party's data protection policies and procedures communicated to them which may be in force from time to time;

ii) it shall not, at any time process data for any purpose other than to the extent necessary for the fulfilment of the terms and conditions of this Agreement; and

iii) it shall ensure that all its systems and operations on which data is processed as part of the performance of its obligations under this Agreement shall, at all times, be of a minimum standard required by all applicable laws and be of a standard no less than the standards which are in compliance with the best industry practice for the protection, control and use of data.

iv) Each Party shall ensure that upon termination, cancellation, expiration or conclusion of this Agreement they shall physically or electronically destroy beyond all ability to recover all information/ data provided to them within 30 (thirty) days, save for that which is required by law to be preserved. Within such a 30-day period, the Party shall certify in writing to the other Party that such destruction has been completed. ..."

- **Notify Individuals when you collect their personal data.**

At every point where personal data is collected (website, apps, physical, etc.), you must inform data subjects that you will be collecting their personal data before this information is collected. The privacy notice is the document that serves to inform data subjects. Your privacy notices must contain information about the types of personal data you will collect, the purpose for which you are collecting it, how long you will keep it, the lawful basis upon which you are collecting it, whether it will be transferred to a third party, the rights they can exercise and how to exercise them, etc.

- **Privacy by design where necessary:** If you have built an app to scale your business, ensure that you have privacy embedded in the app's design and that the app, by default, collects very minimal personal data.

- **Be prepared for a data breach.** Nobody hopes for a data breach. However, it will be safe to prepare for one by having a data breach response plan in place and a backup file. The goal of the response plan is to help you take quick action within 24 hours of finding a data breach. This will help you contain, assess, and respond to the breach quickly, lessen the damage that could happen to the people whose data was compromised, and follow the law on data protection.

Conclusion

In this information age, adhering to data protection principles has become important and entrepreneurs must pay attention to it in order to build a thriving online-enabled business. This is because there is a growing awareness of the protection of people's right to digital privacy as well as ensuring the safe handling of transactions that require personal data.

Adopting a privacy program will not only ensure that your business is not fined for data protection violations, but will also increase your business's reputation, which will ultimately lead to client satisfaction and trust.



Section B – Cybersecurity

According to the ISO/IEC 27032:2012 Information Technology – Security techniques – Guidelines for Cybersecurity Standard, "cybersecurity, or cyberspace security, is defined as the protection of privacy, integrity, and accessibility of data information in the cyberspace. Therefore, cyberspace is acknowledged as an interaction of persons, software and worldwide technological services".

Cybersecurity can also be described as the application of processes and controls for the protection of information and internet-connected systems, such as hardware and software systems, from cyber threats and cyber attacks.

This part of the toolkit provides information on cybersecurity risks and weaknesses that small and medium scale businesses may face and provides guidance to make sure your organisation is well protected as well as cyber-smart.

Legal Framework

The current law regulating cybercrimes in Nigeria is accessible below:

Cybercrime (Prohibition, Prevention, Etc.) Act, 2015



Some of the laws impacting cybersecurity in Nigeria.

Definition of terms

Cybersecurity Vulnerabilities (vulnerabilities): Cybersecurity vulnerabilities refer to weaknesses of an asset or control in modifying a risk that can be exploited by threats.

Cybersecurity Threats (threats): Cybersecurity threats refer to the potential cause of an unwanted incident, which may result in harm to a system or organisation.

OTP (One-Time Password): This is an automatically generated number or alphanumeric string of characters that authenticates a user for a single transaction or login session.

OS (Operating System): is the program that, after being initially loaded into the computer by a boot program, manages all of the other application programs on a computer.

SSL (Secure Sockets Layer): it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. Thus, it is essential for websites to have an SSL certificate.

TLS (Transport Layer Security): TSL is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term. TSL is an essential certificate for websites to implement security.

HTTPS (Hypertext Transfer Protocol Secure (HTTPS): SSL/TLS certificates are what enable websites to move from HTTP to HTTPS, which is more secure.

Cybersecurity Threats

A potential source of an undesirable outcome, including human, environmental, or natural causes, that is capable of acting against an asset in a manner that can result in harm. In a negative situation in which loss is likely to occur, over which one has little control. Cyberthreat actions are malicious attacks that seek to disrupt digital operations and unlawfully access data and information. Threats may emanate from external space, with a direct effect on the device. While some threats may only constitute a nuisance, others are more impactful and may even threaten human life as a result of the sensitivity or criticality of data that might be stolen and leaked in the process. Examples of cybersecurity threats include:

- **Malware:** A malware is any program that is intentionally designed to cause harm. It's a collective term that includes viruses, trojans, worms, ransomware, spyware, adware, etc. A virus is the most common type of malware attack, and in order for a virus to infect a system, it requires a user to click or copy it to media or a host.
- **Web-based attacks:** When criminals exploit vulnerabilities in coding to gain access to a server or database, these types of cyberthreats are known as application-layer attacks. Although bad actors do not generally compromise data through these means, they often use them to "distract" automated systems, leaving them vulnerable to other

malware and criminal activities. Popular web-based attacks include: cross-site scripting (XSS), SQL Injection (SQLI), path traversal, local file inclusion, and distributed denial of service (DDoS) attacks. Fortunately, there are methods you can employ to provide analysis and protection for your site and its underlying servers and databases. They include the following: automated vulnerability scanning and security testing, Web Application Firewalls (WAFs) and Secure Development Testing(SDT),

- **Spam:** Spammers use many forms of communication to bulk-send their unwanted messages. Some of these are marketing messages peddling unsolicited goods. Other types of spam messages can spread malware, trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.
- **Business identity theft:** Business identity theft, also called corporate identity theft, is defined as “identity theft committed with the intent to defraud or hurt a business by creating, using, or attempting to use a business’s identifying information without authority.”
- **Insider threat:** An insider threat is a security risk that originates from within the targeted organisation. It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts, but it does not always have to be that way. Insider threats may sometimes be overlooked within many organisations.
- **Botnets:** Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the words “robot” and “network.” The assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.
- **Ransomware:** The digital version of being evicted and locked out of your digital life. It’s a type of computer program that serves to encrypt the data storage of a target device, thereby making it inaccessible without the use of a key. In most cases, this is done with the intent that some benefit be bestowed on the cybercriminal; otherwise, the data is permanently deleted.
- **Trojan:** They are attack programs hidden in nice looking documents, images, or files. A trojan is usually disguised as genuine software or a program and is installed on the digital device, with no indication of its harmfulness, while it quietly causes damage to data in the background, unnoticed.
- **Worm:** This manifests itself in the nature of a self-replicating program, with the capacity to identify contacts database or file sharing mediums for the purpose of sending itself to unsuspecting recipients in the guise of emanating from the original owner. It could attach itself to an email, for example. The purpose is to expose the data of the unsuspecting recipient to vulnerability. This usually reaches the recipient in the form of ‘phishing.’
- **Phishing:** This kind of attack usually appears as mail from a person of repute requesting the recipient to accept malware. The email would normally not show itself to be from an untrusted source. An example is a cloned email from a company executive to subordinate staff, requesting confidential details. A more advanced level of phishing is “spear phishing,” where the attacker understudies the victim for some time and poses as a trusted friend, before eventually launching an attack.

Cybersecurity Vulnerabilities

Most users of digital devices like phones and computers do not know the kinds of actions or inactions that expose their devices to vulnerability from the inside, even without the activities of attackers from the outside.

In essence, these vulnerabilities are not a creation of the cybercriminal but serve to enhance their activities. We refer, here, to those intentional or unintentional acts by the business woman which expose her systems to risks. They represent the flaws already present in a system that opens the gate for attacks from the outside.

Cybersecurity vulnerabilities are distinguished from cybersecurity threats in the sense that while threats may be launched from the outside, vulnerabilities are already contained in the system. An inexhaustive list of vulnerabilities that may exist on a system is presented below:

- **Employees:** these may constitute the highest vulnerabilities in a workplace if not properly trained or instructed on the use of digital devices and data at their disposal. An employee whose device is not fortified may be the link through which access is gained to the data of others.
- **Hidden backdoor programs:** Hidden backdoors are intentionally installed by software developers to provide remote access for performing legitimate functions such as customer support or resolving software issues. However, they constitute an enormous software vulnerability because they make it all too easy for someone with knowledge of the backdoor to illicitly access the affected computer system and any network it is connected to.
- **Unknown security bugs in software programming:** Computer software is incredibly complicated. When two or more programs are made to interface with one another, the complexity can only increase. The issue with this is that within a single piece of software, there may be programming issues and conflicts that can create security vulnerabilities. When two programs are interfaced, the risk of conflicts that create software vulnerabilities rises. Programming bugs and unanticipated code interactions rank among the most common computer security vulnerabilities—and cybercriminals work daily to discover and abuse them.
- **Unrestricted upload of dangerous file types:** Unrestricted File Upload vulnerability occurs due to insufficient or improper file-type validation controls being implemented prior to files being uploaded to a web application. Without these methods of validation in place, a malicious actor may be able to craft the upload request to bypass the application-layer defences and potentially completely compromise the system.
- **URL redirection to untrusted sites:** URL redirection is a vulnerability that allows an attacker to force users of your application to an untrusted external site. The attack is most often performed by delivering a link to the victim, who then clicks the link and is unknowingly redirected to the malicious website.
- **Unpatched security vulnerabilities:** One of the biggest mistakes that they usually make is to not patch those vulnerabilities once they're discovered. Thus, once a vulnerability is discovered, it should be managed and patched as soon as possible.
- **Weak passwords:** A weak password can give hackers immediate access to your account because, once hackers have cracked one account, it's very easy for them to access your other accounts and devices. For example, access to your email account could easily provide a hacker with access to all other social media platforms.

- **Out-of-date software:** Hackers use exploit attacks to install malware (including backdoors) on user devices. But if you keep all of your software updated, you're probably not going to be the victim of such attacks.

What to do to ensure you are cybersmart?

- **Use complex passwords:** It is advisable to use a good mixture of upper/lower case letters, numbers, and symbols, and the password should be at least seven characters long (the longer the better). Passwords should also not be based on personal information that is easily public knowledge, e.g. first name, last name, date of birth, or phone numbers. We understand it might be tempting to use one password for all your accounts, but this would mean that a compromise to one account is a compromise to all. Therefore, use different passwords for different accounts and make use of a password manager to store passwords.
- **Use multi-factor authentication:** Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application or online account. They could be in the form of hardware token, SMS-based OTPS, mobile in-app notifications or biometric verification. Multi-factor authentication reduces the risk of your accounts or online profiles being compromised.
- **Only download and use services from credible sources:** Avoid downloading or using services that are not credible, For example, clicking on random websites or links to download songs, applications, visit sites, or access free websites might lead to downloading malware or viruses. Thus, it is safer to download from credible and verifiable sources. Always install popular and well-tested anti-virus software and use official distribution websites and platforms only.
- **Use antivirus software:** antivirus products work by detecting, quarantining and/or deleting malicious code, to prevent malware from causing damage to your device. Modern antivirus products update themselves automatically, to provide protection against the latest viruses and other types of malware.
- **Pay attention to phishing signs:** At a certain point, all of us have received an email purporting to be from our bank, a website, or another organisation asking us to update our information or change our password. There are other ways that attackers try to phish you as well, such as by asking you to click on a malicious link or divulging your private information by SMS, social media, or even phone calls. To avoid getting phished, you need to pay attention to minute details such as the sender's email address or manner of request. For example, Instagram would never send you an SMS to change your password. Once you notice a weird email or a look-alike email, avoid opening such emails or downloading attachments from them.
- **Provide firewall security for your Internet connection:** Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Most operating systems (OSs) and internet routers include a built-in firewall feature that you should enable for added protection, even if you have an external firewall. Firewall software is also available separately from your local computer store, software vendor, or ISP. If you download firewall software from the internet, ensure it is from a reputable source.

- **Do not connect to public internet sources:** Remember that free services might not always be free. It is advisable to avoid using public Wi-Fi because it may provide hackers the opportunity to position themselves between you and the connection point. So instead of talking directly with the hotspot, you're sending your information to the hacker, who then relays it on. However, if you must use public Wi-Fi, do not share your private information at any time while connected, don't log into accounts you are not already logged into or share financial information.
- **Backup your data:** In the event of data loss or corruption, a recent and comprehensive data backup is the only way to recover. Your backups must also be protected.
- **Keep all operating systems updated:** Do not postpone updating your systems. It is crucial to keep all your systems and software up to date. When security issues are discovered in software or the OS, security patches and fixes for them are released to users in the form of updates.
- **Training and retraining of employees:** As stated above, employees may be the weakest link through which data is compromised. Cybersecurity training and retraining helps them to identify and avoid attempts at data compromise. Again, the policy of "least privileges" would help to minimise the kind of access to data made available to an employee at a given time, thereby not subjecting too much data to cyber attacks.
- Set computer screens to lock automatically when left unattended for a specific period of time.
- Restrict use of external devices on all company issued computers to authorised people only.

Our periodic security advisory is also available via this link: [Security Advisory - Tech Hive Advisory](#)

Conclusion

Having a cybersecurity program or plan can deliver genuine benefits for small and medium-sized enterprises. With a cybersecurity program, it is easy to protect against risks, vulnerabilities, and threats, thereby building trust and loyalty while avoiding losses that may have otherwise occurred from security breaches and loss.

Resources

The links below provide some useful tools you may consider for your business:

- **Privacy Tools:** This resource recommends privacy tools that are primarily chosen based on security features, with additional emphasis on decentralised and open-source tools. They are applicable to a variety of threat models ranging from protection against global mass surveillance programs and avoiding big tech companies to mitigating attacks.
- **Privacy Toolkit:** This resource provides a toolkit of websites, extensions, and sources that can help you protect your privacy online.
- **URLScan:** this tool helps you understand malicious websites.
- **WebSec Security Test | ImmuniWeb:** The tool can be used to scan websites for vulnerabilities. The web security test scanner allows you to scan websites to check for cybersquatting, typosquatting, cross site scripting, and potential phishing.
- **SSL Security Test | ImmuniWeb:** The tool allows you to scan for the availability of SSL/TLS which indicates a more secure website.

Other Resources

- Microsoft OneDrive - Access Files Anywhere. Create Docs with Free Office Online.' <<https://onedrive.live.com/redirect?resid=2DDD3BCF8A2C0E7C!1642&authkey=!AGvhLfITwt-U5-o&ithint=file%2cpdf>> accessed 13 September 2022
- 'Cyber Security Geek to English Glossary' <<https://www.wizer-training.com/wizernary>> accessed 13 September 2022
- 'Top 5 Computer Security Vulnerabilities - Compuquip' <<https://www.compuquip.com/blog/computer-security-vulnerabilities>> accessed 13 September 2022

